2024

Ризики та загрози легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансування тероризму в умовах військової агресії російської федерації - 2024

Державна служба фінансового моніторингу України

Держфінмоніторинг є підрозділом фінансової розвідки «адміністративного типу», який реалізує державну політику щодо запобігання відмиванню коштів, фінансуванню тероризму та розповсюдженню зброї масового знищення.

Ключове завдання Держфінмоніторингу це збір, обробка та аналіз інформації про фінансові операції, у тому числі що підозрюються у відмиванні коштів, фінансуванні тероризму чи розповсюдженні зброї масового знищення.

У разі підозри на ВК/ФТ/ФРЗМЗ, Держфінмоніторинг передає матеріали правоохоронним та розвідувальним органам, враховуючи визначену законодавством підслідність злочинів.

Типологічні дослідження Держфінмоніторингу включають інформацію, яка була надана учасниками системи фінансового моніторингу та правоохоронними органами на відповідний запитальник.

Детальна інформація про Держфінмоніторинг розміщена на сайті: www.fiu.gov.ua

Посилання для ознайомлення з типологічними дослідженнями Держфінмоніторингу:
www.fiu.gov.ua/pages/dijalnist/tipologi

ЗАТВЕРДЖЕНО
Наказ Державної служби
фінансового моніторингу України
26.12.2024 №95

Типологічне дослідження на тему:
«Ризики та загрози легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансування тероризму в умовах військової агресії російської федерації – 2024»

Російська агресія проти України стала каталізатором зростання нелегальних фінансових потоків на національному та міжнародному рівнях. Війна продовжує підривати глобальну фінансову стабільність, посилює вразливість населення та ускладнює фінансовий моніторинг, створюючи сприятливе середовище для приховування злочинних доходів, розширення тіньової економіки та обходу санкцій.

Дане типологічне дослідження містить виявлені актуальні схеми легалізації (відмивання) злочинних доходів та пов'язаних злочинів, а також фінансування тероризму (сепаратизму), що вчинялись в умовах військової агресії росії, узагальнено методи, інструменти схем ВК/ФТ та індикатори підозрілості.

Застосування ризик-орієнтованого підходу є основоположним для формування підозр у вчиненні злочинів та розробки стратегій для їх запобігання та протидії.

Типологічне дослідження може стати підґрунтям для ідентифікації та протидії поширенню злочинів, що можуть бути характерними під час війни. Дане дослідження також може бути корисним при здійсненні нагляду та внесенні змін до законодавства.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

Держфінмоніторинг	Державна служба фінансового моніторингу України
ВК	легалізація (відмивання) доходів, одержаних злочинним шляхом
ВК/ФТ/ФРЗМЗ	легалізація (відмивання) доходів, одержаних злочинним шляхом, фінансування тероризму та фінансування розповсюдження зброї масового знищення
ПВК/ФТ/ФРЗМЗ	протидія легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансування розповсюдження зброї масового знищення
КБВ	кінцевий бенефіціарний власник
КК України	Кримінальний кодекс України
НПО	неприбуткові організації
ПФР	підрозділ фінансової розвідки
білорусь	республіка білорусь
росія	російська федерація
СПФМ	суб'єкт первинного фінансового моніторингу
СПД	суб'єкт підприємницької діяльності
ФОП	фізична особа–підприємець
FATF	Група з розробки фінансових заходів боротьби з відмиванням грошей

ПЕРЕДМОВА ГОЛОВИ ДЕРЖФІНМОНІТОРИНГУ

2024 рік став важливим у боротьбі з фінансовими злочинами, особливо в умовах триваючої військової агресії росії проти України. Система ПВК/ФТ продовжує свій розвиток.

Війна створює нові загрози для економічної стабільності та фінансової безпеки, підвищуючи ризики відмивання коштів, фінансування тероризму, обходу санкцій та інших злочинів, що продукують незаконні доходи.

Одним із ключових інструментів нівелювання таких ризиків є типологічні дослідження, що дозволяють ідентифікувати та систематизувати схеми злочинів через вивчення фінансової складової причетних до цих злочинів осіб, які сприяють вдосконаленню методів моніторингу та можуть забезпечити ефективні кримінальні розслідування та переслідування.

Тенденції щодо наявних ризиків свідчать про виклики стосовно використання злочинцями криптовалют, транскордонних операцій, шахрайства, кіберзлочинів, обходу санкцій та приховування реальних бенефіціарних власників.

Також, враховуючи розвиток новітніх сучасних технологій та диджиталізацію, виявлення відмивання коштів стає ще складнішим. За таких умов робота системи протидії легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансуванню тероризму, фінансуванню розповсюдження зброї масового знищення та обходу санкцій має бути гнучкою, швидкою та адаптованою до цих викликів.

Ігор Черкаський

ВСТУП

Російська агресія проти України, що розпочалася у 2014 році та досягла небачених масштабів з лютого 2022 року, стала серйозною загрозою для глобальної фінансової стабільності та економічної безпеки. Її наслідки відчуваються далеко за межами України, впливаючи на світову економіку, порушуючи ланцюги постачання та створюючи виклики для міжнародної безпеки.

В умовах військових дій виникли нові виклики для системи ПВК/ФТ/ФРЗМЗ. Війна, як частина гібридної агресії, супроводжується активізацією організованої злочинності та дестабілізацією економічної ситуації в Україні.

Одним з найбільших викликів є поширення схем фінансових злочинів, пов'язаних із ВК/ФТ, які на фоні війни набули нових форм та різновидів.

Це дослідження спрямоване на аналіз сучасних методів легалізації доходів, отриманих злочинним шляхом, фінансування тероризму та уникнення санкцій, що використовуються злочинними угрупованнями та росією. Особливу увагу приділено впливу новітніх технологій, таких як використання криптовалют, та складним схемам обходу міжнародних обмежень.

У документі також розглядаються актуальні приклади корупції, використання окупованих територій для нелегальних фінансових операцій та механізми фінансування терористичної діяльності. Застосування ризик-орієнтованого підходу є ключовим у забезпеченні ефективності системи фінансового моніторингу та розробці стратегій боротьби з такими загрозами.

Актуальність дослідження визначається необхідністю адаптації методів протидії до сучасних викликів, враховуючи використання сучасних технологій і масштабність нових форм злочинної діяльності.

Це типологічне дослідження спрямоване на вивчення сучасних методів та інструментів легалізації злочинних доходів, фінансування тероризму, а також виявлення осіб та активів, причетних до злочинів.

Актуальність цього дослідження обумовлена зростаючими ризиками для національної фінансової безпеки в умовах війни, а також необхідністю розробки нових підходів до ПВК/ФТ/ФРЗМЗ, з урахуванням сучасних реалій та технологічних змін.

РОЗДІЛ І. ЗАГАЛЬНІ ТЕНДЕНЦІЇ

1.1. Росія – держава-спонсор тероризму

Розпочавши збройну агресію проти України, росія порушила фундаментальні норми й принципи міжнародного права, низку двосторонніх і багатосторонніх договорів та угод. Наразі росія військовим шляхом тимчасово захопила та утримує значну частину території України.

Росія як держава-спонсор тероризму, ставить під загрозу не лише стабільність регіональної безпеки, але й глобальну фінансову та політичну стабільність. Основні загрози, пов’язані з підтримкою росією тероризму:

Поширення терористичних актів і дестабілізація регіонів. Росія через терористичні угруповання сприяє дестабілізації ситуації в різних регіонах світу. Це призводить до гуманітарних криз, збільшення числа біженців та масового переміщення людей.

Нарощування фінансових потоків через нелегальні канали. Російські фінансові структури активно використовують кримінальні канали для фінансування терористичних операцій. Це створює значні ризики для міжнародної фінансової безпеки.

Інформаційна війна та маніпуляції. Росія використовує інформаційні війни як частину гібридної тактики для створення дезінформації та виправдання своїх терористичних дій. Інформаційні кампанії сприяють підриву міжнародного порядку, маніпулюючи громадською думкою, підтримуючи дестабілізацію в країнах-супротивниках.

Згідно з міжнародним правом, війна, вчинена росією проти України, супроводжується численними порушеннями, які включають як воєнні злочини, так і злочини проти людяності. Перелік цих злочинів є великим та включає безліч категорій, оскільки кожен злочин, вчинений під час конфлікту, може бути класифікований за різними міжнародними документами.

Фінансування війни та фінансування тероризму. Росія як держава-спонсор тероризму системно фінансує свою агресію проти України, використовуючи механізми, що безпосередньо пов’язані з вищенаведеними фактами. Розуміння джерел фінансування є ключовим для ефективного блокування каналів підтримки війни.

Джерела фінансування війни росії проти України є багатогранними та охоплюють як внутрішні, так і зовнішні механізми. Основні з них:

державний бюджет та державні ресурси – фінансуються артилерійські обстріли, ракетні удари, використання дронів-камікадзе;

експорт енергоресурсів – надходження від продажу нафти, газу та вугілля на міжнародних ринках;

зовнішні джерела фінансування – підтримка союзних країн та приховані канали фінансування;

активи державних корпорацій та олігархічних структур – близькі структури до кремля залучають кошти до підтримання військової агресії росії;

кримінальні канали та нелегальні фінансові потоки – сприяють фінансуванню терористичних актів, депортацій населення, а також співпраці з юрисдикціями, внесеними до чорного списку FATF;

економічний шантаж та енергетичний тероризм – руйнування енергетичних об'єктів та контроль над ядерними станціями створюють гуманітарну кризу та загрожують глобальній стабільності;

використання окупованих територій – ресурси, примусова праця та мобілізація з тимчасово захоплених територій є частиною фінансування війни;

інформаційна війна – підтримує агресію через маніпуляцію громадською думкою для виправдання воєнних злочинів, окупації та дестабілізації регіонів.

Попри міжнародний тиск і санкції, ці механізми підтримують здатність росії продовжувати агресію.

Росія, як держава-спонсор тероризму, використовує комплексні фінансові, економічні та інформаційні механізми для продовження агресії проти України.

Протидія агресору. Важливим елементом протидії агресору стали спільні політико-дипломатичні зусилля міжнародної спільноти.

У рамках міжнародних організацій та на двосторонньому рівні були прийняті численні документи та рішення на підтримку територіальної цілісності України в межах міжнародно визнаних кордонів.

Воєнні злочини та злочини проти людяності. Дії росії, включають воєнні злочини, енергетичний тероризм, масові депортації, співпраця з терористичними угрупованнями, що підриває глобальну стабільність та порушують міжнародне право. Через державний бюджет, нелегальні фінансові канали, використання ресурсів окупованих територій та інформаційний шантаж росія не лише фінансує свою агресію, але й створює гуманітарні кризи, дестабілізує економіку та загрожує міжнародній безпеці.

1.2. Фінансування тероризму та колабораціонізму

У 2024 році Україна посилює боротьбу з фінансуванням тероризму та колабораціонізму, адаптуючись до нових глобальних викликів. Це питання набуває особливої актуальності через російську агресію, яка використовує фінансові інструменти для підтримки терористичних угруповань і підриву стабільності в країні.

Одним із ключових викликів є використання криптовалют, що забезпечують злочинцям анонімність і ускладнюють відстеження незаконних фінансових потоків. Кіберзлочинність також набирає обертів, зокрема через фішингові атаки, крадіжки даних і зломи фінансових систем, які стають джерелами фінансування терористичної діяльності.

Росія спрямовує значні ресурси на фінансування пропаганди, інформаційних атак і підтримку підривних дій через підконтрольні медіа та організації, особливо на тимчасово окупованих територіях України. Ця діяльність включає поширення фейків, дискредитацію опонентів і виправдання терористичних дій.

Незаконні фінансові схеми часто здійснюються через міжнародні мережі з використанням офшорних юрисдикцій для приховування джерел коштів. Крім того, фінансування може здійснюватися через легальні структури, такі як бізнеси або культурно-освітні організації, що виконують роль каналів для підтримки підконтрольних росії угруповань.

Росія продовжує підтримувати терористичні організації та дестабілізуючі режими в різних регіонах світу. Ця діяльність включає фінансування, постачання зброї та надання політичної підтримки, що сприяє поширенню насильства та підриває міжнародну безпеку.

Для поширення ідей тероризму, дестабілізації та пропаганди, спрямованої на підрив міжнародної безпеки та вплив на різні групи населення, росія активно використовує інтернет. Російські пропагандисти та бот-мережі поширюють повідомлення, що виправдовують тероризм, представляючи його як боротьбу за «справедливість» чи «захист» інтересів окремих груп. Кремль використовує інтернет для дискредитації опонентів, поширюючи фейки про події, зокрема пов’язані з війною в Україні.

1.3. Російсько-українська кібервійна

У 2024 році кібервійна продовжує розвиватися, використовуючи нові технології, інструменти та тактики. Цей фронт конфліктів стає стратегічно важливим для держав, приватного сектору та злочинних груп, впливаючи на національну безпеку, економіку та міжнародні відносини.

Основні тенденції кібервійни у світі:

Ускладнення атак. Кібератаки стають дедалі складнішими та спрямованими на конкретні об’єкти, такі як енергетичні системи, транспорт, медичні установи та фінансовий сектор.

Інформаційна війна. Використання соціальних мереж для поширення дезінформації та маніпуляцій досягає нового рівня завдяки технологіям deepfake.

Гібридні атаки. Кібератаки поєднуються з фізичними диверсіями, наприклад, на енергетичні об’єкти чи транспортні вузли. Крім того, хакери займаються розвідкою, щоб отримати доступ до стратегічної інформації.

Атаки через ланцюги постачання. Зловмисники все частіше проникають у системи через слабкі місця постачальників програмного забезпечення чи обладнання.

Використання штучного інтелекту. Хакери використовують штучний інтелект для автоматизації атак. Уряди та приватний сектор впроваджують штучний інтелект для моніторингу, виявлення та блокування загроз.

Фінансовий сектор як мішень. Атаки на банки, криптобіржі та платіжні системи значно зросли. Програми-вимагачі стають більш прибутковими для хакерів.

Геополітичне протистояння. Конфлікти в кіберпросторі стають невід’ємною частиною глобальної політики.

У 2024 році кібервійна між росії проти України характеризується ескалацією та високотехнологічністю. Україна активно протидіє загрозам, розвиваючи свої кіберспроможності та адаптуючи нові стратегії захисту. Масштаб та складність атак з боку росії залишаються серйозною загрозою для національної безпеки України.

Міністерство юстиції України. У 2024 році Україна зіткнулася з наймасштабнішою кібератакою, яка була спрямована на основні системи Міністерства юстиції України. Унаслідок атаки тимчасово припинили роботу державні реєстри Міністерства юстиції України, що суттєво вплинуло на функціонування критично важливої інфраструктури держави.

Відповідальність за кібератаку взяла на себе російська хакерська група XakNet Team, яка у своєму Telegram-каналі заявила про викрадення та видалення понад 1 мільярда рядків даних, включаючи інформацію, що зберігалася в Польщі. За словами хакерів, вони атакували сервіси ДП «Національні інформаційні системи» (НАІС), після чого отримали доступ до інфраструктури Міністерства юстиції України.

Хакерська група XakNet Team є російським угрупуванням, яке спеціалізується на проведенні масштабних кібератак проти державних установ і критично важливої інфраструктури інших країн.

Служба безпеки України повідомила про ознаки причетності до атаки російських спецслужб, що підкреслює державний масштаб загрози та її стратегічний характер.

Служба безпеки України. У 2024 році Служба безпеки України щодня фіксувала в середньому понад 10 спроб здійснення серйозних кібератак на державні ресурси та критичну інфраструктуру України. З лютого 2022 року відбулося орієнтовно 10 тис кібератак та критичних інцидентів, які зафіксовано Службою безпеки України[1] (кількість нейтралізованих атак за участю Служби безпеки України: 2020 рік – 800 кібератак; 2021 –1400; 2022 рік – 4500; 2023 – 4500[2]).

Абсолютна більшість кібератак в Україні здійснюють російські спецслужби або хакерські угруповання, пов'язані з ними.

Служба безпеки України продовжує активну боротьбу з інформаційними загрозами, зокрема з діяльністю ботоферм, які поширюють проросійську дезінформацію.

Енергетична інфраструктура. Російські хакери атакували енергетичну інфраструктуру України та спричинили перебої в електропостачанні в регіонах.

Банківський сектор. Український банківський сектор також став однією з основних цілей російських кібератак. Хакери спрямовували свої дії на порушення роботи фінансових установ, викрадення коштів та компрометацію клієнтських даних. Російські хакери активно використовували фішингові кампанії, які націлені на співробітників банків та їхніх клієнтів.

Приклад 2024.1.3.1. Діяльності ботоферм, спрямованих на дискредитацію оборонних сил і поширення дезінформації[3]

У вересні 2024 року Служба безпеки України ліквідувала дві ботоферми в Полтавській та Закарпатській областях, які працювали на спецслужби росії.

Організатори цих ботоферм створили тисячі фейкових акаунтів для поширення дезінформації та дискредитації Сил оборони України.

За даними відомства, організаторами ботоферм виявилися двоє місцевих фахівців в ІТ-сфері, які продавали росії нібито зареєстровані в Україні фейкові акаунти.

Через ці акаунти російські спецслужби поширювали дезінформацію про суспільно-політичну ситуацію в Україні нібито від імені українських громадян, а також дискредитували діяльність Сил оборони та ситуацію на фронті.

Так, на Полтавщині місцевий житель на замовлення росії створив майже 15 тис. анонімних акаунтів у різних соцмережах та месенджерах. Продавав

[1] https://speka.media/na-porozi-svitovoyi-kiberviini-yak-sbu-protistoyit-kiberatakam-9erl7l?utm_source=chatgpt.com

[2] https://minfin.com.ua/ua/2024/05/07/126427603/?utm_source=chatgpt.com

[3] https://detector.media/infospace/article/231687/2024-09-03-sbu-likviduvala-dvi-botofermy-yaki-poshyryuvaly-dezinformatsiyu-ta-dyskredytuvaly-syly-oborony/?utm_source=chatgpt.com

фейкові акаунти він через даркнет з розрахунку 1,5 долара за одного віртуального «користувача».

За даними слідства, ботоферма з відповідним обладнанням та сім-картками українських операторів містилася безпосередньо в його квартирі.

На Закарпатті фігурант продавав росіянам унікальні IP-адреси, зареєстровані на території регіону. Це давало російським користувачам змогу видавати в інтернеті себе за українців. Кошти він отримував через російські платіжні системи у вигляді криптовалюти.

CERT-UA

У 2024 році Урядова команда реагування на комп'ютерні надзвичайні події України (CERT-UA) продовжувала активно протидіяти кіберзагрозам, спрямованим на державні установи, критичну інфраструктуру та приватний сектор.

Статистика свідчить про зростання інтенсивності російських кібератак: у першому півріччі 2024 року їх кількість збільшилася на 19% порівняно з другим півріччям 2023-го, досягнувши **1 739 інцидентів**.

Основними цілями залишаються урядові органи, оборонний сектор та критична інфраструктура. Інструментами кібершпигунства є фішинг та інфікування шкідливим програмним забезпеченням.

Приклад 2024.1.3.2. Кібершпигунства щодо українських військових

Угруповання UAC-0184, видаючи себе за інших осіб, звертаються до українських військових у будь-яких застосунках (наприклад, Signal) з повідомленням про те, що він потрапив у якийсь список, виплати, перевід в нову військову частину.

Хакери зазначають в повідомленні все що може зацікавити відкрити надісланий архів на комп'ютері з файлом-ярликом, який надалі інфікує систему та дає хакерам доступ до комп'ютера.

Приклад 2024.1.3.3. Кібершпигунства щодо громадян України

Російські хакери, видаючи себе за інших осіб, звертаються у месенджерах до громадян України для голосування за «хресницю у дитячому конкурсі малюнків» або «підтримати петицію за присвоєння звання «Герой України» загиблому захиснику» (наприклад, WhatsApp та Telegram).

Це робота угруповання UAC-0195. Так російські злочинці крали облікові записи українців, щоб шпигувати та далі розповсюджувати фішингові посилання, щоб залучити більшу кількість жертв.

1.4. Використання новітніх технологій для вчинення злочинів

У сучасному світі технологічні новації активно формують майбутнє, пропонуючи нові можливості в різних сферах життя. Технологія блокчейн зробила значний вплив на багато аспектів нашого життя. Фактично криптовалюти сьогодні сприймають як гроші майбутнього.

Одним із позитивних явищ використанням криптовалют є допомога Україні. З 2022 року стали набирати масштабності пожертвування в криптовалюті. Зібрані активи через десятки благодійних проєктів і аукціонів були направлені на допомогу Збройним силам України та постраждалим від військових дій.

Інновації та технології відкривають багато можливостей в тому числі під час війни. Вони обіцяють швидші, дешевші та безпечніші платіжні рішення.

Публічні блокчейни є прозорими та відстежуваними, але злочинці звертаються до криптовалют для ВК/ФТ, з тих самих причин, з яких люди використовують їх у законних цілях: вони є транскордонними, практично миттєвими та, як правило, з мінімальними комісіями за транзакції.

У звітах FATF відзначається зростаюче зловживання віртуальними активами з боку злочинців для приховування своєї діяльності та швидкого переміщення незаконних доходів через кордони. Більшість юрисдикцій лише частково відповідають або не відповідають зазначеним вимогам FATF (Рекомендація 15).

Технологічні новації мають великий потенціал для розвитку суспільства, але вони також можуть створювати ризики ВК/ФТ (наприклад, торгівля наркотиками, незаконна контрабанда зброї, отримання корупційних доходів, шахрайство, ухилення від сплати податків, кібератаки, ухилення від санкцій, експлуатація дітей та торгівля людьми).

Злочини, пов’язані з кіберзлочинністю та криптовалютою, становлять серйозну загрозу глобальному миру та безпеці, оскільки блокчейн використовуються для крадіжки чи переміщення значних сум, часто в десятки мільярдів доларів щороку.

Розуміння етапів відмивання коштів через криптовалюту є ключовим для ідентифікації ризиків, розробки ефективних інструментів моніторингу та запобігання злочинам.

Відмивання коштів у блокчейн може включати наступні етапи:

Розміщення. На цьому етапі незаконно отримані кошти вводяться в фінансову систему. У випадку з криптовалютами це може включати конвертацію готівки в криптовалюту через криптовалютні біржі або банкомати.

Розшарування. Цей етап передбачає створення складного ланцюга транзакцій для приховування джерела коштів. Злочинці можуть використовувати методи, такі як **Міксери (**сервіси змішують кошти різних користувачів) та **мости між блокчейнами** (переміщення коштів між різними блокчейнами).

Інтеграція. «Відмиті» кошти повертаються в легальну економіку. Наприклад, через інвестиції в бізнес, нерухомість або інші активи.

Держави, які ведуть агресивну політику, використовують криптовалюту, щоб уникнути санкцій (росія, Іран) та для фінансування своїх програм створення зброї масового знищення та балістичних ракет (Північна Корея).

Наприклад, уряд росії легалізував використання криптовалют у зовнішньоекономічних розрахунках для мінімізації впливу фінансових обмежень, запроваджених західними країнами. Це дозволяє російським компаніям і банкам проводити транзакції, уникаючи традиційних систем контролю SWIFT.

Також, російські чиновники та бізнесмени, включно з родичами високопосадовців, використовували криптоактиви для приховування своїх коштів, однак деякі їхні рахунки були заблоковані міжнародними біржами (криптобіржа Binance).

Щомісяця через криптоекосистему проходять мільярди доларів — від незаконних гаманців до конвертаційних сервісів. Відмивання грошей у криптовалюті може бути особливо складним, оскільки кіберзлочинці часто використовують міксери, крос-ланцюгові мости та переходи між гаманцями-посередниками, щоб приховати походження та рух своїх коштів.

Криптовалютні біржі

Криптовалютні біржі є ключовими ланками в системі ПВК/ФТ, оскільки з’єднують криптовалютний та традиційний фінансовий світи. Вони забезпечують точку входу та виходу для транзакцій, що робить їх основними об’єктами для моніторингу підозрілої діяльності.

Завдяки аналізу блокчейну можна виявляти підозрілі адреси сервісів обміну криптовалют, відстежуючи транзакції та виявляючи нелегальні операції. Спеціальні програми допомагають виявляти сервіси, які можуть бути причетними до злочинної діяльності.

Надалі співпраця криптовалютних бірж, підрозділів фінансових розвідок та правоохоронних органів дозволяє блокувати такі адреси та зупиняти незаконні потоки.

Криптовалютні біржі, у свою чергу, збирають важливу інформацію про клієнтів, дотримуючись стандартів KYC/AML, що підвищує прозорість криптовалютних операцій.

<u>Інформація криптобіржі може бути корисною для розслідування злочинів у сфері криптовалют та включати:</u>

особисті дані клієнта

- ім’я, прізвище, дата народження. Базові дані для розслідування дозволяють ідентифікувати особу, яка використовувала біржу;
- адреса проживання;
- контактна інформація (телефон, email);
- копії документів, що посвідчують особу;

дані про транзакції

- історія транзакцій, включно з адресами криптогаманців, сумами, часом і датами. Історія переказів допомагає визначити шлях коштів, їхнє джерело та кінцеву мету. Аналізуючи гаманці, можна виявити мережу пов’язаних адрес або платформ;
- тип криптовалют;
- зв’язок між транзакціями (вхідні та вихідні перекази);

дані про платіжні методи

- інформація про банківські рахунки;
- дані про використані платіжні картки;

додаткові дані

- IP-адреси та геолокація під час входу в акаунт. Дані IP-адрес допомагають визначити місце знаходження підозрюваного;
- логи активності на платформі.

Виявлення криптовалютних активів фігурантів кримінальних проваджень дозволяє накладати на них арешт, але транскордонний характер криптовалют вимагає співпраці між країнами для ефективного розслідування та блокування активів.

Незаконні операції за участю криптобірж

У 2024 році криптовалютні біржі зіткнулися з низкою незаконних операцій та правових викликів по всьому світу. Значні інциденти включають:

Binance. У листопаді 2023 року компанія визнала себе винною у порушенні законів США про відмивання грошей і погодилася сплатити штраф у розмірі 4,3 млрд дол США. Генеральний директор Чанпен Чжао залишив посаду в рамках угоди з владою. У квітні 2024 року Чжао був засуджений до чотирьох місяців ув’язнення за нездатність забезпечити адекватний захист біржі від відмивання коштів.

WazirX. У липні 2024 року індійська криптобіржа WazirX зазнала хакерської атаки, внаслідок якої було викрадено приблизно 234,9 млн дол США. Атака була пов’язана з північнокорейською групою Lazarus.

Gotbit. У серпні 2024 року в Португалії за запитом США був затриманий керівник криптокомпанії Gotbit, яка здійснювала фіктивні угоди на мільйони доларів, отримуючи десятки мільйонів у вигляді виторгу за незаконні операції.

Незаконні операції за участю публічних осіб

У 2024 році з'явилися випадки використання криптовалют для вчинення злочинів за участю політично значущих осіб, що підкреслює зростаючу роль криптовалют у схемах відмивання коштів, фінансуванні тероризму та інших незаконних операціях.

Приклад 2024.1.4.1.1. Використання криптовалют для ФТ

У кількох країнах зафіксовано використання криптовалют для фінансування політичних груп та терористичних організацій. Вищі політичні діячі використовували криптовалюти для обходу міжнародних санкцій, перераховуючи кошти на анонімні криптовалютні адреси.

Приклад 2024.1.4.1.2. Зловживання криптовалютами для відмивання активів політиків

У кількох країнах було викрито схеми відмивання коштів через криптовалюти, в яких брали участь колишні політики. Це дозволяло приховувати нелегальні доходи від бізнесів, пов'язаних з державними контрактами, а потім «переміщувати» ці активи через криптовалютні біржі та платформи для подальшого використання.

Незаконні операції виявлені з використанням технологій блокчейн-аналітики

У 2024 році компанії **Chainalysis** та **TRM Labs** використовують технології блокчейн-аналітики для відстеження підозрілих транзакцій та для протидії фінансовим злочинам, таким як відмивання коштів, фінансування тероризму, кіберзлочини та інші нелегальні діяльності.

Chainalysis та **TRM Labs** у 2024 році виділяють наступні основні схеми:

- фінансування тероризму через криптовалюти;
- шахрайства та інвестиційні схеми. Злочинці створюють фіктивні криптовалютні проєкти або токени, залучають інвесторів та потім зникають з коштами;
- кіберзлочини. Використання криптовалют для отримання викупу від атак програмами-вимагачами. Наприклад, зараження великих корпоративних мереж за допомогою програм-вимагачів, з вимогою викупу у криптовалюті;
- використання криптовалют для відмивання коштів. Злочинці використовують криптовалюти для відмивання коштів через складні ланцюги

транзакцій, включаючи використання міксерів. Вони можуть переміщувати кошти через різні платформи для маскування джерела та призначення коштів;

- мобільні криптовалютні шахрайства. Використання мобільних додатків та чат-ботів для шахрайства з криптовалютами. Злочинці створюють фіктивні криптовалютні платформи, які обіцяють високі прибутки за рахунок інвестицій, а потім збігаються з коштами користувачів. Такі додатки здебільшого використовують соціальні медіа для залучення інвесторів, обіцяючи безризикові інвестиції в криптовалюти;
- торгівля нелегальними товарами через криптовалюти. Торгівля забороненими товарами, такими як наркотики, зброя або інші нелегальні предмети, через криптовалютні платформи, включаючи Dark Web;
- обхід санкцій за допомогою криптовалют.

1.5. Використання дітей для вчинення злочину

Правоохоронні органи встановлюють факти вербування через інтернет підлітків спецслужбами росії для скоєння диверсій. Зокрема, для підпалів автомобілів українських військовослужбовців.

Для вербування українських підлітків окупанти використовують соціальні мережі, підконтрольні інформаційні канали та ігрові інтернет-платформи. Представники спецслужб росії «знайомляться» з дітьми користувачами й пропонують їм співпрацю. Дуже часто для схилення дітей до підривної діяльності ворог застосовує методи шантажу та психологічних маніпуляцій, а також пропонує «легкі» гроші.

Приклад 2024.1.5.1. Залучення неповнолітніх осіб до шпигунства на користь федеральної служби безпеки росії під виглядом квест-гри

Служба безпеки України та Національна поліція викрили нову технологію російських спецслужб, яка полягає у втягненні неповнолітніх українців у злочинну діяльність під виглядом «квест-ігор».

За результатами багатоетапної спецоперації у Харкові правоохоронці затримали дві агентурні групи федеральної служби безпеки росії, які складалися винятково із дітей віком 15 та 16 років. Неповнолітні виконували ворожі завдання із проведення розвідки, коригування ударів та підпалів.

Для маскування підривної діяльності обидва ворожі осередки діяли окремо один від одного.

За «правилами квест-гри» діти отримували від федеральної служби безпеки росії геолокації, після чого їхнім завданням було добратися до точки, зробити фото та відео потрібного об’єкта, а також надати короткий опис місцевості.

Отримані у такий спосіб розвіддані кожна з агентурних груп відправляла своєму спільному куратору з Федеральної служби безпеки росії через анонімні чати.

Надалі окупанти використовували агентурні відомості для здійснення повітряних ударів по Харкову.

Співробітники Служби безпеки України затримали всіх учасників ворожих груп, коли вони фотографували об'єкти української ППО, що захищає місто.

Також під час розслідування було викрито ще одне завдання російських агентів – підпали трансформаторів, які забезпечують рух ешелонів Збройних сил України у напрямку східного фронту.

Слідчі Служби безпеки України вже повідомили організатору однієї з ворожих груп про підозру за ч. 2 ст. 113 КК України (диверсія, вчинена в умовах воєнного стану). Фігурант перебуває під вартою. Йому загрожує довічне ув'язнення.

Також встановлено особу «зв'язкового» агентурних груп федеральної служби безпеки росії. Ним виявився співробітник поліції Краснодарського краю росії, який співпрацює з російською спецслужбою.

Йому готується заочна підозра за ч. 2 ст. 113 КК України (диверсія, вчинена в умовах воєнного стану).

Комплексні заходи проводили співробітники Головного управління внутрішньої безпеки та Департаменту військової контррозвідки СБУ за процесуального керівництва Харківської обласної прокуратури.

Приклад 2024.1.5.2. Вербування підлітків для диверсій

У червні 2024 року поліцейські спільно з СБУ викрили схему російських спецслужб з вербування підлітків для вчинення диверсій. Юнаків віком від 13 до 18 років, яких росія втягнула в злочинну діяльність, затримано. Тепер їм загрожує покарання до 15 років позбавлення волі або довічне ув'язнення.

Приклад 2024.1.5.3. Залучення підлітків до підпалів автомобілів військовослужбовців

На Миколаївщині затримали двох підлітків 16 та 17 років, які, спокусившись на «легкий заробіток» в інтернеті, облили легкозаймистою рідиною та підпалили дві автівки військовослужбовців на Одещині.

Замовник цих підпалів перебуває за кордоном. За рішенням суду хлопцям обрано запобіжний захід у вигляді тримання під вартою.

Також, затримано чотирьох мешканців Дніпропетровщини віком від 17 до 21 року, які підпалили військовий мікроавтобус у Дніпрі. Вони діяли за завданням спецслужб росії, спокусившись на грошову винагороду.

Кримінальна відповідальність. Вказані злочини можуть бути кваліфіковані відповідно до низки статей КК України, за які передбачені суворі покарання – до довічного позбавлення волі, зокрема, за статтями:

- ст. 111 (Державна зрада), карається позбавленням волі на строк до п’ятнадцяти років або довічним позбавленням волі, з конфіскацією майна;
- ст. 113 (Диверсія, вчинена в умовах воєнного стану), карається позбавленням волі на строк п’ятнадцять років або довічним позбавленням волі, з конфіскацією майна;
- ч. 2 ст. 194 (Умисне знищення або пошкодження майна), карається позбавлення волі до десяти років та інші.

Згідно ч. 3 ст. 111 КК України, громадяни України, які на виконання злочинного завдання іноземної держави не вчинили ніяких дій і добровільно повідомили органам державної влади України про свій зв’язок з ними та про отримане завдання, звільняються від кримінальної відповідальності.

Служба безпеки України запустила спеціальний чатбот «Спали ФСБшника» для оперативного збору інформації про спроби вербування російськими спецслужбами.

Чатбот **t.me/spaly_fsb_bot** створено в телеграмі, оскільки цю мережу ворог найчастіше використовує для того, щоб залучити громадян України, а особливо молодь та неповнолітніх, до підпалів авто Збройних сил України, приміщень Територіальних центрів комплектування та соціальної підтримки, мінувань, різного роду диверсій і терактів.

Служба безпеки України закликає повідомляти про спроби вербування через чатбот, гарантуючи конфіденційність та ретельну перевірку кожного звернення.

Кібербулінг. З розвитком месенджерів та соціальних мереж виникло явище кібербулінгу. Слід зазначити, що кібербулінг може використовуватися агентами росії, країни, яка вчиняє збройну агресію проти України, як один з інструментів вербування підлітків для подальшого вчинення дій на користь ворога.

Булінг (англ. bullying - цькування) – цілеспрямоване застосування психологічного, фізичного, економічного або сексуального насильства для завдання шкоди або приниження іншої людини, найчастіше дитини чи підлітка.

У випадку кібербулінгу така деструктивна поведінка реалізується кривдником/кривдницею з використанням засобів електронного зв'язку (інтернет, соціальні мережі, мобільні телефони тощо).

Основні види булінгу:

- систематичні погрози, в тому числі у месенджерах та соціальних мережах (часто анонімні);
- цілеспрямований злам облікових записів жертви для подальшого використання отриманої особистої інформації для шантажу або морального насильства;
- сталкінг (від англ. stalking – переслідування) – небажана нав'язлива увага до людини, що може проявлятися, зокрема, у відстежуванні жертви та її онлайн-активності, погрозах та залякуванні;
- хепі слепінг (від англ. happy slapping – «радісне побиття») – насильницькі дії щодо людини під запис з можливим подальшим розміщенням в інтернеті або поширенням таких записів серед знайомих постраждалої особи;
- розповсюдження принизливої, інтимної або неправдивої інформації або інтернет-контенту про жертву;
- умисне розміщення провокативних повідомлень для розпалювання конфліктів між учасниками онлайн-спільнот;
- грумінг (від англ. grooming – залицяння) – це встановлення дорослими довірливих стосунків з неповнолітніми, в тому числі через інтернет, для подальшого вступу з ними в інтимний зв'язок, вчинення сексуального насильства, шантажування або залякування.

Правоохоронні органи продовжують отримувати чисельні анонімні погрози щодо підриву державних установ, шкіл, лікарень та інших місць масового скупчення людей.

Більшість інформації про псевдо мінування надходила як інтернет-повідомлення з території росії, а також встановлені повідомлення від українських «абонентів». Встановлено, що для «розсилання» терористичних повідомлень російські спецслужби залучають дітей.

Європол повідомляє про організовані злочинні групи, які вербують неповнолітніх

Згідно з дослідженням, проведеним Європолом[4], злочинні мережі все частіше націлюються на молодь у віці від 12 до 17 років, залучаючи їх через соціальні мережі, онлайн-ігри та місцеві спільноти.

Основними причинами є вразливість підлітків, брак соціальної підтримки, фінансові труднощі та пошук визнання.

Залучення молоді стає вигідною тактикою, оскільки неповнолітні не мають кримінальних досьє, що ускладнює їхнє переслідування правоохоронними органами. Крім того, ці особи зазвичай ізольовані від верхніх ешелонів злочинної ієрархії, що зводить до мінімуму їхню обізнаність про структуру і діяльність угруповання. Такий підхід створює буфер між лідерами мережі й виконавцями злочинів, ускладнюючи доведення вини керівників та організаторів.

Особливою загрозою є зростання залучення неповнолітніх у наркоторгівлю, зокрема в сегменті ринку кокаїну. Молоді люди, починаючи з 13 років, можуть виконувати різні ролі: від дилерів і кур'єрів до працівників складів. Також дедалі частіше злочинні угруповання доручають молодим людям завдання, пов'язані з насильством, включаючи вимагання, фізичні напади та навіть вбивства.

Методи вербування неповнолітніх значно еволюціонували. Сучасні злочинні угруповання активно використовують соціальні медіа для пошуку потенційних «співробітників». Соціальні платформи дозволяють їм швидко виявляти молодь, яка потребує емоційної підтримки, відчуває себе ізольованою або шукає приналежності до певної спільноти. Рекрутери часто використовують маніпулятивну мову, що викликає довіру та формує у жертви почуття лояльності та вдячності. У багатьох випадках це дозволяє злочинцям майже безперешкодно залучати молодих людей до виконання кримінальних завдань.

Документ підкреслює, що така діяльність поширена у багатьох європейських країнах і має тенденцію до подальшого розширення.

[4] https://www.europol.europa.eu/cms/sites/default/files/documents/IN_The-recruitment-of-young-perpetrators-for-criminal-networks.pdf

Запобігання залученню неповнолітніх до злочинів та посилення фінансового моніторингу щодо операцій неповнолітніх клієнтів.

Суб'єкти первинного фінансового моніторингу мають приділяти підвищену увагу операціям неповнолітніх клієнтів, які можуть стати мішенню для злочинних угруповань та агресора.

Важливо застосовувати різні індикатори для виявлення підозрілих операцій (підозрілої діяльності). Наприклад, отримання «великих» переказів для неповнолітньої особи, часті транзакції, незвичні витрати або надходження тощо.

Додатково суб'єкти первинного фінансового моніторингу можуть розробляти власні індикатори та скорингові моделі для управління ризиками неповнолітніх клієнтів для ПВК/ФТ та фінансовій експлуатації неповнолітніх осіб.

РОЗДІЛ ІІ. САНКЦІЇ

Після повномасштабного вторгнення росії в Україну 24 лютого 2022 року міжнародна спільнота, зокрема Європейський Союз, США, Сполучене Королівство та інші країни, запровадили жорсткі економічні санкції проти агресора.

Введенні санкції мали на меті послабити економіку агресора, ускладнити його здатність вести війну та змусити владу росії переглянути свою політику. Санкції постійно еволюціонували, та у 2023 та 2024 роках їхній характер став більш жорстким і направленим на різні сектори економіки агресора.

Міжнародна підтримка України, зокрема через санкційний тиск на росію, продовжує залишатися важливим фактором у боротьбі з агресором. Санкції мають практичний вплив на росію та призвели до послаблення економіки агресора та збільшення логістичного шляху проходження товарів.

Дотримання санкційного режиму

Росія активно шукає способи обійти санкції. Представники росії для обходу санкцій використовують міжнародні корупційні зв’язки, посередників із третіх країн та прогалини в обмеженнях.

Запровадження покарання за обхід санкцій здатне значно сприяти дієвості виконання санкцій та відповідно досягнення мети їх застосування.

З метою забезпечення ефективного застосування обмежувальних заходів Європейського Союзу та цілісності внутрішнього ринку ЄС, а також досягнення високого рівня безпеки у сфері свободи, безпеки та правосуддя, Європейський Парламент та Рада Європейського Союзу 24 квітня 2024 року прийняла Директиву № 2024/1226 про виявлення правопорушень, пов’язаних з порушеннями обмежувальних заходів та санкцій ЄС за такі порушення.

Директива зобов’язує країни ЄС запровадити кримінальну відповідальність за порушення санкцій і встановлює мінімальні правила з визначення злочином діянь щодо порушення санкцій і визначення покарання за них. Країни зобов’язані запровадити Директиву до травня 2025 року.

Відповідно до статті 3 Директиви, під порушенням обмежувальних заходів ЄС визначені наступні дії:

1. Надання прямо чи опосередковано коштів або економічних ресурсів призначеній фізичній, чи юридичній особі чи органу або на їх користь, порушуючи заборону, що є обмежувальним заходом ЄС;
2. Не замороження коштів або економічних ресурсів, що належать або контролюються призначеною фізичною або юридичною особою або органом, порушуючи зобов'язання, що є обмежувальним заходом ЄС;

3. Надання дозволу зазначеним фізичним особам в'їжджати або транзитом проходити через територію держави-члена з порушенням заборони, що становить обмежувальний захід ЄС;

4. Вчинення або продовження операцій з третьою країною, органами влади третьої країни або організаціями чи органами, що належать прямо чи опосередковано третій країні або органам влади третьої країни, або контролюються третьою країною або органами влади третьої країни, включаючи укладення або подальше виконання контрактів на державні закупівлі або концесій, якщо такі дії, операції, контракти або їх виконання заборонені або обмежені як обмежувальний захід ЄС;

5. Маркетинг, імпорт, експорт, продаж, купівля, передача, транзит або транспортування товарів, а також надання посередництва, технічної допомоги або інших послуг, пов’язаних з такими товарами, якщо такі дії, операції, контракти або їх виконання заборонені або обмежені як обмежувальний захід ЄС;

6. Надання фінансових послуг або діяльності, якщо такі дії, операції, контракти або їх виконання заборонені або обмежені як обмежувальний захід ЄС;

7. Надання послуг, відмінних від тих, що зазначені в пункті (6), якщо заборона або обмеження такої поведінки є обмежувальним заходом ЄС;

8. Обхід обмежувальних заходів ЄС;

9. Порушення або недотримання умов, викладених у дозволах, виданих компетентними органами на здійснення діяльності, яка, за відсутності такого дозволу, є порушенням заборони або обмеження, що становить обмежувальний захід ЄС.

Норми зазначеної Директиви передбачають відповідальність за порушення обмежувальних заходів ЄС для фізичних та юридичних осіб.

Порушники фізичні особи.

Що стосується штрафних санкцій для фізичних осіб, то залежно від правопорушення держави-члени зобов'язані забезпечити застосування ефективних, пропорційних та стримуючих покарань.

Держави-члени зобов’язані забезпечити, щоб правопорушення, зазначені у статті 3 Директиви, каралися максимальним покаранням у вигляді позбавлення волі.

Порушники юридичні особи.

Серед санкцій, що розповсюджуються на юридичних осіб, згідно з положеннями Директиви, держави-члени вживають кримінальні або некримінальні санкції чи заходи, такі як:

- позбавлення права користуватися державними благами або допомогою;
- позбавлення доступу до державного фінансування, включаючи тендерні процедури, гранти та концесії;

- заборона на ведення підприємницької діяльності;
- відкликання дозволів на провадження діяльності, що призвела до вчинення злочину, а також дозволів на провадження такої діяльності;
- передача під судовий нагляд;
- судова ліквідація;
- закриття закладів, які використовуються для вчинення злочинів;
- якщо в цьому є суспільний інтерес, публікація всього або частини судового рішення, що стосується вчиненого правопорушення та застосованих санкцій або заходів, без шкоди для положень про недоторканність приватного життя та захист персональних даних.

Виявлення схем обходу санкцій можливе лише при здійсненні постійного моніторингу. Наприклад, база даних Comtrade ООН збирає детальну глобальну річну та місячну статистику торгівлі.

База даних Comtrade ООН – це глобальний інформаційний ресурс створений ООН, який надає дані про торгівлю товарами та послугами між країнами. Обсяг даних охоплює торгівельні операції більш ніж у 170 країнах. Доступ можливий через вебінтерфейс або API для автоматизованого доступу.

Росія продовжує переорієнтування на країни Азії, які стали основними транзитними точками для імпорту підсанкційних товарів, зокрема мікрочипів та обладнання подвійного призначення. Основним торговим партнером росії стає Китайська Народна Республіка, зокрема у постачанні автомобілів і високотехнологічних товарів.

Після запровадження міжнародних санкцій росія активно шукає шляхи їх обходу, використовуючи посередництво третіх країн для імпорту підсанкційних товарів. Основними транзитними пунктами стали держави Центральної Азії, Кавказу та Близького Сходу.

Приклад 2024.2.1. Ухилення від санкцій для російських еліт з використанням криптовалют

У листопаді 2024 року Міністерство фінансів США повідомлено про викриття механізму, що використовуються для відмивання коштів через складні корпоративні структури, криптовалютні платформи та транснаціональні схеми. Викриття злочинної схеми є результатом спільних зусиль із Національним агентством із боротьби зі злочинністю Сполученого Королівства (Великобританії), урядом Об'єднаних Арабських Еміратів (ОАЕ), Управлінням боротьби з наркотиками та Мережею боротьби з фінансовими злочинами.

Так, Управлінням контролю за іноземними активами Міністерства фінансів США (OFAC) викрито Компанію (міжнародну незаконну фінансову мережу), яка дозволяє російським елітам обходити американські та міжнародні санкції.

Російські еліти намагалися через Компанію використовувати криптовалюти, зокрема стейблкойни, забезпечені доларами США, щоб уникнути санкцій США та міжнародних санкцій, ще більше збагачуючи себе та Кремль.

Міністерство фінансів США наклало санкції на причетних осіб, які мають зв'язки з російською компанією. До списку потрапили громадяни України, Латвії та росії. Компанія активно працювала в Європі, Азії та Великій Британії, допомагаючи російським елітам купувати нерухомість та приховувати свої активи.

Компанія – це мережа, контрольована громадянином України Джорджес Россі, яка займається ухиленням від санкцій і відмиванням грошей, використовуючи криптовалюти, зокрема стейблкойни Tether (USDT). Її діяльність включає: відмивання коштів для підсанкційних суб'єктів; незареєстрований обмін готівки та криптовалюти; приховування джерел коштів для купівлі нерухомості.

Компанія співпрацює з іншими незаконними суб'єктами, під керівництвом громадян росії. 3 листопада 2023 року OFAC ввів санкції проти групи громадян росії за участь у фінансових операціях на користь російської еліти.

Приклад 2024.2.2. Постачальники російського військово-промислового комплексу замовляють мікросхеми в обхід санкцій

Російські дистриб'ютори інтегрували інформацію з інтернет-магазину американської компанії на свої торгові платформи з метою відображення інформації про запаси напівпровідників та ціни на продукцію. Надалі російські дистриб'ютори опрацьовують замовлення, які виконуються та доставляються через компанії за межами росії.

Протягом січня-серпня 2024 року один із найбільших дистриб'юторів росії опрацював понад 4000 замовлень на сотні тисяч продуктів американської компанії на суму близько 6 млн доларів. Російський дистриб'ютор застосував 40% націнки до цін американської компанії, щоб покрити весь процес постачання та оплати.

Товари американської компанії потрапляють в росію через треті країни, а замовлення можуть бути виконані через дистриб'юторів, перепродаж або старі запаси на складах. Постачаннями переважно займаються компанії, зареєстровані у Гонконгу.

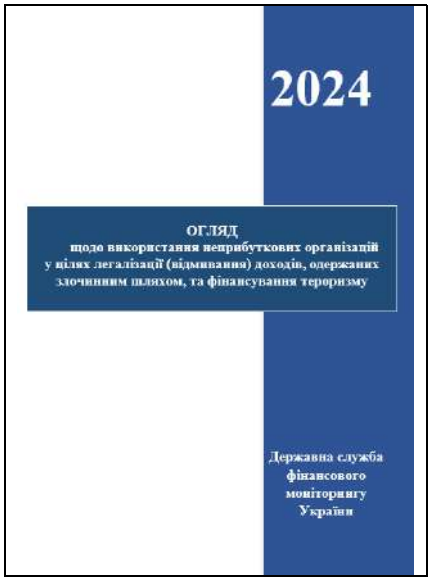
РОЗДІЛ ІІІ. ОГЛЯД АКТУАЛЬНИХ ДОСЛІДЖЕНЬ

Держфінмоніторинг надає методологічну підтримку суб'єктам фінансового моніторингу, зокрема через вивчення, узагальнення та поширення найкращих практик у цій сфері.

Держфінмоніторингом розпочато підготовку щотижневих Методологічних Бюлетенів у сфері ПВК/ФТ/ФРЗМЗ. Бюлетені містять актуальні дані про нові методи та схеми відмивання коштів та фінансування тероризму.

Для регуляторів та правоохоронних органів вказані матеріали стануть важливим інструментом для розробки ефективних стратегій ПВК/ФТ/ФРЗМЗ.

Бюлетені розміщені в рубриці «Методологія» офіційного вебсайту Держфінмоніторингу та будуть доповнюватися щотижнево, забезпечуючи найсвіжішу інформацію та рекомендації у цій критично важливій сфері.



Держфінмоніторингом за результатами проведеного дослідження ризиків використання НПО підготовлено огляд на тему «Використання неприбуткових організацій у цілях легалізації (відмивання) доходів, одержаних злочинним шляхом, та фінансування тероризму».

Дослідження зосереджене на підвищенні обізнаності про ризики використання НПО у незаконних схемах, таких як ВК/ФТ/ФРЗМЗ, а також на розробці заходів для управління цими ризиками.

Огляд розміщено в рубриці «Діяльність/Протидія тероризму/Інформаційні матеріали/Інформація для неприбуткового сектору» офіційного вебсайту Держфінмоніторингу.

3.1. Публікації FATF

FATF постійно стежить за новими методами або методами, що розвиваються, які злочинці використовують для відмивання доходів, отриманих злочинним шляхом, а також за тим, як терористи збирають, використовують і переміщують необхідні їм кошти. Звіти про типології FATF мають на меті підвищити обізнаність органів влади, а також приватного сектору про ризики певних секторів або продуктів, щоб вони могли вжити відповідних заходів для пом'якшення цих ризиків.

Віртуальні активи: Цільове оновлення щодо впровадження стандартів FATF щодо VA та VASP[5]

Цей звіт надає п'яте оновлення щодо дотримання юрисдикціями Рекомендації 15 FATF та Пояснювальної примітки до неї (R.15/INR.15).

Рекомендацію 15 FATF було оновлено у 2019 році для застосування заходів протидії відмиванню коштів та фінансуванню тероризму (ПВК/ФТ) до віртуальних активів (ВА) і постачальників послуг віртуальних активів (ВАСП).

У звіті також міститься інформація про нові ризики та розвиток ринку, пов'язаний з використанням VA для відмивання грошей, фінансування тероризму та фінансування розповсюдження зброї масового знищення.

[5] https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2024.html

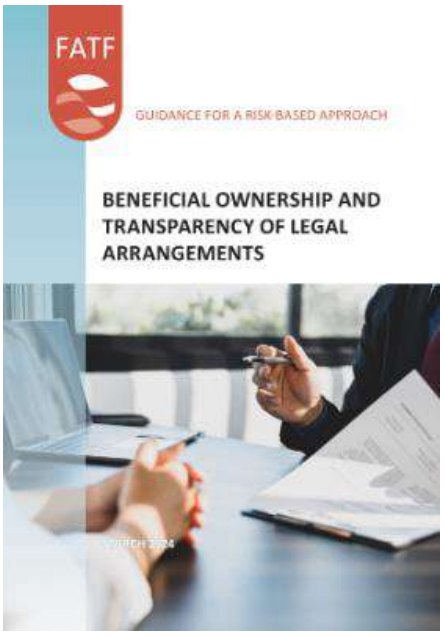
Горизонтальний огляд технічної відповідності гейткіперів у сфері протидії корупції[6]

Горизонтальний огляд технічної відповідності гейткіперів у сфері протидії корупції, опублікований 8 липня 2024 року FATF, аналізує ефективність заходів, які вживають ключові суб'єкти (гейткіпери) для протидії корупційним ризикам.

Основна увага приділяється технічній відповідності міжнародним стандартам, зокрема виконанню рекомендацій FATF щодо належної перевірки клієнтів, виявлення підозрілих транзакцій та співпраці з державними органами.

Документ містить оцінку практик у різних країнах, виявляє типові прогалини в системах фінансового моніторингу та пропонує заходи для їх усунення.

Цей звіт є цінним ресурсом для розуміння ролі приватного сектору, зокрема юридичних, бухгалтерських фірм і фінансових інститутів, у забезпеченні прозорості фінансових операцій і запобіганні корупційним схемам.



Керівництво щодо бенефіціарної власності та прозорості юридичних структур[7]

Керівництво надає рекомендації для покращення прозорості юридичних осіб і механізмів розкриття бенефіціарної власності.

У документі викладено ключові принципи та найкращі практики для забезпечення доступності точних і актуальних даних про бенефіціарів, що є важливим для боротьби з відмиванням грошей, фінансуванням тероризму та іншими злочинами. Окрема увага приділяється ролі державних органів і приватного сектору в ідентифікації та перевірці власників компаній і трастів.

[6] https://www.fatf-gafi.org/en/publications/Fatfgeneral/Gatekeeper-TC-Corruption.html
[7] https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-Beneficial-Ownership-Transparency-Legal-Arrangements.html

Зловживання програмами громадянства та резидентства за інвестиції[8]

Дослідження описує ризики використання програм громадянства та резидентства за інвестиції для уникнення фінансового моніторингу та здійснення незаконної діяльності, зокрема відмивання грошей та фінансування тероризму.

У звіті аналізуються способи, якими недобросовісні особи використовують ці програми для приховування своїх справжніх бенефіціарів або джерел доходів.

Документ містить рекомендації для урядів, спрямовані на вдосконалення процедур належної перевірки, посилення прозорості ідентифікації осіб і впровадження механізмів моніторингу, які унеможливлюють зловживання цими програмами.

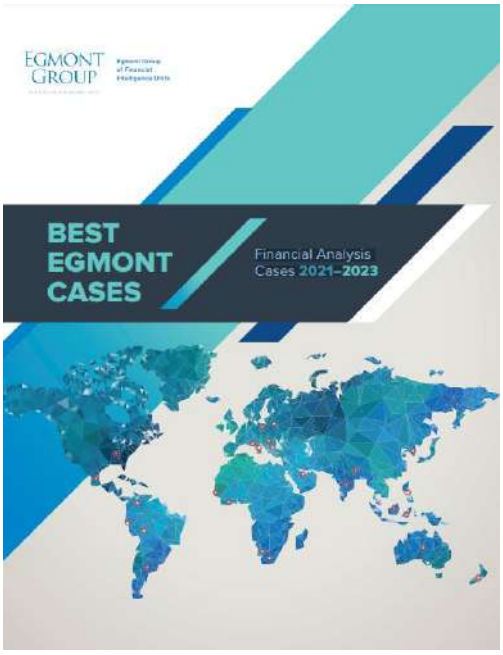
3.2. Публікації Egmont Group

Egmont Group – це міжнародна організація, створена для сприяння співпраці та обміну інформацією між фінансовими розвідувальними підрозділами (Financial Intelligence Units, FIUs) різних країн з метою боротьби з відмиванням грошей (money laundering) та фінансуванням тероризму.

За ініціативи Egmont Group проводиться конкурс BECA (Best Egmont Group Cases Award), який ставить за мету виявлення, аналіз і нагородження найкращих кейсів, що демонструють успішну роботу підрозділів фінансової розвідки (ПФР) у сфері ПВК/ФТ.

[8] https://www.fatf-gafi.org/en/publications/Methodsandtrends/misuse-CBI-RBI-programmes.html

Типологічне дослідження «Ризики та загрози легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансування тероризму в умовах військової агресії російської федерації – 2024»



Найкраща справа Егмонтської Групи

Книга «Найкраща справа Егмонт» пропонує актуальний погляд на еволюцію типологій та предикатних злочинів ВК/ФТ через 24 різноманітні справи з різних юрисдикцій у всьому світі.

Типологія демонструє новаторські підходи та ефективні стратегії фінансового аналізу, що були використані підрозділами фінансової розвідки для ПВК/ФТ.

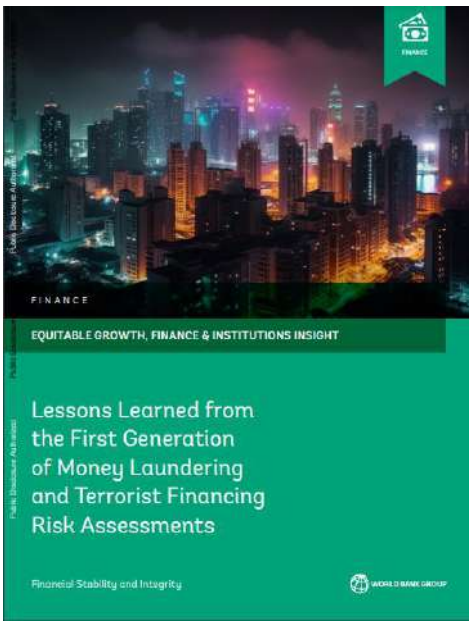
Кейси охоплюють широкий спектр злочинних схем, включаючи використання криптовалют, складних мереж компаній та фінансових посередників.

Цей збірник є життєво важливим ресурсом для спільноти ПВК/ФТ, демонструючи реальні випадки. Кейси охоплюють широкий спектр злочинів, включаючи хабарництво, шахрайство, ухилення від сплати податків, кіберзлочинність, нелегальне використання криптовалют, контрабанду наркотиків, дитячу порнографію, азартні ігри, тероризм і торгівлю людьми.

Ці приклади підкреслюють складність злочинних схем і демонструють інноваційні методи їх розслідування, забезпечуючи важливий інструмент для вдосконалення міжнародної співпраці та ефективності підрозділів фінансової розвідки.

3.3. Публікації Світового банку

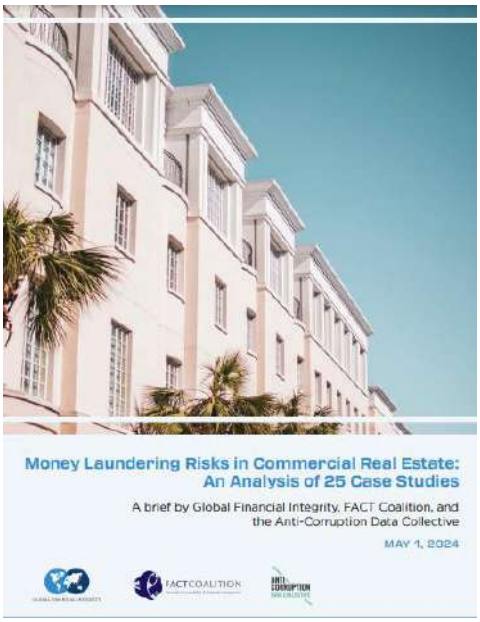
Світовий банк відіграє ключову роль у глобальній економіці як одна з найвпливовіших фінансових установ світу. Світовий банк активно залучений до ПВК/ФТ оскільки відповідно до свого мандату забезпечує сприяння економічній стабільності та розвитку.



У роки, отримані з першого покоління оцінок ризиків відмивання коштів і фінансування тероризму[9]

Документ Світового банку розглядає досвід проведення національних оцінок ризиків у ПВК/ФТ. Документ надає розкриває рекомендації для вдосконалення ризик-орієнтованих підходів у цій сфері.

3.4. Публікації Global Financial Integrity



Ризики відмивання грошей у сфері комерційної нерухомості: аналіз 25 прикладів[10]

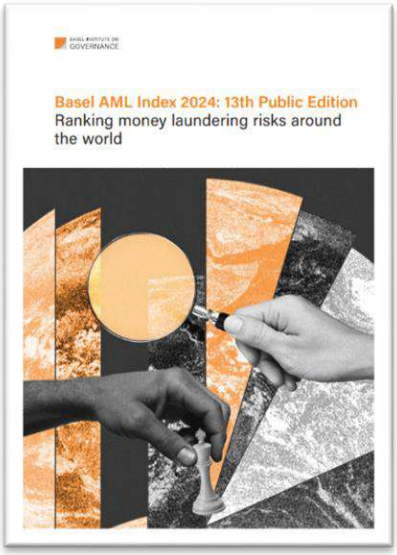
Документ розкриває способи, якими комерційна нерухомість використовується для ВК, і вказує на вразливі місця цього сектора. Зловмисники у сфері нерухомості використовують підставні компанії, заплутані структури власності, штучне завищення чи заниження вартості активів та поєднують законні та нелегальні фінансові потоки.

Брак прозорості щодо кінцевих бенефіціарів і слабкий контроль у багатьох країнах дозволяють використовувати комерційну нерухомість для незаконної діяльності.

[9] https://documents.worldbank.org/pt/publication/documents-reports/documentdetail/099052110042330899/idu0c1b39c8c0bfd604cf608ad40de3e4e0e24b8

[10] https://gfintegrity.org/wp-content/uploads/2024/05/Money-Laundering-Risks-in-Commercial-Real-Estate-FINAL-5-1-2024-1.pdf

3.5. Публікації Basel Institute



Базельський індекс AML 2024. Рейтинг ризиків відмивання коштів[11]

Дослідження є незалежним глобальним інструментом оцінки ризиків ВК/ФТ, опублікованим Інститутом управління в Базелі.

Версія рейтингу аналізує 164 юрисдикції на основі даних із 17 загальнодоступних джерел, таких як FATF, Transparency International, та Глобальна ініціатива проти транснаціональної організованої злочинності.

[11] https://index.baselgovernance.org/api/assets/0789b440-8537-45b4-8bfd-e44ac456c15d.pdf

РОЗДІЛ IV. СПЕЦІАЛЬНА ЧАСТИНА ТИПОЛОГІЇ

Рівень усіх ризиків, які впливають на економічну стабільність та підривають національну безпеку України, внаслідок широкомасштабної збройної агресії росії проти України, залишаються найвищими. Злочинці продовжують шукати слабкі зони у системі фінансового моніторингу та недоліки законодавства для проведення незаконних фінансових операцій.

У контексті широкомасштабної збройної агресії типології ВК/ФТ у цьому дослідженні умовно розподілені за ключовими напрямами, що відображають найактуальніші загрози та ризики для фінансової та національної безпеки:

- ФТ та ВК як частина фінансування війни;
- обхід санкцій;
- корупція в державному секторі та публічних закупівлях;
- незаконне використання НПО та волонтерської діяльності;
- транскордонне ВК;
- незаконне використання готівкових коштів;
- незаконний трафік культурних цінностей;
- шахрайство та кіберзлочини;
- використання віртуальних активів та нелегального грального бізнесу для ВК/ФТ;
- торгівля зброєю, людьми та наркотичними засобами.

Система ПВК/ФТ/ФРЗМЗ в Україні активно вдосконалюється, ефективно виявляючи нові злочинні схеми та способи їх реалізації. Аналіз підозрілих фінансових операцій свідчить про зростання використання злочинцями міжнародних професійних мереж із групами фіктивних суб'єктів господарювання та численними рахунками в різних банках, що суттєво ускладнює їх ідентифікацію СПФМ.

Зберігається практика використання підставних осіб, переважно серед соціально незахищених верств населення. Через складні життєві обставини такі особи часто погоджуються на участь у незаконних схемах, не усвідомлюючи повної відповідальності. Широке застосування дропів — підставних осіб або рахунків — дозволяє злочинцям розшаровувати незаконні доходи, ускладнюючи їхнє відстеження.

У 2024 році використання криптовалют стає одним із ключових трендів у сфері фінансових злочинів. Недостатній розвиток регуляторного середовища криптовалют дозволяє злочинцям проводити анонімні транзакції, приховувати джерела коштів і розшаровувати фінансові потоки, що створює значні виклики у боротьбі з ВК/ФТ.

Викрадені або отримані шахрайським шляхом дані стали поширеним інструментом у схемах ВК/ФТ. Зловмисники використовують персональні дані фізичних осіб або реквізити компаній для відкриття рахунків, проведення фінансових операцій і створення фіктивних суб'єктів господарювання. Це дозволяє приховувати реальних вигодонабувачів і ускладнює ідентифікацію учасників незаконної діяльності.

Юридичні особи дедалі частіше ухиляються від сплати податків використовуючи фізичних осіб-підприємців (ФОПів).

Залучення неповнолітніх осіб до незаконної діяльності тривожна тенденція, яка має серйозні соціальні та правові наслідки. Діти стають об'єктами маніпуляцій через свою вразливість і недосвідченість, виконуючи завдання у злочинних схемах, таких як передача нелегальних товарів чи участь у шахрайських операціях.

Операції з ресурсами, викраденими на тимчасово окупованих територіях, та обходи санкцій створюють серйозні загрози економічній і національній безпеці. Зловмисники використовують незаконно захоплені природні, промислові чи культурні ресурси, переправляючи їх через нелегальні канали на міжнародні ринки. Для уникнення санкцій застосовуються складні схеми, такі як реєстрація компаній у третіх країнах, підробка документів або зміна походження товарів.

Ці виклики потребують посилення фінансового моніторингу, вдосконалення законодавства та розширення міжнародної співпраці.

РОЗДІЛ 4.1. ФІНАНСУВАННЯ ТЕРОРИЗМУ ТА ВІДМИВАННЯ КОШТІВ ЯК ЧАСТИНА ФІНАНСУВАННЯ ВІЙНИ

Агресивна війна, яку веде росія, потребує величезних фінансових ресурсів. Військові дії включають в себе не лише забезпечення армії технікою, озброєнням, боєприпасами, а й утримання особового складу, розвідувальні операції, медичне забезпечення та логістичну підтримку. Окремих видатків потребує пропагандистська діяльність. За першу половину 2024 року федеральний бюджет росії витратив за оборонними статтями рекордні 5,3 трильйона рублів. У порівнянні з першою половиною 2023 року військові витрати росії збільшилися на 36%, або 1,4 трильйона рублів.

Витрати на виплати військовим, зокрема масовий набір «добровольців» і контрактників, якими кремль компенсує фронтові втрати, збільшилися на 25% відносно минулого року і на 175%, якщо порівнювати з 2022-м. Також сильно злетіли витрати на міжнародне військово-технічне співробітництво, до яких може бути включено фінансування закупівель боєприпасів і ракет в Іран і КНДР, це обійшлося бюджету майже в 120 млрд рублів у першому кварталі 2024 року і понад 150 млрд – у другому.

Країна-агресор використовує різні способи для поповнення свого військового бюджету, особливо в умовах міжнародних санкцій, які обмежують доступ до глобальних фінансових ринків, технологій та товарів.

У листопаді 2024 року Бюро Європейського Союзу по боротьбі з шахрайством OLAF розпочало розслідування схем, які дозволяють таким країнам, як Туреччина, експортувати підсанкційну російську нафту до ЄС під іншою маркою. Ця схема вже дозволила москві отримати до 3 мільярдів євро тільки з трьох турецьких портів за цей рік. Така практика, на жаль, демонструє способи росії обійти санкції ЄС та захистити свою торгівлю паливом, що становить майже половину доходів кремля.

Зважаючи на масштаби військової агресії та плани захопити як можна більше території України, росія залучає агентів із проросійською позицією, які є колаборантами, коригувальниками вогню, агітаторами «руського міра», пропагують російські наративи, виправдовують військову агресію та заперечують тимчасову окупацію частини території України.

На тимчасово непідконтрольних територіях підприємці із дозволу загарбників скуповують гривню за рублі, сприяючи «рубльовій зоні». Також поширені схеми збору коштів для бойовиків через афілійовані організації, фейкові благодійні проєкти та соціальні мережі.

Російські спецслужби активно залучають агентів до диверсійної діяльності, зокрема на об’єктах критичної інфраструктури. Для фінансування такої діяльності впроваджуються різноманітні інструменти, в яких, зокрема, використовується проведення великої кількості p2p-переказів з конвертацією криптовалюти у фіат та доходи, отримані від онлайн казино, на карткові рахунки «дропів» з подальшим обготівковуванням.

Узагальнені типові приклади, пов’язані з фінансуванням війни, у т.ч. через ФТ та ВК, наведено нижче.

Приклад. 2024.4.1.1. Залучення неповнолітніх осіб для здійснення підривної діяльності в умовах війни

Держфінмоніторингом з урахуванням інформації правоохоронного органу виявлену схему, спрямовану на фінансування підривної діяльності на території України.

Так, правоохоронним органом встановлено перелік осіб, які підозрюються у здійсненні диверсійних заходів в різних населених пунктах України за вказівками спецслужб рф (вчинити підпал військового автомобіля, закласти вибухівку та ін.), при цьому це переважно **неповнолітні особи** віком від 14 до 18 років, школярі та студенти.

Держфінмоніторингом здійснено аналіз фінансових операцій по карткових рахунках підозрюваних **неповнолітніх осіб**, на які могла надходити винагорода

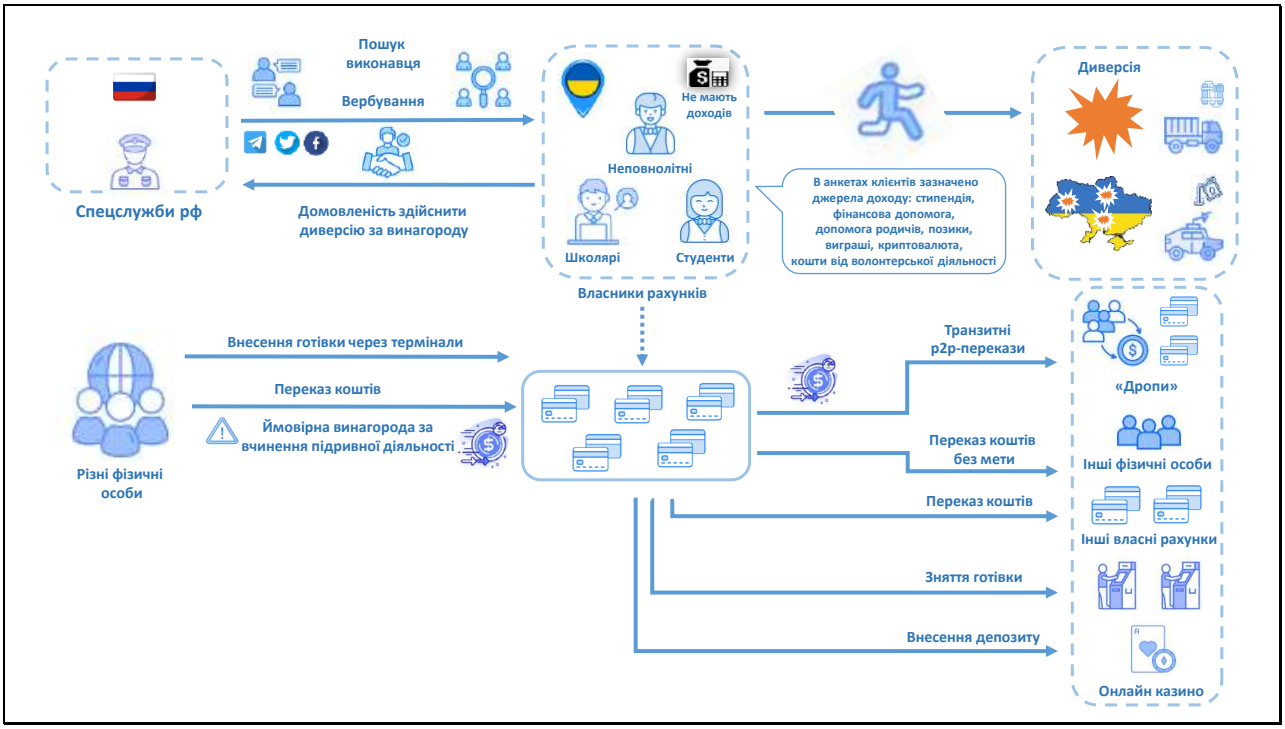
за вчинення підривної діяльності, та виявлено зарахування, у т.ч. в готівковій формі, значної суми коштів від різних фізичних осіб з подальшим їх перерахуванням на інші власні рахунки, на користь інших фізичних осіб, зняттям готівкою та використанням на безготівкові витрати, внесення депозиту на акаунти в онлайн казино, тощо.

При відкритті рахунків **неповнолітні особи** зазначали в анкетах джерела доходів – стипендію, фінансову допомогу, допомогу родичів, позики, виграші, криптовалюту, кошти від волонтерської діяльності, тощо, проте інформації щодо задекларованих ними доходів не виявлено.

У проведених фінансових операціях привертає увагу аномально велика кількість відкритих рахунків **неповнолітніх осіб**, відсутність зазначення мети переказів, перерахування коштів на користь фізичних осіб, що мають ознаки «дропів», здійснення переказів на користь спільних контрагентів. Частині осіб банки відмовили у підтриманні ділових відносин.

Враховуючи природу фінансових операцій, проведених на рахунках **неповнолітніх осіб**, є підстави вважати, що це може бути та сама винагорода за виконану диверсійну роботу на користь спецслужб росії.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2024.4.1.2. Використання активів на тимчасово окупованих територіях за участю українського суб'єкта господарювання

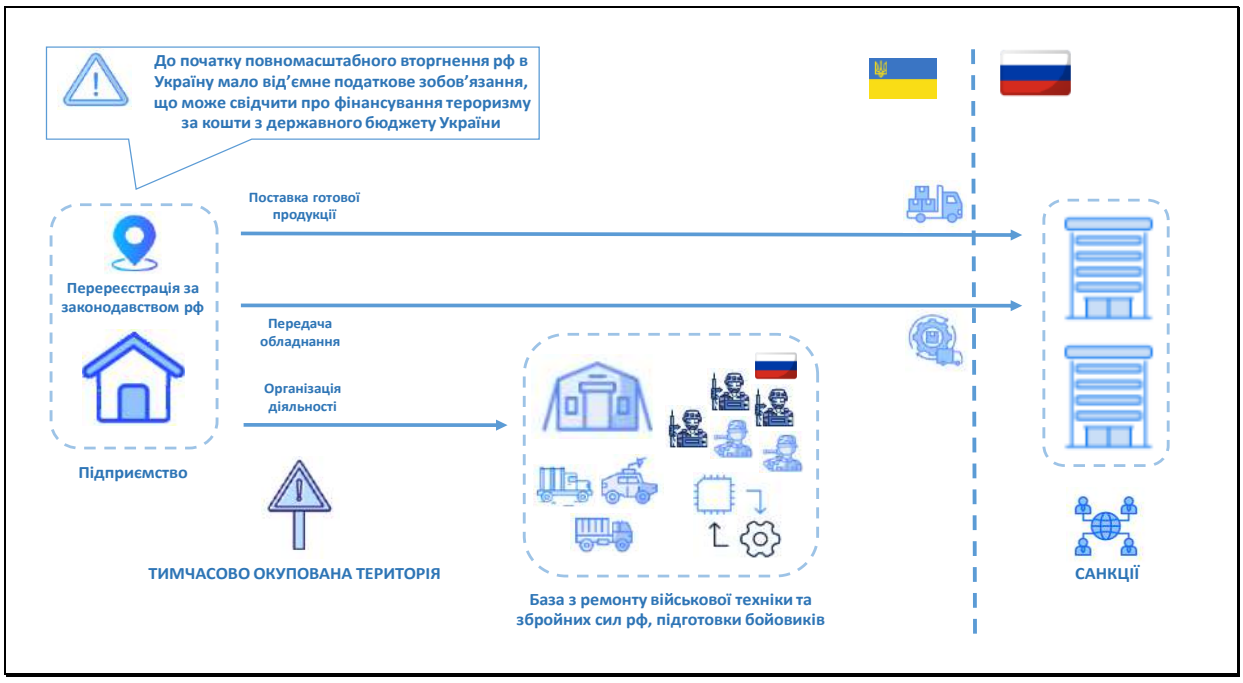
Держфінмоніторингом, з урахуванням інформації ПФР іноземних держав та правоохоронного органу, виявлено схему фінансування військових дій на території України та можливого обходу санкційних обмежень за участю української компанії.

Встановлено, що українське **Підприємство**, яке знаходиться на тимчасово окупованій території, було перереєстровано за законодавством росії, продовжило здійснювати фінансово-господарську діяльність та постачати готову продукцію на територію росії через неконтрольовані ділянки державного кордону України.

Крім того, встановлено, що все обладнання, транспорт українського **Підприємства** було незаконно передано у користування до підсанкційного підприємства російської федерації. На території **Підприємства** організована база з ремонту військової техніки збройних сил росії, а також підготовки бойовиків.

Також встановлено, що до початку повномасштабного вторгнення **Підприємство** мало від'ємне податкове зобов'язання, що може свідчити про фінансування тероризму за кошти з державного бюджету України. Крім того, **Підприємство** виступало відправником товарів на користь іноземних компаній, проте останніми було сплачено значно меншу суму за поставлений товар, а сама діяльність деяких з цих компаній не відповідає природі проведених ними операцій.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2024.4.1.3. Фінансування військової агресії за послуги інтернет-ботів

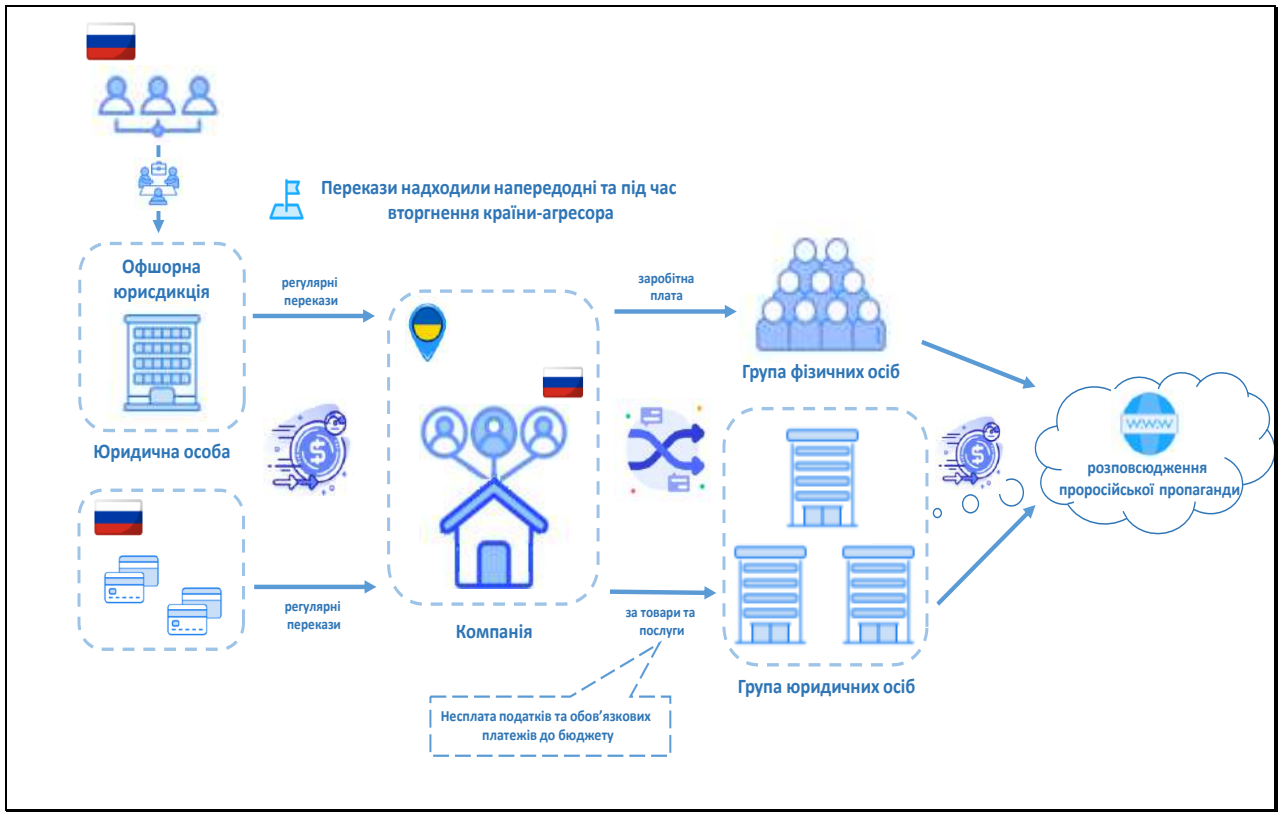
Держфінмоніторингом виявлено схему фінансових операцій за участю іноземних компаній та громадян країни-агресора, спрямованих на фінансування повномасштабного вторгнення росії в Україну.

В ході фінансового розслідування встановлено, що напередодні та під час військової агресії російської федерації проти України здійснювалось регулярне надходження коштів з-за кордону, а саме від **Юридичної особи**, зареєстрованої в офшорній юрисдикції, а також з російських рахунків, на користь української **Компанії**. Відомо, що засновниками іноземної **Юридичної особи** та керівниками української **Компанії** є громадяни росії.

Надалі отримані кошти було перераховано на користь **групи фізичних осіб** під виглядом виплати заробітної плати, та на рахунки **групи юридичних осіб** під виглядом розрахунків за товари та послуги без сплати податків та інших обов'язкових платежів.

Враховуючи, що діяльність української **Компанії** пов'язана з комп'ютерним програмуванням, не виключено, що грошові виплати здійснювались за послуги інтернет-ботів для розповсюдження проросійської пропаганди.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2024.4.1.4. Отримання незаконних доходів за диверсійну діяльність та відмивання незаконних доходів

Держфінмоніторингом, з урахуванням інформації, отриманої від правоохоронних органів, встановлено схему отримання фізичною особою доходів за здійснену диверсійну діяльність.

Встановлено, що після початку повномасштабної агресії проти України на рахунки **Громадянина А** зараховувались значні обсяги коштів, переважно як перекази від фізичних осіб.

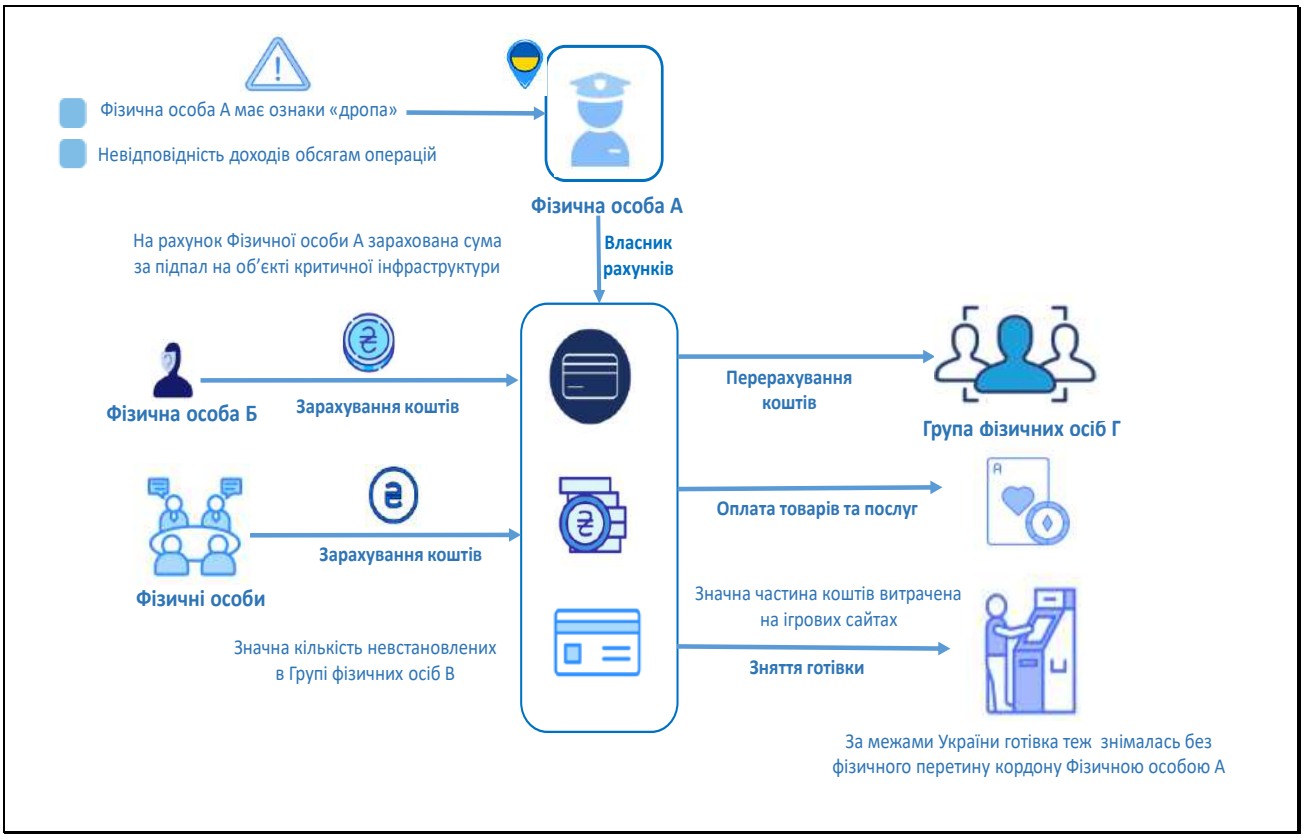
Зокрема, виявлено зарахування коштів на картку **Громадянина А** від **Фізичної особи Б**, які попередньо було зараховано на криптогаманець та конвертовано у фіатні гроші. За інформацією правоохоронного органу зазначена сума була отримана за вчинення підпалу на об'єкті критичної інфраструктури.

Надалі **Громадянин А** використовував кошти для придбання товарів (послуг), зокрема, на ігрових сайтах, переказував на користь **Групи фізичних осіб Г** або знімав готівкою, у тому числі за межами України. При цьому, операції по картковим рахункам в інших країнах були здійснені без фізичного перетину кордону, ймовірно за участі третіх осіб. Крім того, виявлено невідповідність задекларованих/отриманих доходів **Громадянина А** обсягам проведених фінансових операцій.

Враховуючи значну кількість відкритих рахунків, великі обсяги операцій по них, можливість їх використання іншими особами, можливо зробити висновок, що **Громадянин А** має ознаки «дропа»[12]. Таким чином, переважна частина коштів, отриманих **Громадянином А,** не виключено, є незаконно здобутим доходом, одержаним внаслідок здійснення диверсійної діяльності та відмивання незаконних доходів, а також транзитного перенаправлення на користь інших осіб.

Правоохоронним органом здійснюється досудове розслідування.

[12] Дропи – це люди, які за оплату передають реквізити та дані своїх карткових рахунків у користування третім особам. Ці рахунки використовують як «транзитні» для переказу та "відмивання" незаконних коштів.
https://bank.gov.ua/ua/news/all/timchasoviy-limit-na-sumu-perekaziv-z-karti-na-kartu-zapobigatime-vikoristannyu-platijnoyi-infrastrukturi-v-protipravnih-tsilyah-ta-ne-vpline-na-diyalnist-volonteriv



Приклад 2024.4.1.5. Отримання доходів з метою фінансування здійснення фізичними особами диверсійних актів

Держфінмоніторингом, з урахуванням інформації правоохоронного органу, виявлено схему отримання фізичними особами незаконних доходів, які використовуються для здійснення диверсійної діяльності на території України.

Встановлено, що на рахунки **Групи фізичних осіб** – громадян України, які за інформацією правоохоронного органу можуть бути пов'язаними зі здійсненням диверсійної діяльності та її фінансуванням, зараховується велика кількість переказів, отриманих від виграшів в онлайн казино та від операцій з криптовалютами, без зазначення мети таких переказів, які мають транзитний характер.

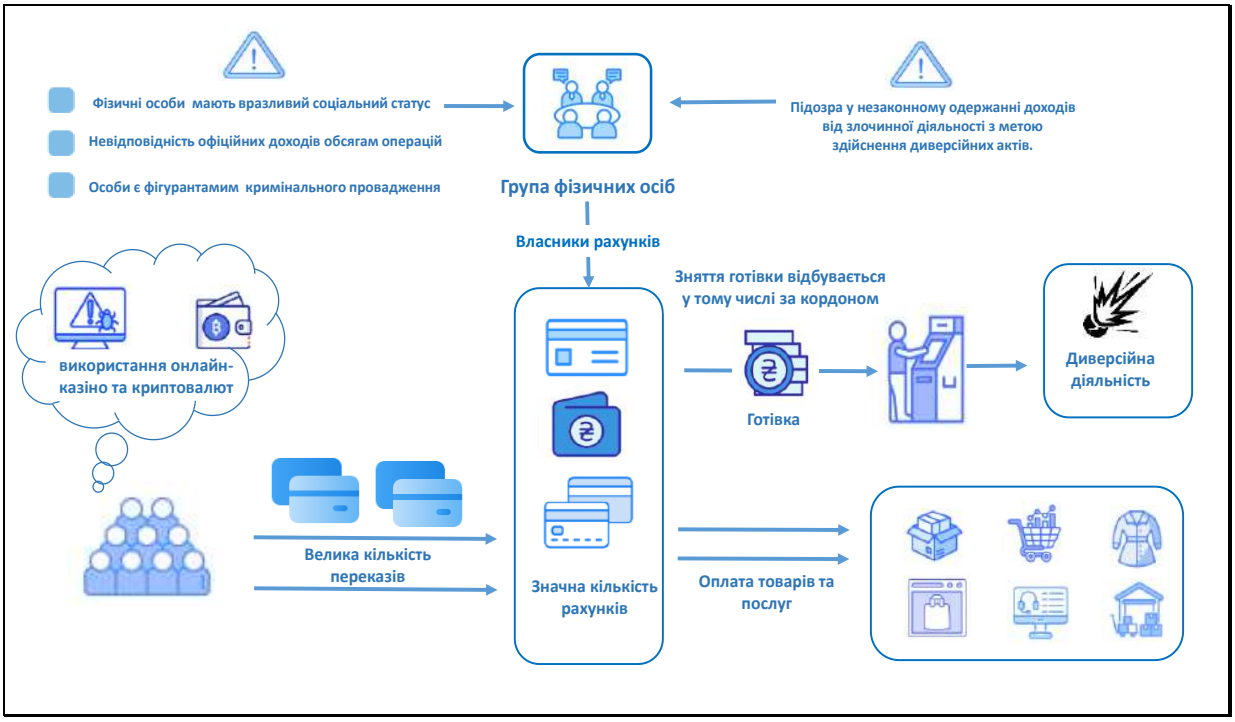
Надалі кошти з рахунків **Групи фізичних осіб** використовуються для придбання товарів (послуг) або знімаються готівкою, у тому числі за межами України. Водночас в державних реєстрах відсутня інформація про перетин ними державного кордону. Також встановлено, що рахунки деяких представників **Групи фізичних осіб** були використані для шахрайського заволодіння коштами інших фізичних осіб та їх подальшою легалізацією.

Крім того, відомо, що представники **Групи фізичних осіб** мають вразливий соціальний статус (молодий вік, безробітні, студенти), інформація про обсяги задекларованих/отриманих доходів відсутня. Більшість з них пов'язана між собою спільними контрагентами та IP-адресами, з яких

здійснювалось підключення до їх банківських рахунків. Діяльність **Групи фізичних осіб** також має ознаки «дропів».

Таким чином, переважна частина доходів, отриманих **Групою фізичних осіб**, не виключено, є незаконно здобутою, одержаною внаслідок злочинної діяльності з метою здійснення диверсійних актів, а також для перенаправлення коштів іншим особам.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2024.4.1.6. Колабораційна діяльність та отримання незаконних доходів від діяльності телеграм-каналу

Держфінмоніторингом виявлено підозрілі фінансові операції **Фізичної особи К**, діяльність якої може бути спрямована на пособництво державі-агресору.

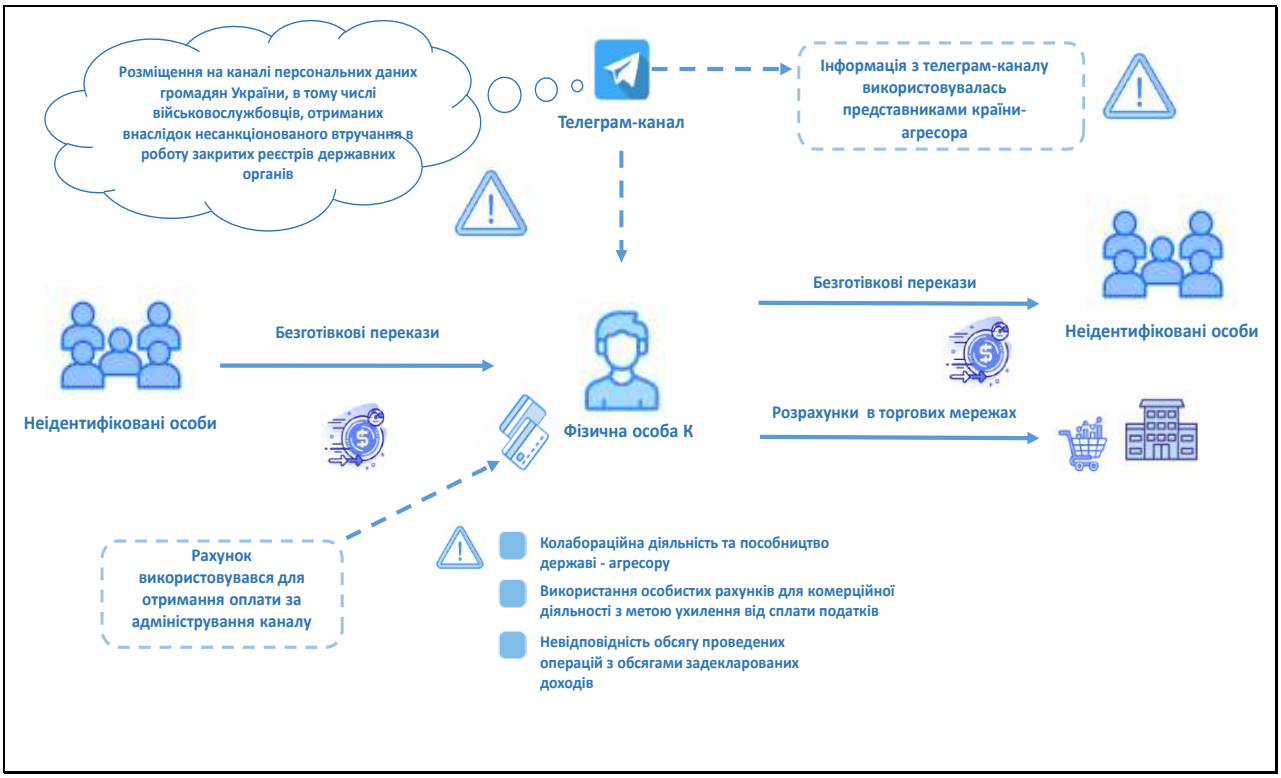
Встановлено, що з початку повномасштабного військового вторгнення в Україні функціонує телеграм-канал, на якому розміщено персональні дані громадян України, в тому числі військовослужбовців, отримані внаслідок несанкціонованого втручання в роботу закритих реєстрів державних органів. Інформація з телеграм-каналу використовувалась представниками країни-агресора.

При цьому виплата грошової винагороди особі, причетній до адміністрування зазначеного телеграм-каналу, здійснювалась на рахунок **Фізичної особи К**.

Встановлено, що на рахунок **Фізичної особи К** від неідентифікованої групи суб'єктів у безготівковій формі зараховано значну кількість переказів. Надалі, зазначені кошти в основному транзитом перераховано іншій групі неідентифікованих осіб та використано як оплату за товари/послуги.

При цьому, обсяг фінансових операцій **Фізичної особи К** значно перевищує обсяг офіційно задекларованих доходів, а особисті рахунки використовуються для здійснення комерційної діяльності. Також наявна інформація щодо ухилення особою від сплати податків. Таким чином, виникають підозри щодо здійснення **Фізичною особою К** фінансових операцій з коштами, одержаними за колаборaційну діяльність та відмивання.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2024.4.1.7. Підтримка фізичною особою держави-агресора

Держфінмоніторингом, з урахуванням інформації, отриманої від ПФР іноземної держави, виявлено фінансові потоки на рахунках фізичної особи, спрямовані на передачу активів росії.

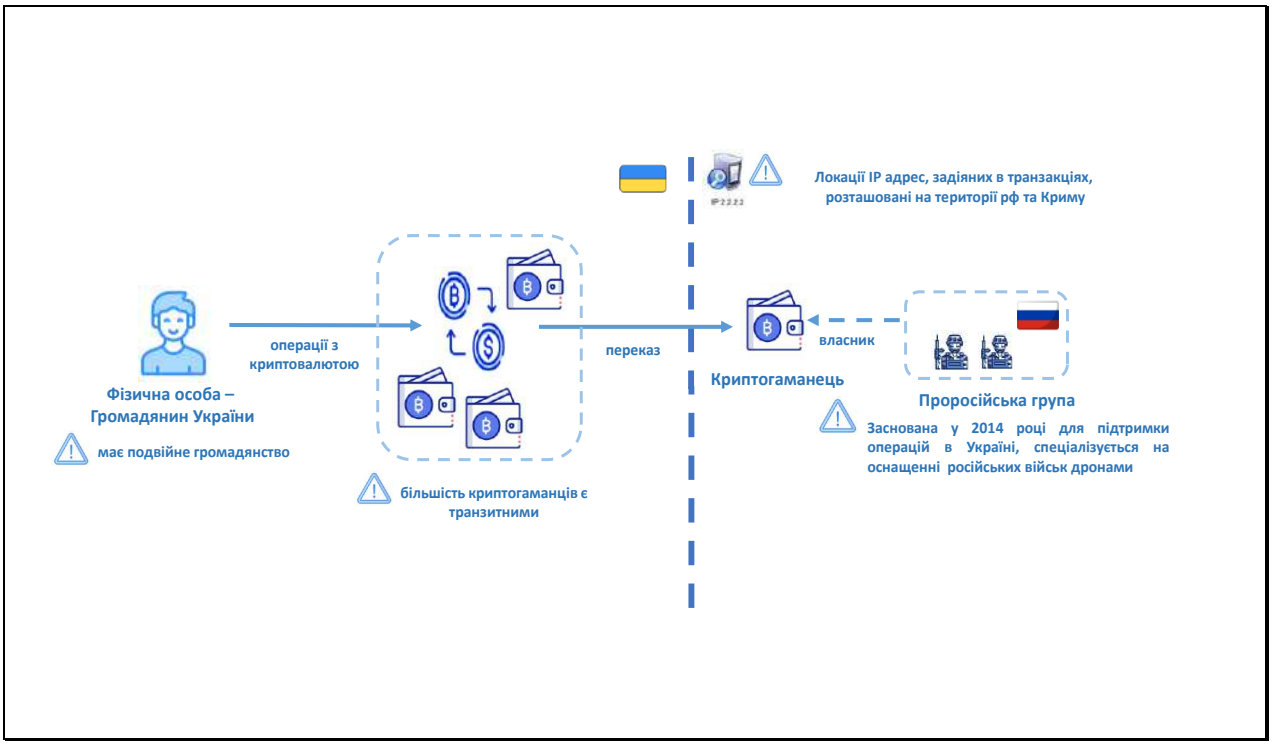
Встановлено, що **Фізичною особою –** громадянином України, який має подвійне громадянство, здійснено операції з придбання BTC та переведення їх на криптогаманці, більшість з яких є транзитними та надалі BTC спрямовуються на криптогаманець, що належить **Проросійській групі**. Локації IP адрес, які були задіяні в транзакціях по зазначеному криптогаманцю розташовані на території росії та в тимчасово окупованому Криму.

Вказана **Проросійська група** була заснована у 2014 році для підтримки операцій в Україні та спеціалізується на оснащенні російських військ дронами. За інформацією ЗМІ більшість надходжень донатів даним угрупованням було зібрано саме в біткойнах.

Враховуючи вищезазначене, існують підстави вважати фінансові операції, пов’язані з переказом **Фізичною особою** біткойнів на користь

Проросійської групи такими, що спрямовані на фінансування збройної агресії росії.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2024.4.1.8. Відмивання доходів, одержаних від співпраці з країною-агресором

Держфінмоніторингом виявлено схему легалізації коштів із невстановлених джерел шляхом придбання та набуття у власність високоліквідних активів.

Встановлено, що **Колишнім посадовцем** внесено готівкою на власний рахунок значну суму коштів. Джерелом походження коштів зазначено подарунок від **Матері посадовця** великого обсягу готівки в іноземній валюті. Проте **Мати посадовця** – літня людина, яка вже давно досягла пенсійного віку та не має відповідних доходів.

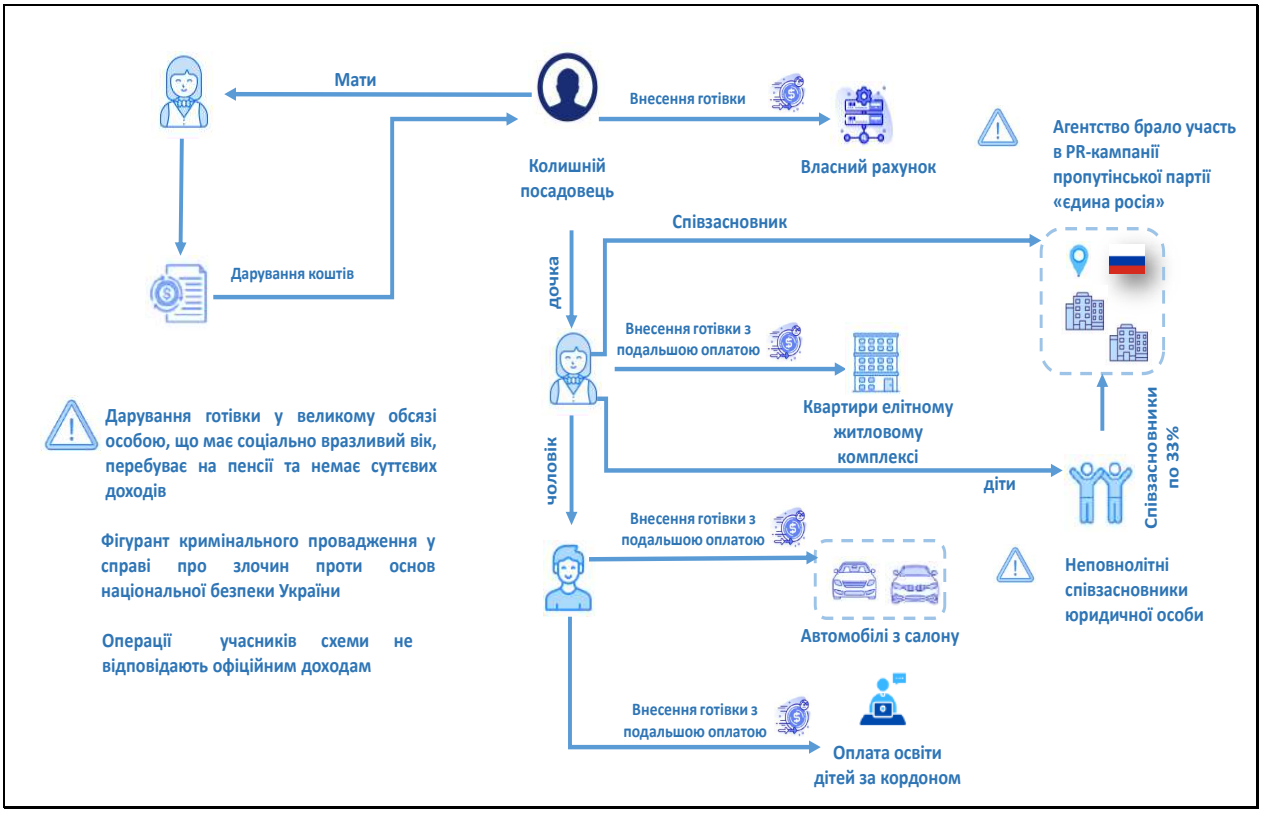
Також, **Дочка посадовця зі своїм чоловіком** вносили значні суми коштів готівкою на власні рахунки та спрямовували їх надалі на придбання квартир в елітному житловому комплексі, дороговартісні автомобілі та оплату навчання дітей за кордоном. Джерелом походження коштів для здійснення таких операцій зазначено власні та родинні заощадження. Водночас витрати на дані покупки значно перевищують їх офіційно задекларовані доходи.

Крім того, **Дочка колишнього посадовця** з **двома неповнолітніми дітьми** є співзасновником двох російських компаній. Компанії – рекламні агентства що брали участь в PR-кампанії пропутінської партії «єдина росія».

Привертає увагу, що **Колишній посадовець** фігурує у справі про злочини проти основ національної безпеки України та внесений до сайту «Миротворець» за пособництво терористам та окупантам, розповсюдження кремлівської пропаганди та участь в гуманітарній агресії.

Таким чином, ймовірно припустити, що джерело походження коштів вказане **Колишнім посадовцем** під виглядом подарунка від матері та використані членами кошти сім'ї на придбання активів, є незаконними доходами, отриманими від співпраці з росією.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2024.4.1.9. Легалізація коштів від незаконної діяльності

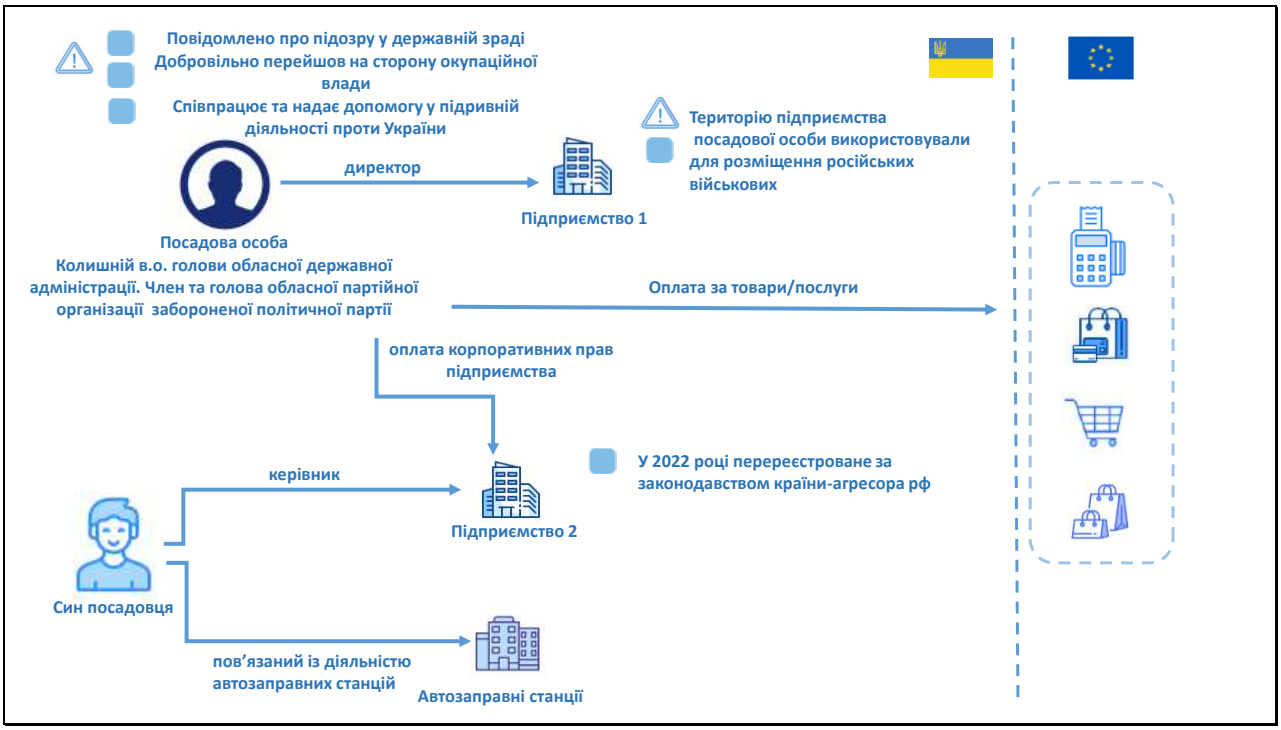
Держфінмоніторингом в ході аналізу встановлено особу, що здійснює колабораційну діяльність на території України.

З початку повномасштабної військової агресії росії, **екс-в.о. Голови ОДА** добровільно перейшов на сторону загарбників, співпрацював та надавав допомогу у підривній діяльності проти України, зокрема розміщував російських військових на території підконтрольної йому установи.

Встановлено, що зараховані на його рахунки кошти невідомого походження надалі списувались для оплати товарів і послуг, у тому числі за кордон та на користь невстановлених осіб. Також кошти перераховувались на оплату корпоративних прав підприємства, що належить **Сину** посадовця. **Син** посадовця є власником ряду підприємств, одне з яких знаходиться на тимчасово окупованих територіях України та перереєстроване за законодавством росії.

Крім того, **Син** посадовця пов'язаний з діяльністю автозаправних станцій. Незаконні доходи отримані від цього бізнесу, розміщеного на тимчасово окупованих росії територіях України, можуть легалізовуватись його батьком на території України.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2024.4.1.10. Створення за участю мігранта організованого злочинного угрупування для підтримки тероризму

В ході досудового розслідування правоохоронним органом встановлено, що **Громадянин** – уродженець північноафриканської країни, який набув українське громадянство, проживає на території України та має в Україні власний бізнес, через власні комерційні структури здійснює зовнішньоекономічну діяльність, спрямовану на постачання товарів та сировини до країни Близького сходу, у тому числі в інтересах міжнародної терористичної організації.

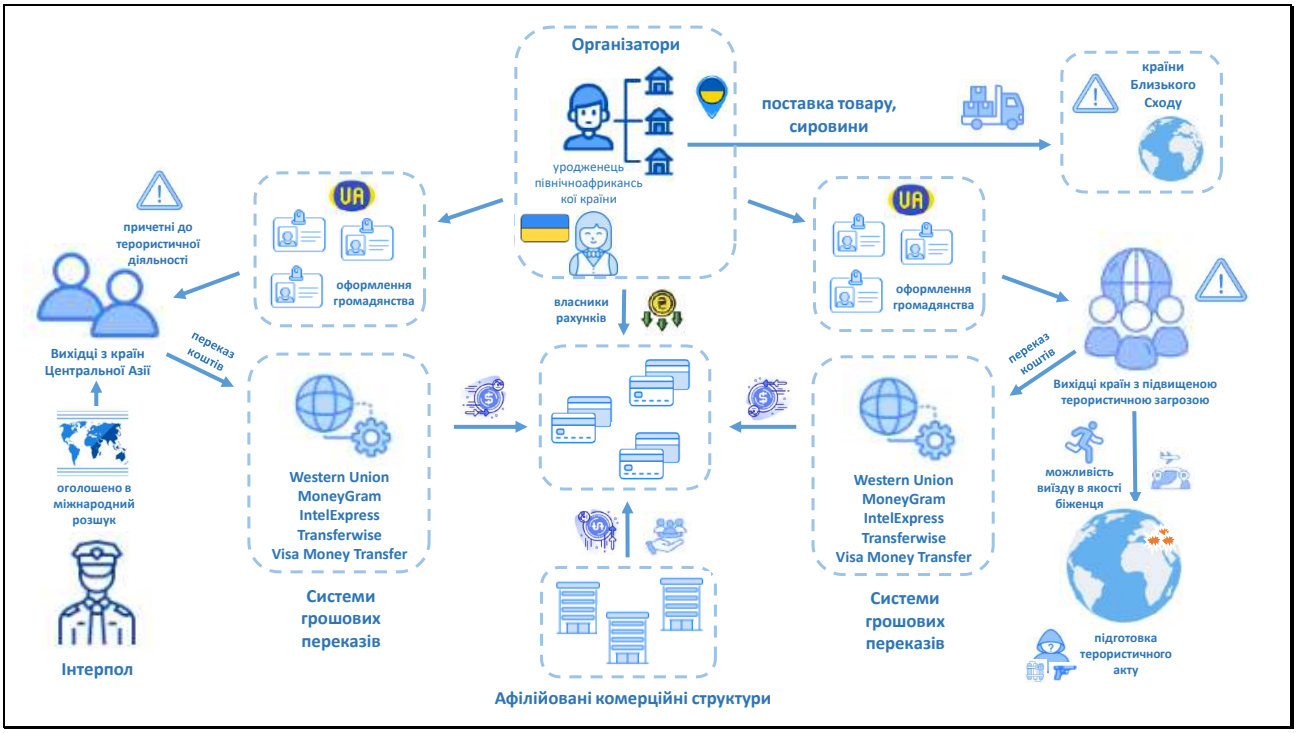
Зазначений **Громадянин** створив організоване злочинне угрупування для здійснення діяльності з легалізації вихідців з країн з підвищеною терористичною загрозою.

У період російсько-української війни членами угрупування здійснено сприяння в оформленні українського громадянства або документів, що дають право легального проживання на території України. Надалі, під виглядом біженців такі особи виїжджали на території країн Європейського Союзу з метою підготовки терористичних актів.

Також ними легалізовано на території України вихідців з центральноазіатської країни, які перебувають у міжнародному розшуку Інтерпол через причетність до терористичної діяльності.

Держфінмоніторингом встановлено, що за вказані послуги члени злочинного угрупування отримували перекази на власні банківські рахунки/платіжні картки з використанням систем грошових переказів Western Union, MoneyGram, IntelExpress, Transferwise, Visa Money Transfer, від більше як двохсот осіб. Також, безпосередньо власники рахунків поповнювали їх готівкою та, крім цього, на рахунок організатора незаконної діяльності надходила благодійна допомога від афілійованих комерційних структур.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2024.4.1.11. Організації незаконної діяльності, спрямованої на переміщення коштів членам терористичної організації

Держфінмоніторингом, з врахуванням інформації, отриманої від правоохоронного органу, проведено дослідження незаконного використання особистих рахунків/карток фізичних осіб з метою сприяння діяльності міжнародних терористичних організацій та подальшої легалізації доходів, отриманих злочинним шляхом.

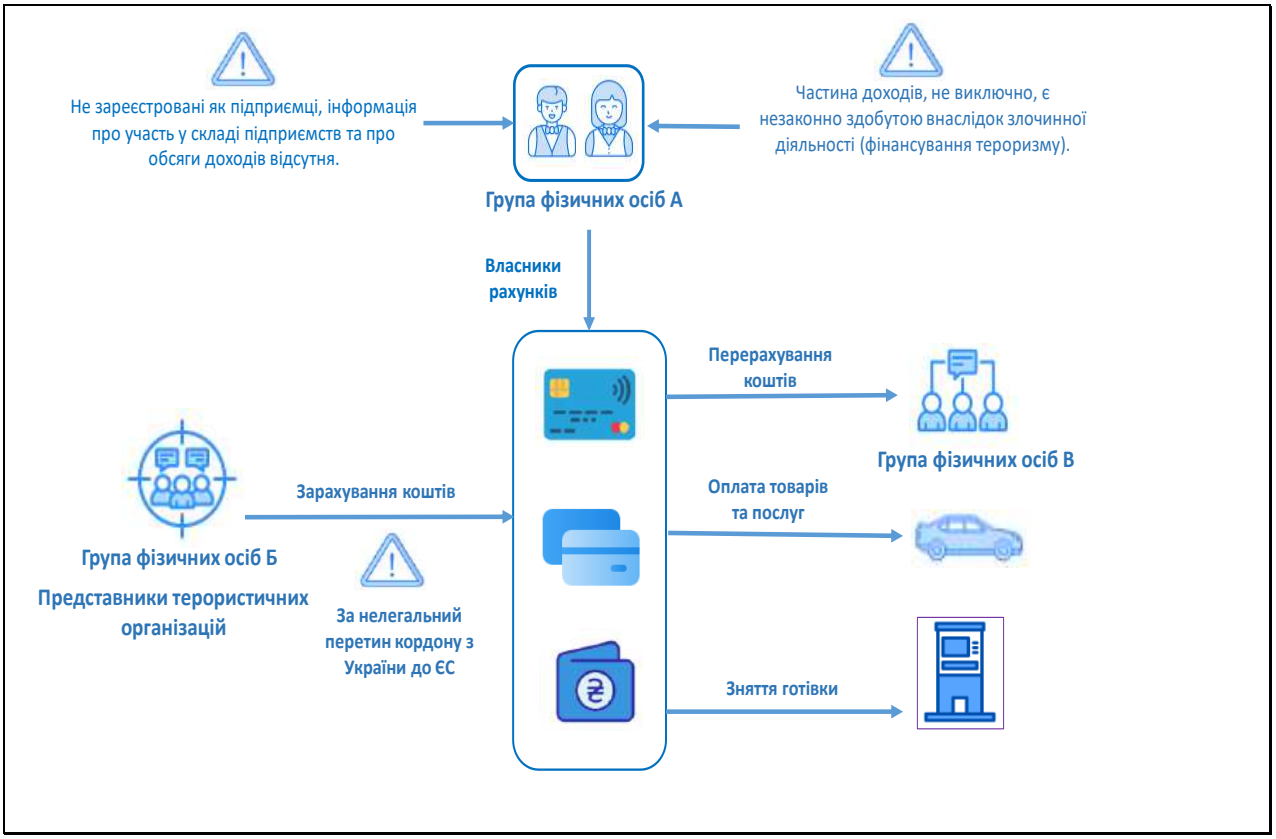
Встановлено, що на рахунки, відкриті в українських банках **Групи фізичних осіб А** зараховано грошові кошти від значної **Групи фізичних осіб Б**, які представляють міжнародні терористичні організації, за нелегальне перетинання державного кордону України до країн Європейського Союзу. Надалі кошти з рахунків **Групи фізичних осіб А** перераховано на користь

Групи фізичних осіб В, використано для придбання товарів (послуг) або знімаються готівкою, у тому числі за межами України.

Крім того, представники **Групи фізичних осіб А** не зареєстровані як підприємці, інформація про їх участь у посадово-засновницькому складі підприємств та про обсяги отриманих доходів відсутня.

Переважна частина отриманих **Групою фізичних осіб А** коштів має транзитний характер та спрямована на фінансування тероризму.

Правоохоронним органом здійснюється досудове розслідування.



РОЗДІЛ 4.2. ОБХІД ФІНАНСОВИХ ОБМЕЖЕНЬ ТА САНКЦІЙ

Санкції – це ефективний інструмент, який використовує світова спільнота з метою позбавлення економічної бази росії для ведення агресивної війни проти України та компенсації наслідків від таких дій. Сьогодні російська федерація є найбільш підсанкціонованою країною світу і наразі саме санкції є найбільш дієвим інструментом впливу на країну-агресора.

Україна також впровадила інститут санкцій. Відповідно до даних Державного реєстру санкцій, під санкціями України перебувають 17 211 осіб: 10 085 фізичних та 7 126 юридичних.

Україна на тлі передачі Північною Кореєю росії балістичних ракет закликала партнерів посилити експортний контроль і санкції, оскільки наразі створюються всі умови для застосування в майбутньому іранської, російської та північнокорейської зброї проти демократичного світу. Крім того, українська сторона передала європейським партнерам списки компаній, які продають свою продукцію до росії попри санкції. Станом на листопад 2024 року Радою ЄС ухвалено 14 пакетів економічних та індивідуальних санкцій у зв'язку з військовою агресією росії проти України.

Російські компанії, перебуваючи в умовах санкцій, змушені здійснювати платежі за контрактами з використанням криптоактивів, що дозволяє обходити обмеження традиційних фінансових систем.

Також, санкційний тиск змушує росію використовувати канали «сірого імпорту», причому не лише для заміщення промислових технологій, але й для постачання простих побутових технологій, виробництво яких відсутнє в країні. Для цього, уряд росії дозволив «паралельний» або «сірий» імпорт окремих видів товарів. Тепер в країну можна буде ввозити товари без дозволу правовласника. Проте, росії важко отримувати сучасне оптичне обладнання, електроніку, чіпи та схеми в необхідних обсягах, а «сірий імпорт» і контрабанда не можуть повністю покрити потреби.

Для обходу санкцій росія залучає так звані «дружні» до агресора країни. При цьому, до зовнішньоекономічних операцій часто залучаються компанії-прокладки з країн Центральної Азії без фактичного відправлення товарів до цих країн.

Таким чином, схеми, які організовує російська сторона або недобросовісні українські громадяни для обходу накладених обмежень і санкцій та можливості отримувати необхідну продукцію і компоненти для ведення агресивної війни проти України, залишаються актуальними.

Узагальнені типові приклади, пов'язані з обходом фінансових обмежень та інших санкцій, наведено нижче.

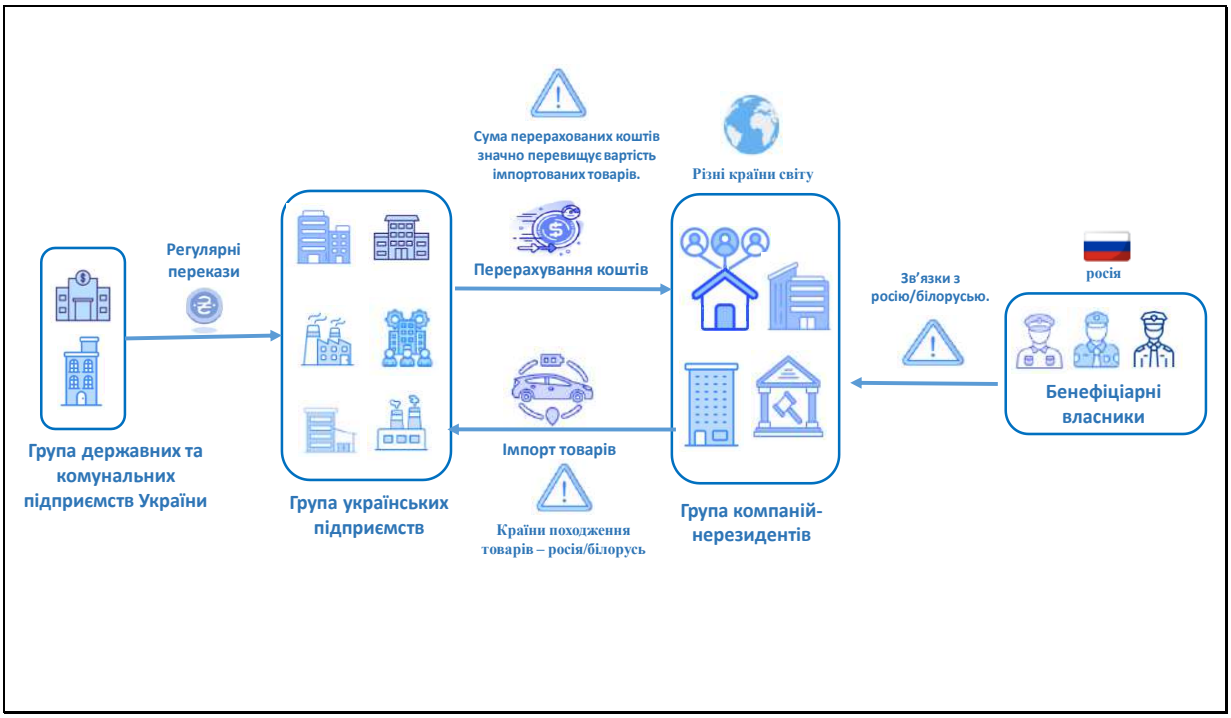
Приклад 2024.4.2.1. Отримання незаконних доходів від співпраці з компаніями-нерезидентами, кінцеві бенефіціарні власники яких пов'язані з росією/білоруссю

Держфінмоніторингом, з врахуванням інформації отриманої від ПФР іноземних держав, проведено дослідження транскордонних операцій українських підприємств з компаніями-нерезидентами, які мають фінансові зв'язки з представниками росії/білорусі, або з яких здійснюється імпорт продукції з місцем походження у зазначених країнах.

Встановлено, що **Групою українських підприємств** отримано кошти від **Групи державних та комунальних підприємств України**. До повномасштабного вторгнення росії в Україну **Група українських підприємств** здійснювала активну діяльність по зовнішньоекономічних імпортних контрактах з російськими/білоруськими компаніями. Після 24.02.2022, з метою уникнення порушень діючого законодавства України, зазначена **Група українських підприємств** почала здійснювати транзитні перекази коштів по контрактах на користь **Групи компаній-нерезидентів**, зареєстрованих у різних країнах, при цьому у переважній більшості випадків **Бенефіціарні власники** зазначених нерезидентів мають зв'язки з росією/білоруссю. Також було здійснено митне оформлення імпортних товарів від **Групи компаній-нерезидентів**, реальним місцем походження яких є зазначені країни, при цьому сума перерахованих за кордон коштів значно перевищила вартість отриманих товарів.

Таким чином, значна частина доходів, отриманих **Групою українських підприємств**, не виключено отримані шляхом обходу запроваджених обмежень шляхом використання компаній-нерезидентів, кінцеві бенефіціарні власники яких пов'язані з росією/білоруссю. Крім того, з рахунків **Групи українських підприємств** виведено кошти без фактичного постачання товарів на їх користь.

Держфінмоніторингом здійснено передачу матеріалів зазначеного дослідження до правоохоронних органів.



Приклад 2024.4.2.2. Обхід санкцій шляхом переміщення матеріальних активів підсанкційним особам з використанням фізичних осіб

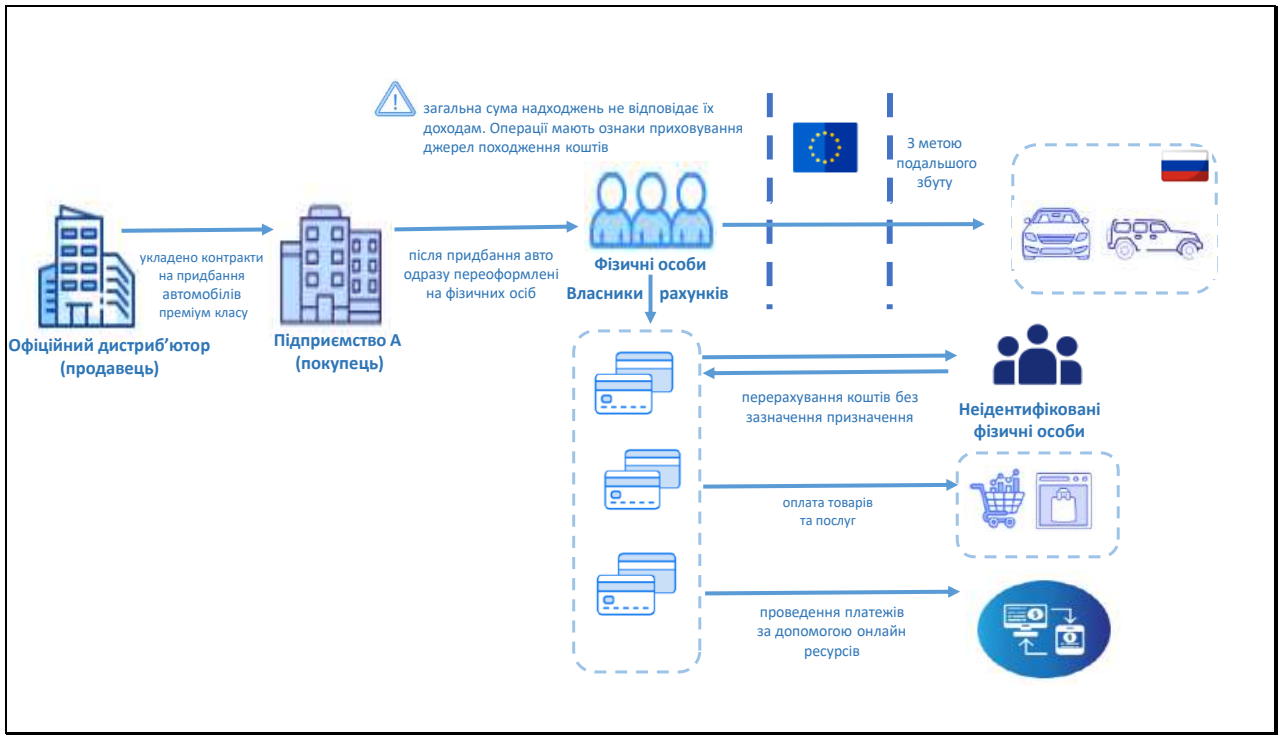
Держфінмоніторингом, з врахуванням інформації, отриманої від правоохоронного органу, виявлено схему протиправної передачі матеріальних ресурсів на користь представників країни-агресора всупереч запровадженим санкціям.

Встановлено, що **Підприємством А** було здійснено придбання автомобілів преміумкласу у офіційного дистриб'ютора, які після надходження були одразу переоформлені на підставних **Фізичних осіб** та переміщені з території України до російської федерації через країни ЄС та СНД з метою подальшого збуту.

Також, встановлено, що на рахунки **Фізичних осіб** зараховано готівкові та безготівкові кошти від великої кількості інших фізичних осіб та надалі перераховано на користь інших фізичних осіб без зазначення призначення платежів, які використано для придбання товарів та послуг, проведення платежів за допомогою онлайн ресурсів.

При цьому, загальні суми надходжень на рахунки **Фізичних осіб** не відповідають їх фінансовому профілю та, не виключено, є незаконно здобутими доходами, одержаними внаслідок протиправної діяльності.

Правоохоронним органом здійснюється досудове розслідування.



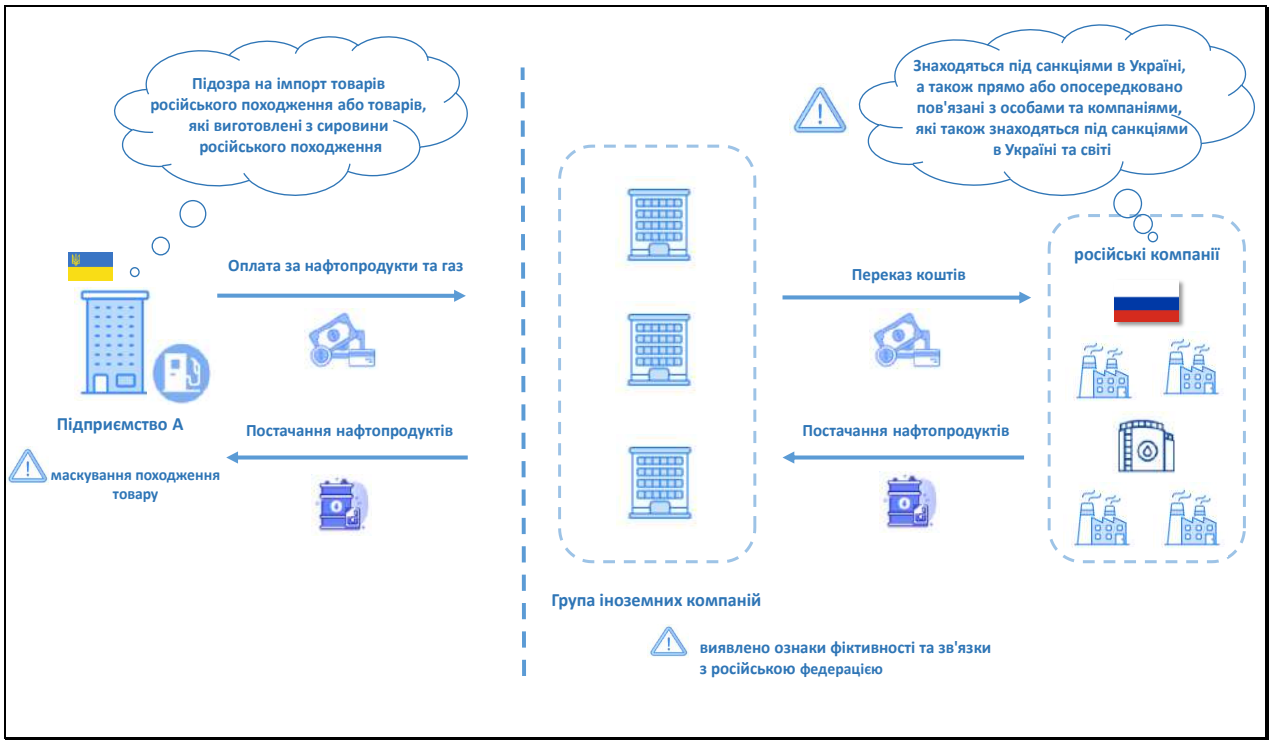
Приклад 2024.4.2.3. Використання транзитних компаній для обходу запроваджених санкцій

Держфінмоніторингом, з урахуванням інформації правоохоронного органу та ПФР іноземної держави, виявлено схему постачання продукції російського походження на територію України в обхід вітчизняних санкцій та національних заборон щодо розрахунків з російською федерацією.

Встановлено, що **Підприємство А** здійснювало оплату за нафтопродукти та газ на користь **Групи іноземних компаній**. В свою чергу, іноземні компанії отримували вищезазначені товари від російських компаній, які знаходяться під санкціями в Україні, а також прямо або опосередковано пов'язані з особами та компаніями, які також знаходяться під санкціями в Україні та світі.

Встановлено, що деякі іноземні компанії, які залучені до схеми, мають ознаки фіктивності та зв'язки з російською федерацією.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2024.4.2.4. Обхід санкцій з використанням резидентів іноземних юрисдикцій та пов'язаних осіб

Держфінмоніторинг, з урахуванням даних правоохоронних органів та ПФР іноземних держав, виявив схему незаконної зовнішньоекономічної діяльності, спрямованої на підтримку держави-агресора під час повномасштабного вторгнення росії в Україну.

Встановлено, що **громадянин України**, зареєстрований на тимчасово окупованій території АР Крим, здійснював контроль за рядом **українських підприємств**, що здійснюють діяльність в авіаційній сфері та надають послуги з перевезення пасажирів, вантажу повітряним транспортом.

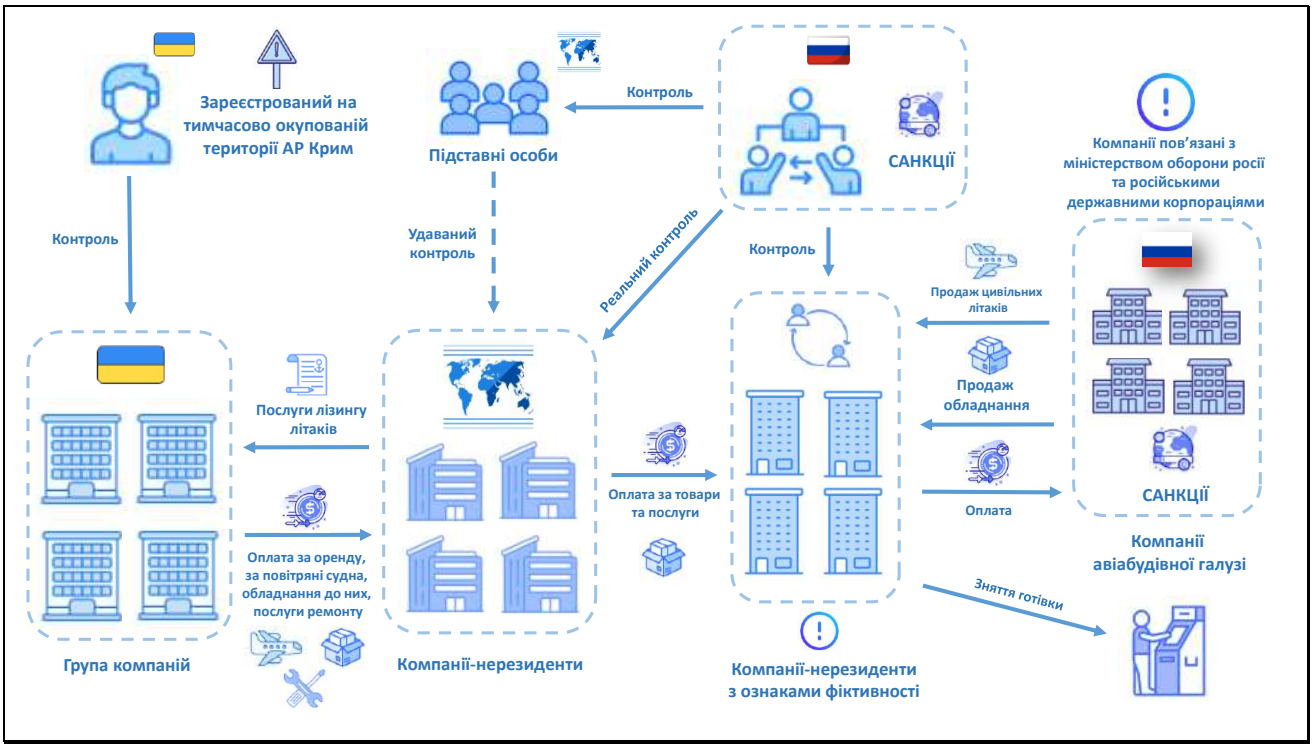
З метою обходу санкцій та заборони на співпрацю з російськими компаніями, **українські підприємства**, підконтрольні **громадянину України**, уклали договори лізингу повітряних суден з рядом **компаній-нерезидентів**, створених у вільній економічній зоні однієї з країн Західної Азії, які надалі здійснювали купівлю літаків цивільної авіації російського виробництва, обладнання до них та надавали їх в оренду **українським підприємствам**. При цьому, більшість цих компаній-нерезидентів є пов'язаними між собою через засновників, керівників, фінансові операції, контрагентів, та мають зв'язок з громадянами росії, в тому числі підсанкційними, напряму та через підставних осіб.

Встановлено, що літаки російського виробництва закуповувались у підсанкційних російських компаній авіабудівної галузі, пов'язаних з міністерством оборони росії та російськими державними корпораціями, через

ланцюг інших компаній-нерезидентів, що мають ознаки фіктивності та підконтрольні громадянам росії.

На виконання договорів лізингу **українськими підприємствами**, підконтрольними **громадянину України**, було перераховано кошти у значних обсягах на користь **компаній-нерезидентів**. Оплата здійснювалась за оренду та придбання повітряних суден, обладнання до них та послуги ремонту. Надалі ці кошти було перераховано по ланцюгу іншим пов'язаним з громадянами росії **іноземним компаніям** у вигляді оплати за товари та послуги, та частково знято готівкою.

Правоохоронним органом здійснюється досудове розслідування.



РОЗДІЛ 4.3. КОРУПЦІЙНІ ЗЛОЧИНИ ТА СХЕМИ ВІДМИВАННЯ ЗЛОЧИННИХ ДОХОДІВ

Корупція залишається однією з найбільших загроз для України, особливо під час воєнного стану. Її прояви підривають нашу обороноздатність, послаблюють державні інституції, зменшують ефективність міжнародної допомоги й руйнують віру суспільства у справедливість і прозорість влади.

Корупція як соціальне явище завжди викликає підвищену увагу громадськості, особливо в умовах воєнного стану. Будь-які корупційні дії під час воєнного стану, що відволікають ресурси з оборони та безпеки або ставлять під загрозу національні інтереси, насправді сприяють послабленню держави та ускладнюють її здатність протистояти агресору.

Актуальними залишаються схеми, пов’язані з корупційними злочинами (розкрадання бюджетних коштів, зловживання владою та службовим становищем, хабарництво). Війна завжди створює додаткові можливості для незаконного збагачення, зокрема, через значні фінансові потоки та екстрені закупівлі. Це явище спостерігалося протягом всієї історії воєн, незалежно від країни.

Узагальнені типові приклади відмивання злочинних доходів, отриманих від корупції, наведено нижче.

Приклад 2024.4.3.1. Незаконне привласнення бюджетних коштів через фіктивні підприємства та підроблені документи

Держфінмоніторингом, виявлено фінансові потоки, пов’язані із незаконним заволодінням бюджетними коштами та їх подальшою частковою легалізацією шляхом переказу за кордон.

Під час фінансового дослідження встановлено, що **Бюджетною установою** перераховано кошти на рахунок **ФОП** за товар військового призначення, який він мав придбати у **Підприємства** та поставити його до **Бюджетної установи**. Проте зазначений товар так і не був поставлений, що свідчить про можливі зловживання.

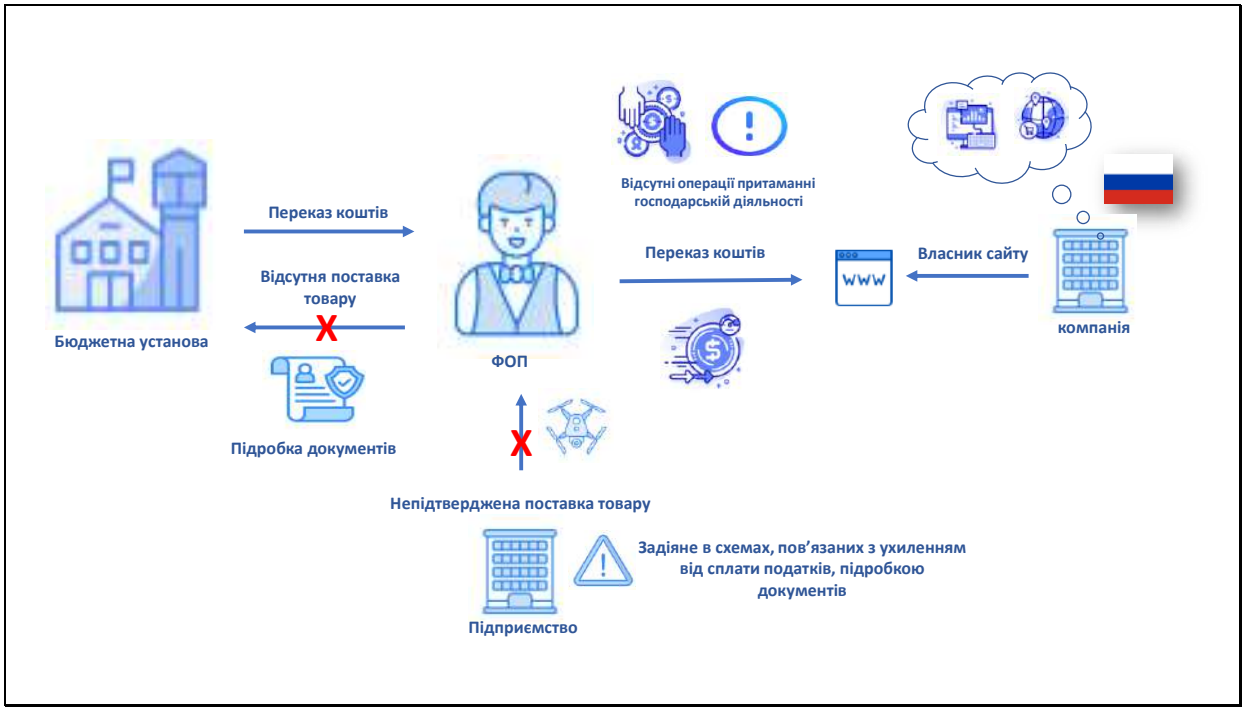
Водночас, документи на придбання та фактичне отримання товару містили ознаки підробки: договір та видаткова накладна оформлені раніше дати реєстрації **ФОП**, в договорі вказано номер рахунку **ФОП**, який фактично відкрито пізніше дати укладання договору. Крім того, відсутні фінансові операції **ФОП**, пов’язані із розрахунками з **Підприємством** за товар військового призначення.

Підприємство раніше брало участь у схемах, пов’язаних з ухиленням від спати податків, підробкою документів, які подаються для проведення державної реєстрації, та легалізацією доходів, одержаних злочинним шляхом.

Вивченням фінансових потоків встановлено, що по рахунку відсутні платежі, притаманні звичайній господарській діяльності.

В свою чергу, отримані кошти **ФОП** від **Бюджетної установи** було перераховано за кордон на користь отримувача, пов'язаного з країною-агресором росією. Товар військового призначення до **Бюджетної установи** не поставлено.

Правоохоронним органом здійснюється досудове розслідування.



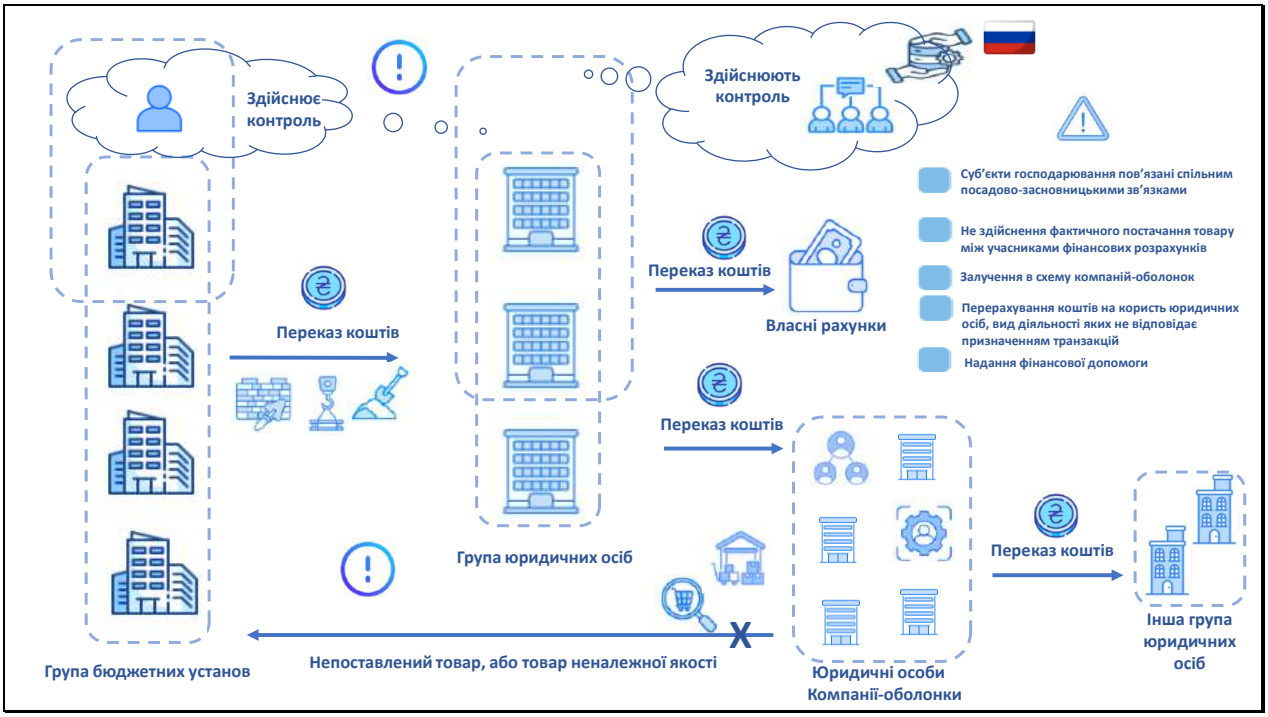
Приклад 2024.4.3.2. Використання мережі з незаконних послуг для привласнення та нецільове використання бюджетних коштів

Держфінмоніторингом, з урахуванням інформації, отриманої від правоохоронного органу, виявлено фінансові операції, пов'язані із привласненням бюджетних коштів та ВК.

Встановлено, що **Групою бюджетних установ** перераховано грошові кошти на користь **Групи юридичних осіб** як оплату за товарно-матеріальні цінності. Деякі з цих **юридичних осіб** підконтрольні фізичним особам, пов'язаним із забороненою в Україні політичною партією, з представниками росії та з посадовою особою бюджетної установи.

Надалі **Групою юридичних осіб** було здійснено перерахування частини отриманих бюджетних коштів на інші власні рахунки та на користь **Юридичних осіб**, які пов'язані спільними посадово-засновницькими зв'язками та мають ознаки компаній-оболонок. Товари, за які перераховано бюджетні кошти, поставлялися неналежної якості, або взагалі не надходили до кінцевого споживача. Також, **Юридичними особами** перераховано отримані кошти на користь **Іншої групи юридичних осіб**, діяльність яких не відповідала призначенню транзакцій і яка здійснювала транзитну діяльність.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2024.4.3.3. Привласнення коштів комунального підприємства та їх легалізація через псевдоінвестування, фінансову допомогу та конвертацію в готівку

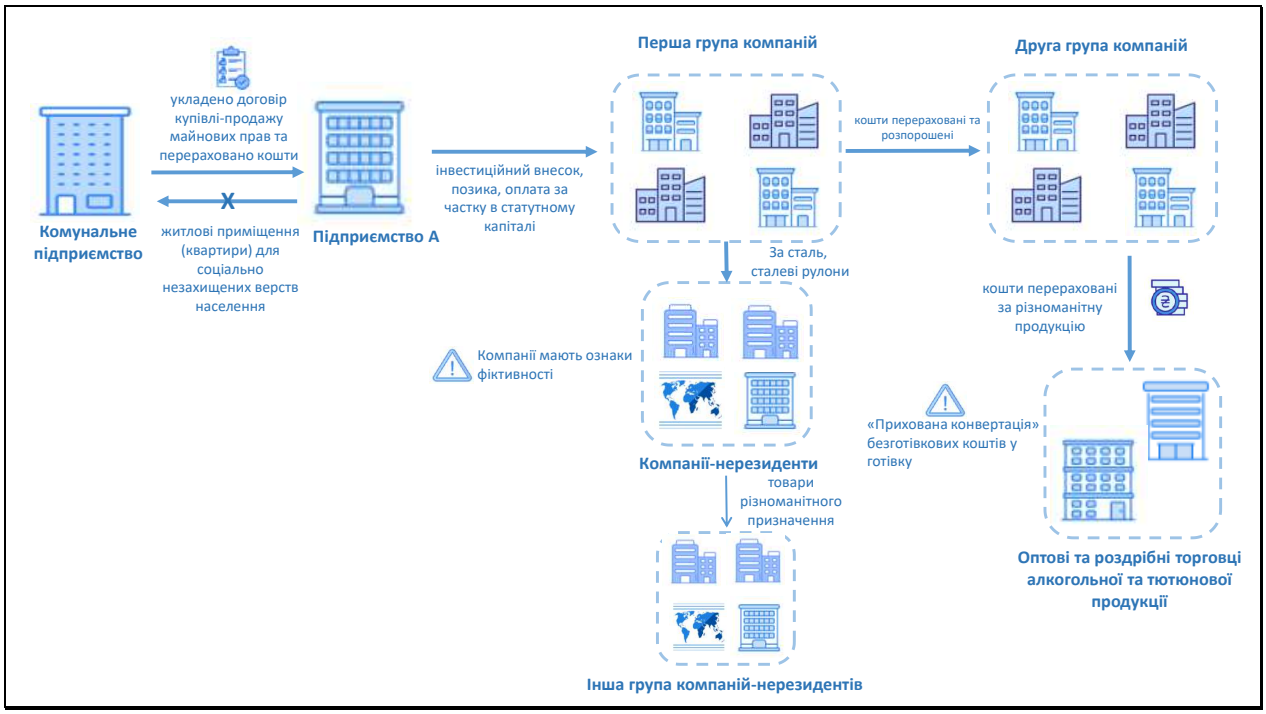
Держфінмоніторингом, з врахуванням інформації, отриманої від правоохоронного органу, виявлено схему привласнення майна комунального підприємства та її подальшої легалізації.

Комунальне підприємство, незважаючи на підвищену ризиковість об'єкта інвестування, уклало з **Підприємством А** договір купівлі-продажу майнових прав, за яким мало отримати у власність квартири для соціально незахищених верств населення. Квартири до **Комунального підприємства** не передавались.

Встановлено, що кошти перераховані **Комунальним підприємством** на рахунки **Підприємства А** надалі переказано на рахунки **Першої групи компаній** як інвестиційний внесок, надання позики, оплату за частку в статутному капіталі. З рахунків **Першої групи компаній** кошти частково розпорошені на рахунки **Другої групи компаній** та частково перераховані на користь **Компаній-нерезидентів**, які мають ознаки фіктивності, та надалі перераховано кошти **Іншій групі компаній-нерезидентів** за товари різноманітного призначення.

В свою чергу, з рахунків **Другої групи компаній** кошти **Підприємства А** надалі частково легалізували шляхом перерахувань на користь **Оптових та роздрібних торговців** алкогольної та тютюнової продукції з метою «прихованої конвертації» безготівкових коштів у готівку.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2024.4.3.4. Відмивання коштів, одержаних від продажу незаконно привласненого державного майна, з використання переуступлення прав вимог, сміттєвих цінних паперів та фінансової допомоги

Держфінмоніторингом, з урахуванням інформації правоохоронного органу, виявлено схемні операції, які можуть бути спрямовані на легалізацію коштів, отриманих від продажу незаконно привласненого державного майна за участю посадових осіб підприємства з державною часткою власності.

Підприємством-виробником, часткою якого володіє держава (Голова Наглядової ради – **Фізична особа 1**, генеральний директор – **Фізична особа 2**), реалізовано готову продукцію на користь **Компанії А** на підставі укладеного договору, проте не отримано коштів за поставлений товар.

У зв'язку з невиконанням умов договору **підприємство-виробник** переуступило право вимоги боргу від **Компанії А** на користь **Компанії Б**. На момент переуступки боргу **підприємство-виробник** вже мало штучно створені боргові зобов'язання перед **Компанією Б** за договорами позики.

В свою чергу, привласнену готову продукцію **Компанією А** було реалізовано підприємствам реального сектору економіки, а кошти, накопичені від продажу цієї продукції, **Компанією А** надалі було перераховано:

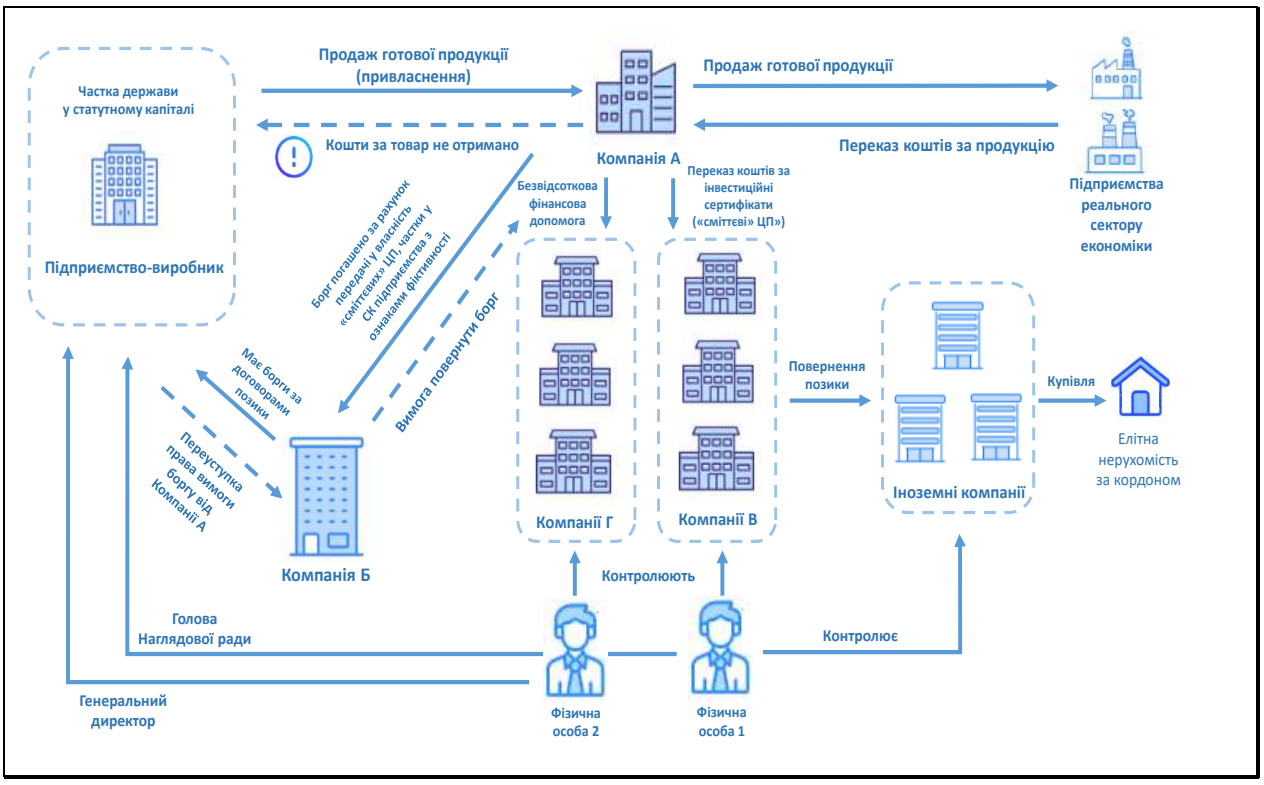
- **Компаніям В**, підконтрольним **Фізичній особі 1**, на підставі договорів купівлі інвестиційних сертифікатів («сміттєвих» цінних паперів), які згодом по ланцюгу було виведено під виглядом повернення позики на користь підконтрольних їй **іноземних компаній** та використано для купівлі елітної нерухомості за кордоном;

- **Компаніям Г**, підконтрольним **Фізичній особі 2**, у вигляді надання безвідсоткової фінансової допомоги, яка була використана для ведення господарської діяльності.

Борг **Компанії А** перед **Компанією Б** за договором переведення прав вимоги було погашено шляхом передачі у власність «сміттєвих» цінних паперів та частки у статутному капіталі підприємства, що має ознаки фіктивності, тобто, без фізичного перерахування коштів.

Враховуючи зазначене, посадовими особами підприємства з державною часткою власності було реалізовано злочинну схему виведення коштів, одержаних від продажу привласненого майна **Підприємства-виробника**, шляхом їх маскування та подальшої легалізації через компанії, у т.ч. іноземні, підконтрольні цим посадовим особам.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2024.4.3.5. Заволодіння бюджетними коштами та ухилення від сплати податків шляхом придбання обладнання за завищеними цінами з використанням посередництва та компаній з ознаками фіктивності

Держфінмоніторингом, з урахуванням інформації, отриманої від правоохоронного органу та ПФР іноземних держав, виявлено схему заволодіння бюджетними коштами шляхом придбання обладнання за значно завищеними цінами з подальшою їх легалізацією шляхом перерахування на користь ряду іноземних юридичних осіб.

Державне підприємство уклало з **Компанією А** (Країна 1) контракт на постачання обладнання польського виробництва, та, відповідно до контракту, перераховано на користь **Компанії А** значну суму коштів.

Водночас **Компанія А** виступала лише посередником та придбала зазначене обладнання вдвічі дешевше у **Юридичної особи з України**, що є офіційним представником з реалізації зазначеного обладнання в Україні від **Компанії Б** – польського виробника.

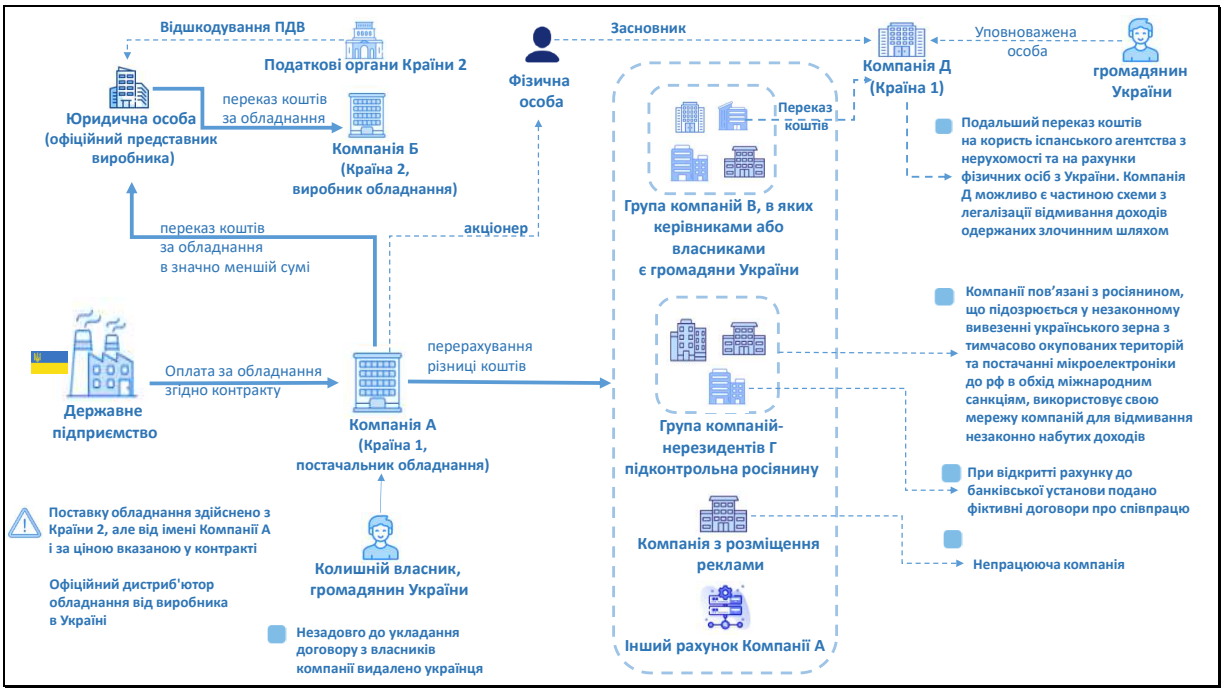
При цьому, фактичне постачання обладнання здійснено від імені **Компанії А**, але з Країни 2. На користь **Юридичної особи** зараховано відшкодування ПДВ з податкових органів Польщі. Слід зазначити, що власником **Компанії А** був громадянин України, якого було вилучено з переліку власників незадовго до укладання контракту.

Надалі різницю коштів між реальною вартістю обладнання та сплаченою **Державним підприємством**, що залишилися на рахунку **Компанії А**, перераховано на інший рахунок **Компанії А**, а також на користь:

- **Компанії з розміщення реклами**, що не працює;
- **Групи компаній В**, у яких керівниками або власниками є громадяни України;
- **Групи компаній Г**, які пов’язані з росіянином, який отримав український паспорт та наразі проживає в Країні 3. Дана особа підозрюється у незаконному вивезенні українського зерна з тимчасово окупованих територій та постачанні мікроелектроніки до росії в обхід міжнародних санкцій. Також особа використовує мережу власних компаній для відмивання злочинних доходів. Відомо, що при відкритті рахунку однією з компаній до банківської установи подано фіктивні договори про співпрацю з іншою компанією.

Також, встановлено, що одна з **Групи компаній В**, здійснювала перекази на користь **Компанії Д** (Країна 1), уповноваженою особою в якій є громадянин України, а засновницькими зв’язками вона пов’язана з **Компанією А**. Надалі отримані від однієї з **Групи компаній В** кошти, **Компанія Д** перерахувала на користь іноземного агентства з нерухомості та на рахунки фізичних осіб з України. Таким чином, **Компанія Д** може бути частиною схеми з легалізації відмивання доходів одержаних злочинним шляхом.

Правоохоронним органом здійснюється досудове розслідування.



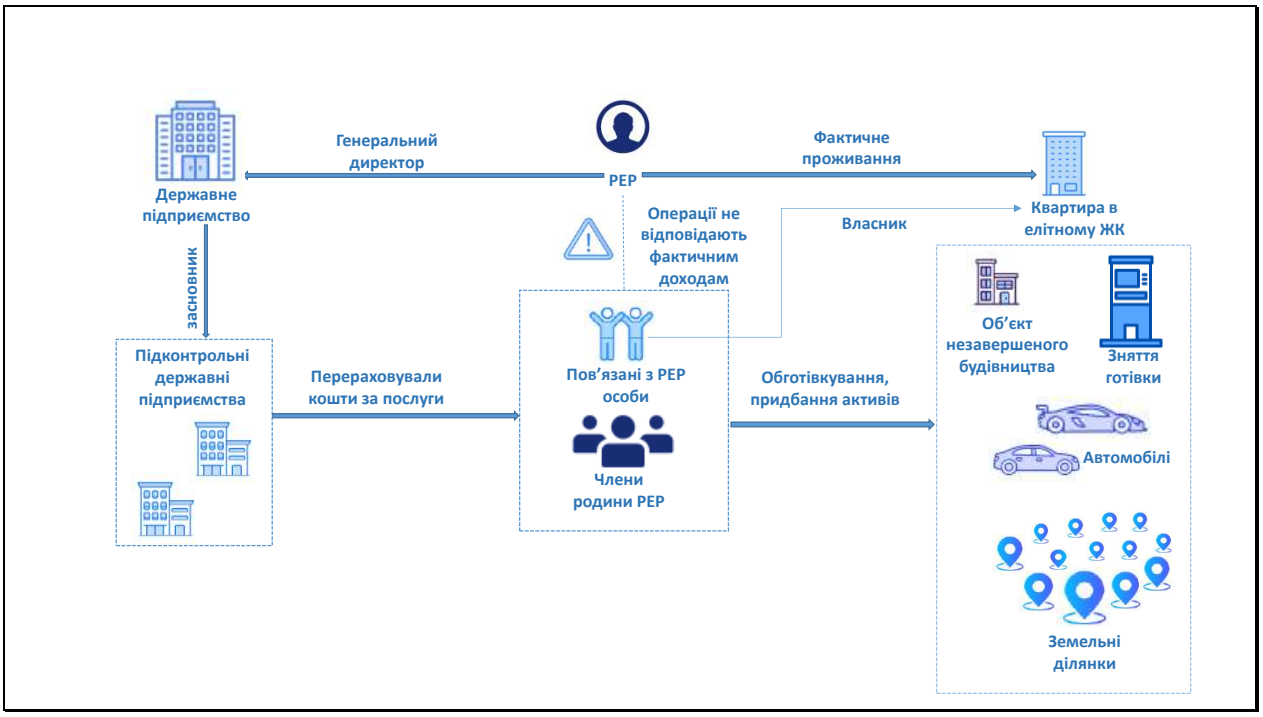
Приклад 2024.4.3.6. Виведення коштів з державних підприємств з метою легалізації злочинних доходів шляхом завищення ціни наданої послуги, вартість якої складно оцінити

Держфінмоніторингом з урахуванням інформації, отриманої від правоохоронного органу, виявлено схему, яка була направлена на використання коштів виведених з підконтрольних державних підприємств.

Встановлено, що **Пов'язана з РЕР** особа отримувала кошти за послуги від Державних підприємств, фактично підконтрольних РЕР, з подальшим їх обготівковуванням.

Крім того, **РЕР** та члени родини **РЕР** набули у власність дороговартісні автомобілі, квартиру в елітному житловому комплексі, об'єкт незавершеного будівництва та ряд земельних ділянок. Враховуючи, що вартість придбаних активів значно перевищувала офіційні доходи родини, та з метою їх приховування чи маскування, оформлення здійснювалось на пов'язаних з **РЕР** осіб. Зокрема відомо, що **РЕР** користується квартирою в елітному житловому комплексі, власником якої є пов'язана з **РЕР** особа.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2024.4.3.7. Відмивання коштів, одержаних від корупційних діянь, з використанням кеш-кур'єрів

Держфінмоніторингом з урахуванням інформації, отриманої від правоохоронного органу та ПФР іноземних держав, виявлено схему, яка була направлена на легалізацію коштів, отриманих внаслідок зловживання владою або службовим становищем, корупційних діянь.

Встановлено, що **Керівник закладу охорони здоров'я** та **члени сім'ї** посадової особи вивезли з України значні обсяги готівки на територію Країни 1. До схеми переміщення коштів також були залучені **Кеш-кур'єри**.

При цьому більша частина готівки не була задекларована при перетині державного кордону України. Натомість при перетині кордону Країни 1 кошти були задекларовані в повному обсязі.

Задекларовані готівкові кошти були внесені на рахунки **Керівника закладу охорони здоров'я** та **членів сім'ї**, відкриті на території Країни 1. Надалі кошти перераховано на рахунок **Керівника закладу охорони здоров'я**, відкритий у Країні 2, та на користь підконтрольних **членам сім'ї** посадової особи компаній, зареєстрованих у Країні 3 та Країни 1.

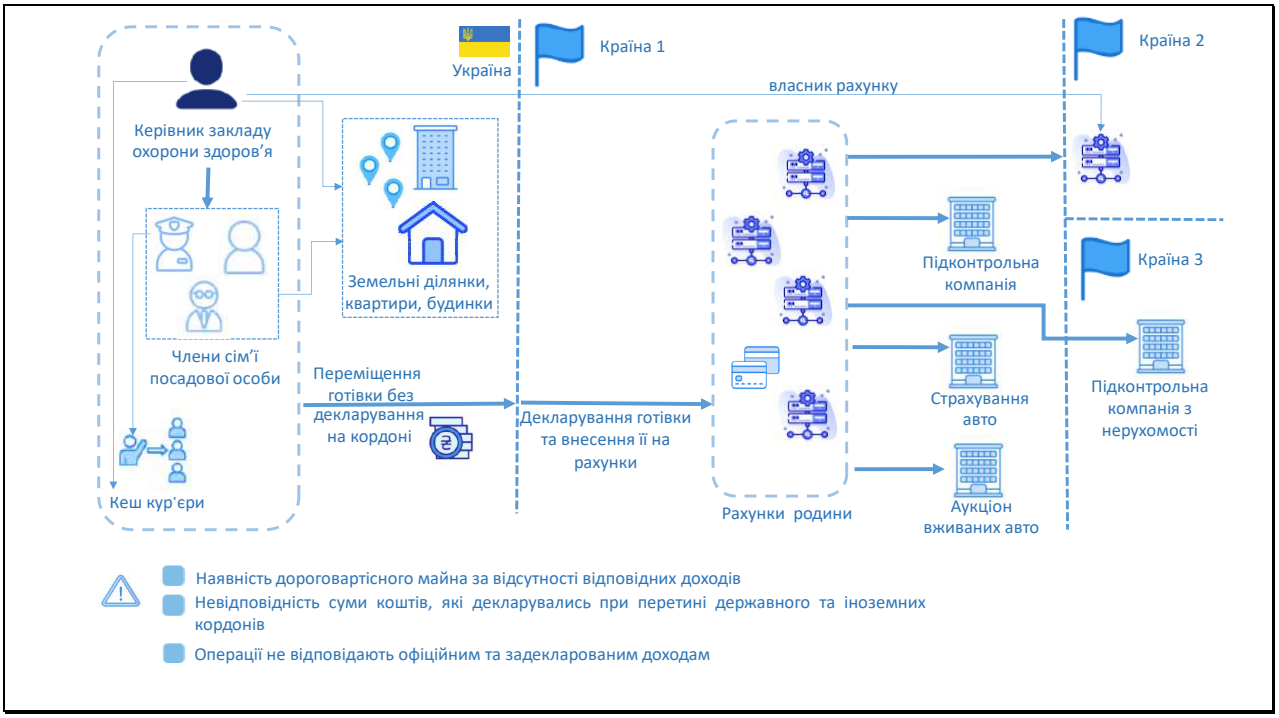
Також, одним з **членів сім'ї** посадової особи з рахунку, відкритого на території Країни 1, здійснено переказ значних сум коштів на аукціон вживаних, але, ймовірно, дороговартісних авто та в оплату страхування авто.

Водночас, родина володіє великою кількістю квартир, житлових будинків та земельних ділянок.

Слід зазначити, що **члени сім'ї** посадової особи також є, або були посадовими особами державних установ. Обсяги фінансових операцій

Керівника закладу охорони здоров'я та **членів сім'ї** посадової особи не відповідають їх офіційним та задекларованим доходам.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2024.4.3.8. Відмивання коштів, отриманих внаслідок корупційних діянь, з використанням родичів посадової особи

Держфінмоніторингом, з урахуванням інформації правоохоронного органу та ПФР іноземної держави, виявлено схему легалізації (відмивання) коштів, отриманих внаслідок корупційних діянь.

Міським головою при виконанні своїх обов'язків, організовано схему легалізації незаконних доходів через своїх родичів зокрема через **Доньку** та її **Чоловіка** (громадянина Країни 1).

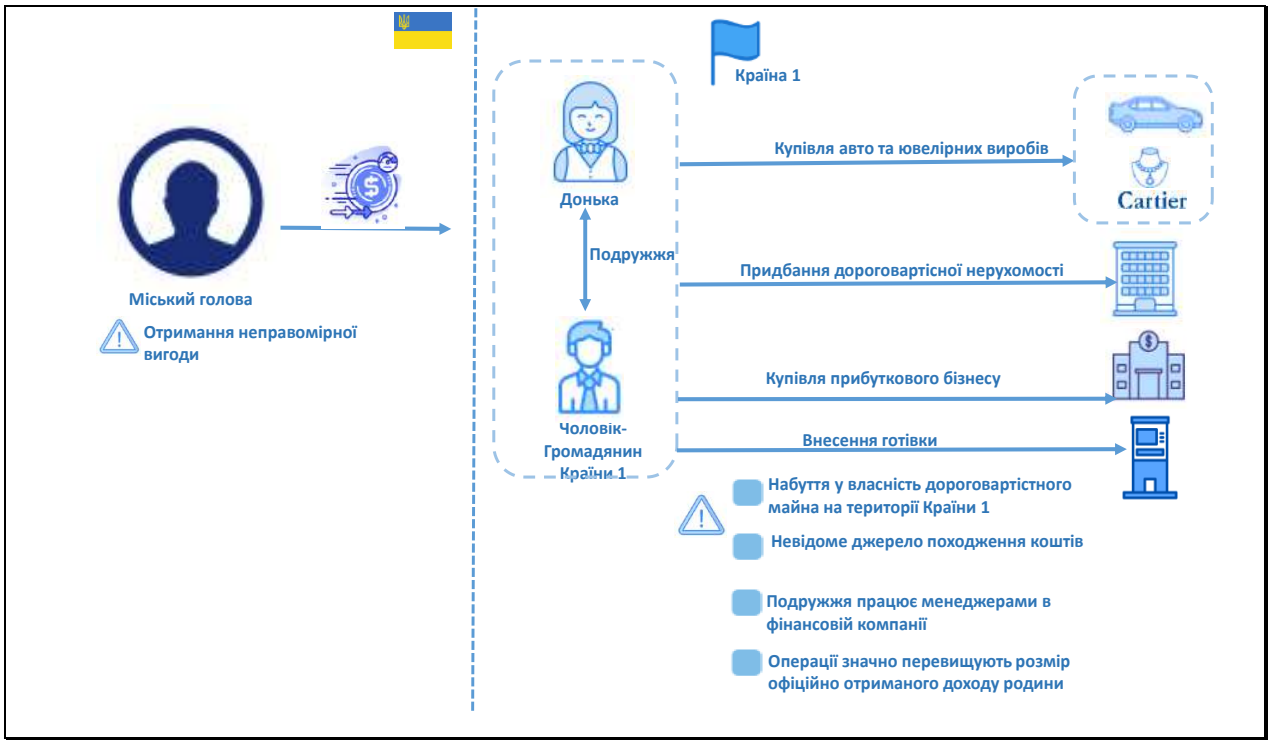
Встановлено, що **Донька** отримувала кошти від свого батька **Міського голови** та витрачала їх на території Країни 1, купуючи дороговартістні активи, зокрема: нерухоме майно, автомобіль (Porsche Cayenne) та прикраси (Cartier).

Також, **Чоловік** придбав корпоративні права компанії резидента Країни 1.

При цьому **Донька** та її **Чоловік** працюють менеджерами в фінансовій компанії, а їх офіційні доходи не відповідають обсягам здійснених операцій.

Крім того, **Донькою** та її **Чоловіком** здійснювалось внесення готівки до банківських установ на території Країни 1. Однак вказані операції були зупинені через відсутність достатнього доходу та невідомого джерела походження коштів.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2024.4.3.9. Відмивання коштів через послуги сумнівної вартості

Держфінмоніторингом, з урахуванням інформації, отриманої від правоохоронного органу, встановлено ланцюг перерахування коштів, які були використані для надання неправомірної вигоди з метою підкупу представників судової влади у своїх інтересах.

Так, у **Фізичної особи А** виник злочинний умисел з надання неправомірної вигоди **Голові Суду** за прийняття рішення в інтересах підконтрольних йому підприємств. Для цього було залучено **Фізичну особу Б** та **Фізичну особу В**. Відомо, що у **Фізичної особи Б** дружні відносини з **Головою Суду**.

В результаті розроблено схему обготівкування коштів для надання неправомірної вигоди з використанням рахунку **Юридичної фірми**, співзасновником якої є **Фізична особа В**.

Встановлено, що на рахунок **Юридичної фірми** було зараховано значні суми коштів від **Групи компаній**, власником якої є **Фізична особа А**.

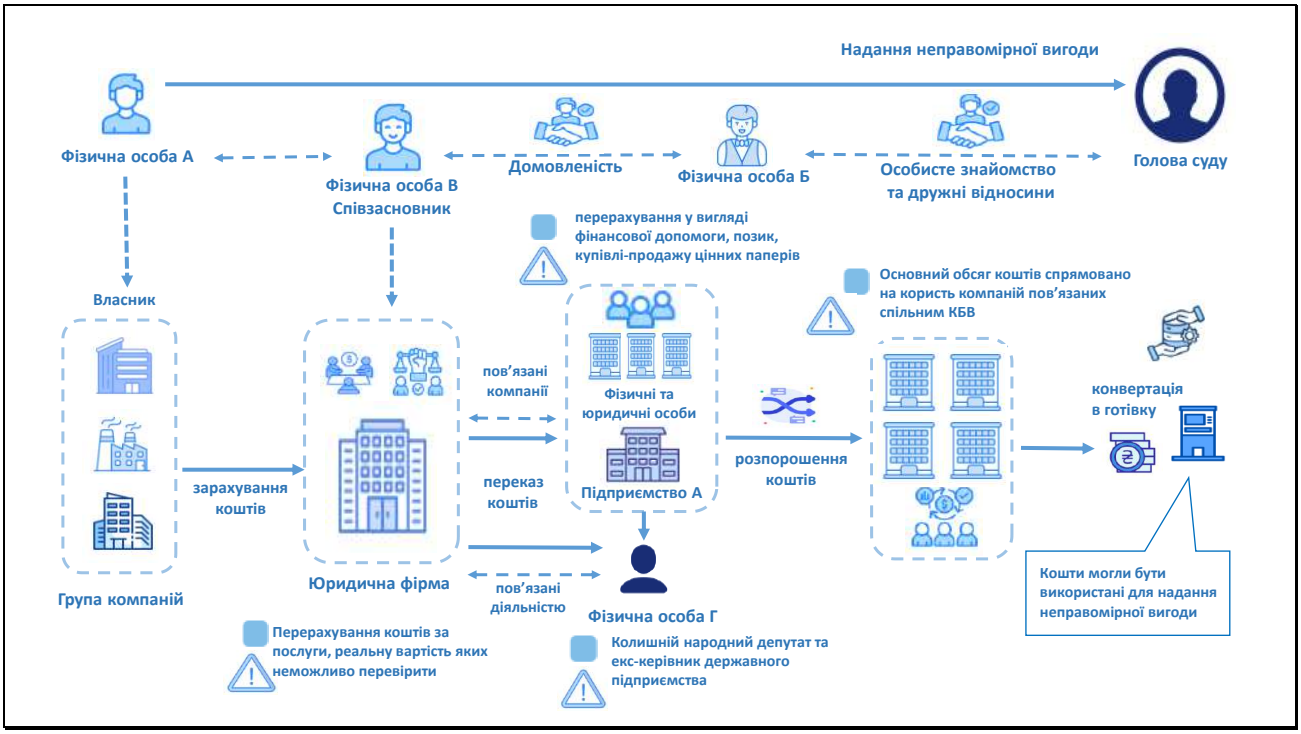
Надалі **Юридична фірма** здійснила перерахування коштів на користь фізичних та юридичних осіб, більшість з яких є прямо або опосередковано пов'язаними з нею, у вигляді сумнівних розрахунків за послуги, реальну вартість яких неможливо перевірити.

Одним з основних отримувачів даних коштів є **Підприємство А**, з рахунків якого надалі кошти розпорошено між групою отримувачів у вигляді фінансової допомоги, позик, купівлі-продажу цінних паперів. Основний обсяг коштів спрямовано на користь компаній, пов'язаних спільним бенефіціарним власником.

Крім того, одним з отримувачів значної суми коштів, як від **Підприємства А**, так і напряму від **Юридичної фірми** є **Фізична особа Г** – колишній народний депутат та екскерівник державного підприємства, яке було тісно пов'язане із діяльністю **Юридичної фірми**.

Таким чином, кошти проведені через рахунок **Юридичної фірми** та її контрагентів, надалі могли бути конвертовані в готівку та використані для надання неправомірної вигоди **Голові суду** для сприяння в інтересах **Фізичної особи А**.

Правоохоронним органом здійснюється досудове розслідування.



РОЗДІЛ 4.4. ВИКОРИСТАННЯ НЕПРИБУТКОВИХ ОРГАНІЗАЦІЙ В НЕЗАКОННІЙ ДІЯЛЬНОСТІ ТА НЕЗАКОННЕ ЗАВОЛОДІННЯ ТА ПРИВЛАСНЕННЯ БЛАГОДІЙНОЇ ДОПОМОГИ

НПО, через особливості їхньої діяльності, можуть бути вразливими до ризику зловживань, зокрема у вигляді ВК/ФТ. Це потребує дотримання міжнародних стандартів, таких як Рекомендація 8 FATF. Метою цієї рекомендації є створення збалансованого підходу до регулювання неприбуткового сектору, який одночасно забезпечує ефективний нагляд за фінансовою діяльністю організацій та не обмежує їх законну діяльність.

Згідно з наведеним у Рекомендації 8 визначенням, для цілей зазначеної Рекомендації, НПО відноситься до юридичної особи або правового утворення чи організації, яка в першу чергу здійснює збір чи витрачання коштів для благодійних, релігійних, культурних, освітніх, соціальних або братських цілей, чи для здійснення інших видів «добрих справ».

З урахуванням зазначених положень під визначення Рекомендації 8 FATF підпадають:

громадські об’єднання;
релігійні організації;
благодійні організації;
професійні спілки, їх об’єднання та організації профспілок;
спілки (асоціації);
творчі спілки.

НПО під час повномасштабної агресії росії стали ключовими у наданні гуманітарної допомоги, підтримці постраждалих, відновленні інфраструктури та захисті прав людей. НПО забезпечують допомогу внутрішньо переміщеним особам, постачають гуманітарні вантажі, документують воєнні злочини та сприяють зміцненню громадянського суспільства.

Окремо слід виділити внесок українських та іноземних аналітичних центрів у посилення санкційного тиску на агресора та протидію обходу санкцій. На тлі посилення моніторингу ефективності санкцій, НПО надають важливу аналітичну підтримку державним органам та іноземним партнерам України.

Як і будь-яка юридична чи фізична особа, НПО піддаються ризику використання у незаконній діяльності, зокрема з метою ВК/ФТ/ФРЗМЗ. Ці ризики зростають у ситуаціях, коли організація має непрозору діяльність, не формує звітні документи та не застосовує належні ефективні заходи управління своїми ризиками.

Глобальний рівень

На глобальному рівні незаконне заволодіння гуманітарною допомогою є поширеною проблемою під час воєн і криз. У багатьох війнах (конфліктах) у світі гуманітарна допомога часто ставала об'єктом корупції, зловживань або маніпуляцій.

Приклад 1. По закінченню Другої світової війни виникла величезна гуманітарна криза. Міжнародна спільнота почала активно організовувати гуманітарну підтримку, але й тут мали місце корупція, зловживання та нерівномірний розподіл ресурсів[13].

Приклад 2. У конфліктах, таких як війни на Близькому Сході чи в Африці, корупція та крадіжка гуманітарної допомоги є одним із викликів для міжнародних організацій.

Приклад 3. У Сирії гуманітарна допомога неодноразово блокувалася, викрадалася чи продавалася зацікавленими сторонами.

Приклад 4. На Балканах після війни, зловживання гуманітарною допомогою створювало соціальні напруження, оскільки ресурси не завжди доходили до найуразливіших груп населення.

[13] Після закінчення Другої світової війни світ зіткнувся з масштабною гуманітарною кризою, яка охопила значну частину Європи, Азії та інших регіонів, постраждалих від війни. Воєнні дії залишили руїни міст і сіл, зруйновану інфраструктуру, мільйони біженців, голод і хвороби. Руйнування спричинили колапс економіки та системи життєзабезпечення. Багато транспортних мереж, промислових об'єктів і житлових будинків не підлягали відновленню. Мільйони людей залишили свої домівки через бойові дії, депортації, окупацію та етнічні переселення.

У 1945 році створили Організацію Об'єднаних Націй, метою якої стало підтримання миру та надання гуманітарної допомоги. Для негайної допомоги заснували Адміністрацію допомоги та відновлення Об'єднаних Націй (ЮНРА), яка займалася постачанням продуктів харчування, медикаментів і поверненням переміщених осіб додому (Архіви та управління записами Організації Об'єднаних Націй. Архіви Адміністрації допомоги та відбудови Об'єднаних Націй (1943–1948). URL: https://archives.un.org/content/records-united-nations-relief-and-rehabilitation-administration-1943%E2%80%931948).

Надалі, щоб відновити економіку, запрацював План Маршалла, який надав фінансову допомогу країнам Європи для відбудови їхньої інфраструктури.

В будь-якій масштабній програмі, існували ризики корупції, розкрадання та нецільового використання коштів. Ці ризики відображають загальну проблему для великих гуманітарних та економічних програм, коли недосконалість механізмів контролю може сприяти зловживанням. Сьогодні розвиток цифрових технологій дозволив значно знизити ці ризики шляхом покращення прозорості та звітності, але в умовах війни не завжди наявні релевантні дані.

Корупція у гуманітарній допомозі в умовах конфліктів[14]

Дослідження зосереджене на ризиках корупції у розподілі гуманітарної допомоги в регіонах, охоплених конфліктами.

У таких умовах доставка допомоги ускладнена через політичні, військові та логістичні виклики. Основні форми корупції включають перенаправлення допомоги збройними угрупованнями, вимагання «зборів» на гуманітарні ресурси, маніпуляції списками отримувачів та зловживання під час транспортування або зберігання допомоги.

Таким чином, корупція у сфері гуманітарної допомоги є глобальною проблемою, яка проявляється в кожному конфлікті, хоча рівень реагування та боротьби з нею залежить від конкретної країни.

Важливо підкреслити, що в Україні боротьба зі зловживаннями є показовою завдяки високому рівню громадського контролю.

Це стало можливим завдяки активній участі громадянського суспільства, яке не лише контролює діяльність державних органів, але й підтримує прозорість у сфері розподілу гуманітарної допомоги, громадських фінансів та взаємодії з міжнародними донорами.

Заходи обачливості для мінімізації ризиків. Для мінімізації ризиків використання НПО в незаконній діяльності необхідно впроваджувати заходи обачливості. Це може включати перевірку реєстраційних документів, аналіз мети діяльності організації, ідентифікацію бенефіціарних власників та вивчення джерел фінансування.

Таким чином, корупція у сфері гуманітарної допомоги є глобальною проблемою, яка проявляється в кожному конфлікті, хоча рівень реагування та боротьби з нею залежить від конкретної країни.

[14] https://www.u4.no/publications/corruption-in-humanitarian-assistance-in-conflict-settings.pdf

Заходи обачливості для мінімізації ризиків. Для мінімізації ризиків використання НПО в незаконній діяльності необхідно впроваджувати заходи обачливості. Це може включати перевірку реєстраційних документів, аналіз мети діяльності організації, ідентифікацію бенефіціарних власників та вивчення джерел фінансування.

ФТ/ВК/Санкції

НПО можуть бути використані для фінансування терористичної діяльності, ВК, отриманих від злочинної діяльності та обходу санкцій. Також НПО можуть використовуватись для пропагування, популяризації та поширення сепаратистських настроїв у населення, втілення стандартів «руського миру» тощо.

Особливості діяльності. НПО мають високий рівень довіри в суспільстві, вони мають доступ до джерел фінансування, які складно контролювати (наприклад, благодійні внески), а їхня діяльність передбачає можливість використання готівкових коштів. Водночас, особливості діяльності НПО та волонтерської активності роблять їх привабливими для терористичних організацій і вразливими для злочинного використання.

Псевдоволонтери. Додаткові ризики несуть збори коштів псевдоволонтерами, які зловживаючи довірою та користуючись загальним піднесеним патріотизмом українців можуть здійснювати неконтрольований збір коштів шляхом p2p-переказів на карткові рахунки без надання звітності їх цільового використання.

Прикриттям для незаконної діяльності. НПО можуть використовуватися безпосередньо у схемах вчинення ВК/ФТ, а також слугувати прикриттям для незаконної діяльності інших суб’єктів. Існують випадки привласнення активів НПО шляхом укладання «фіктивних» договорів на купівлю товарів / надання послуг. Також виявлялися факти продажу гуманітарної та інших видів матеріальної допомоги з метою подальшого привласнення отриманих коштів, така діяльність маскувалась під надання допомоги населенню в натуральній формі.

Організації сепаратистського спрямування. На території України під виглядом законних структур, наприклад, спортивних клубів чи громадських об’єднань, діють організації сепаратистського спрямування, які спонсоруються іноземними фондами різних форм власності, приватними особами, в тому числі представниками олігархічних структур, та іноземними маргінальними політичними партіями, які зацікавлені в ескалації напруженості та дестабілізації ситуації в Україні. Непоодинокі випадки пропагування сепаратистських настроїв серед парафіян служителями церкви.

Узагальнені типові приклади використання НПО в незаконній діяльності наведено нижче.

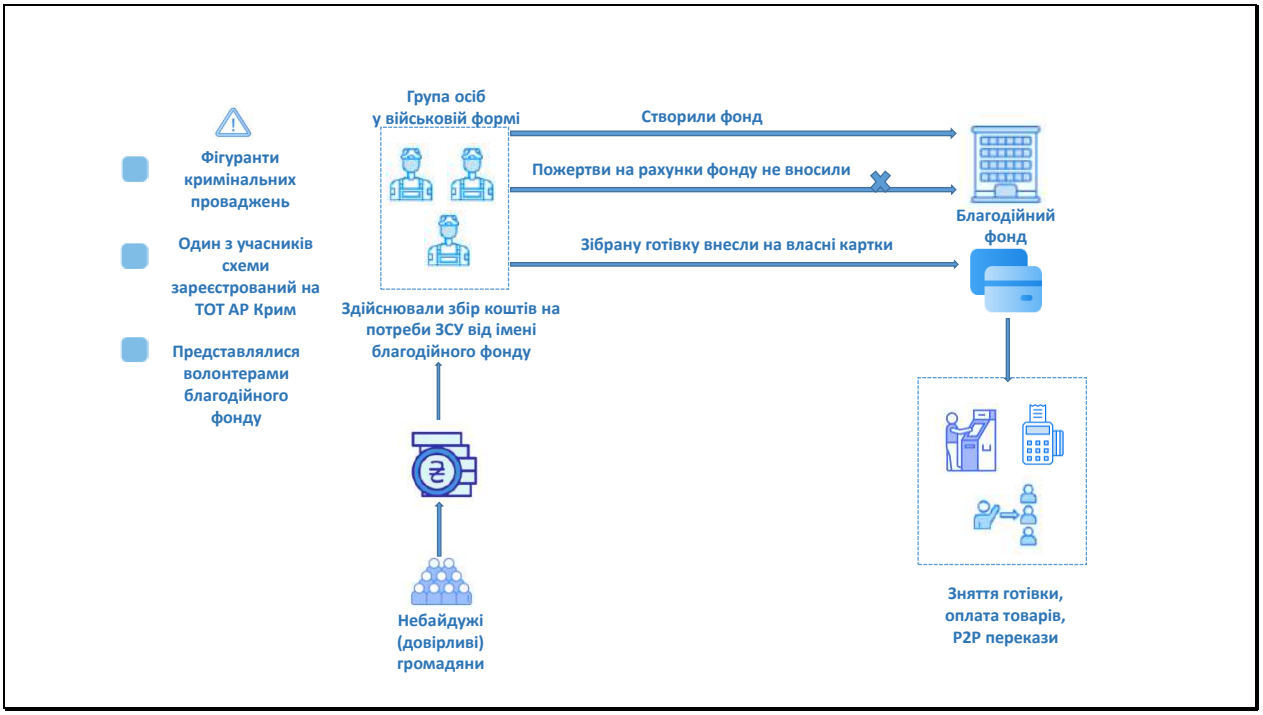
Приклад 2024.4.4.1. Фіктивні неприбуткові організації

Держфінмоніторингом з урахуванням інформації, отриманої від правоохоронного органу, виявлено схему, яка була направлена на привласнення благодійних пожертв.

Встановлено, що група осіб, щодо яких наявні кримінальні провадження, створили **Благодійний фонд** з патріотичною назвою. Надалі, одягнувшись у військову форму, особи представлялись волонтерами цього фонду та збирали кошти у громадян на вулиці, нібито на потреби Збройних Сил України.

Водночас отримані від небайдужих (довірливих) громадян кошти, не були зараховані на рахунки **Благодійного фонду**, а були внесені на власні картки псевдоволонтерів, та надалі використовувалися на їх особисті потреби в оплату за товари та послуги, P2P перекази з невизначеними призначеннями, зняттям готівки.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2024.4.4.2. Діяльність оперативно-бойових груп російського ГРУ під виглядом НПО

Правоохоронні органи України викрили оперативно-бойову групу воєнної розвідки росії в Одесі. Вилучено понад 70 одиниць вогнепальної зброї з оптичними прицілами та боєприпаси, а також бронежилети, шоломи, балістичні окуляри та інше тактичне спорядження.

За інструкцією російської спецслужби ще на початку повномасштабного вторгнення росії зловмисники готувалися до силового захоплення державних установ на Одещині. Зловмисників також планувалось залучити до атак сил оборони з тилу.

Після початку повномасштабної агресії у 2022 році та затримки просування військ росії на фронті цю оперативно-бойову групу перевели в режим очікування і активували лише влітку 2024 року, коли вона отримали таємні завдання.

За матеріалами справи, резидентом групи російського ГРУ був 49-річний мешканець тимчасово окупованого Криму, який після захоплення півострова переїхав до Одеси.

На початку повномасштабної війни почав формувати оперативно-бойові загони під виглядом декількох **Громадських організацій (НПО)**. Дані організації начебто займалися питаннями військової історії, екології та юриспруденції, а насправді створили підпільні групи: снайперів, розвідки, зв'язку, оперативного забезпечення і одну з основних – штурмову групу.

Загалом фігуранти завербували до складу ворожого осередку понад два десятки осіб, які підпорядковувалися своєму керівнику за принципами військової ієрархії.

Під час обшуків у фігурантів окрім зброї і тактичного спорядження вилучено інструкції з підривної діяльності, холодну зброю, зокрема з логотипом спецслужб росії, та комп'ютерну техніку із доказами злочинів.

Приклад 2024.4.4.3. Легалізація привласнених благодійних внесків з використанням транскордонної мережі ВК

Держфінмоніторингом з урахуванням інформації правоохоронних органів та ПФР іноземної держави, виявлено схему, яка була направлена на привласнення благодійних внесків громадян європейської країни з використанням підконтрольних благодійних організацій та інших суб'єктів господарювання.

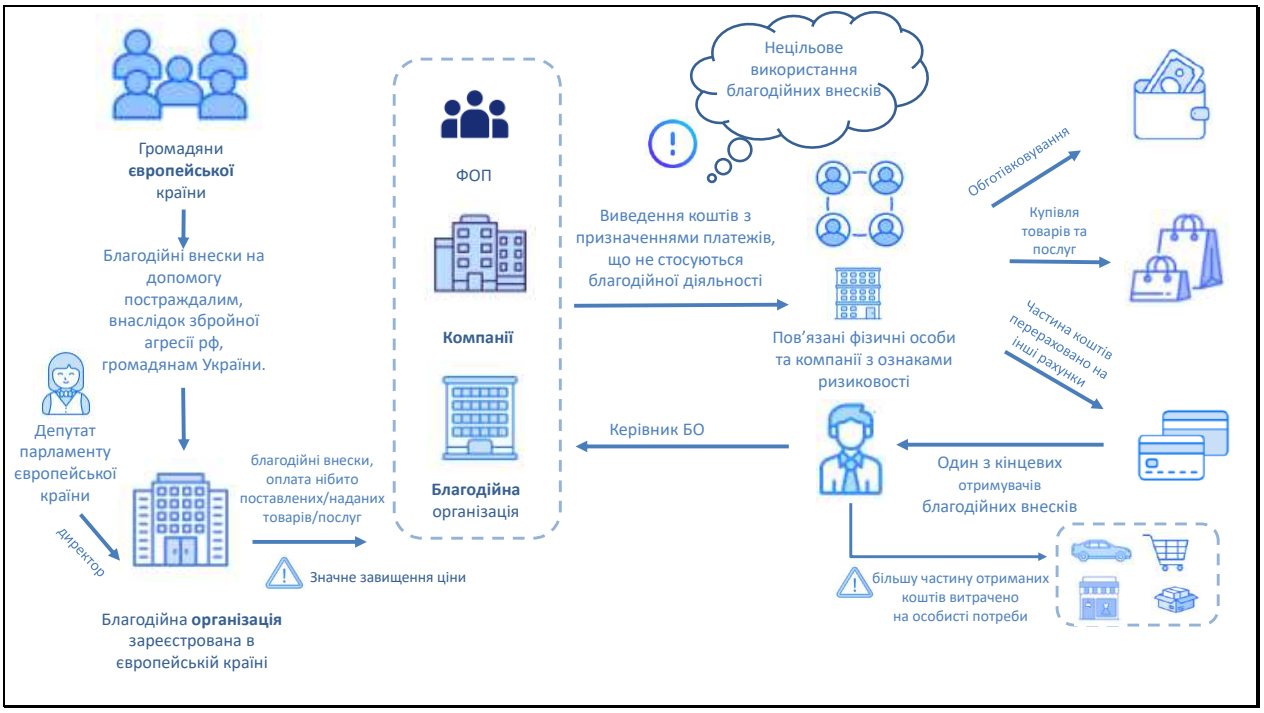
Встановлено, що на рахунки **європейської благодійної організації** (директором якої є **депутат парламенту європейської країни**) від громадян та юридичних осіб тієї ж країни було зараховано кошти на значні суми у вигляді благодійних внесків для надання допомоги постраждалим громадянам України, внаслідок збройної агресії росії.

Надалі отримані благодійні кошти було направлено на рахунки пов'язаних між собою українських **суб'єктів господарювання** та **благодійної організації** як благодійний внесок, оплату нібито поставлених/наданих товарів/послуг, при цьому, за значно завищеними цінами.

Згодом, основну частину зарахованих коштів переказано на користь іншої групи фізичних (в т.ч. керівників вищезгаданих суб'єктів господарювання) та юридичних осіб (що мають ознаки фіктивності та фінансові операції яких мають транзитний характер), з призначеннями платежів, що не стосуються благодійної діяльності. Зокрема перекази здійснювались в якості надання фінансової допомоги, оплати за паливо, запчастини, оренду приміщення, авто, виплати доходу від підприємницької діяльності та в результаті частково знімались готівкою чи використовувались для власних потреб.

Таким чином, групою фізичних осіб було реалізовано шахрайську схему заволодіння коштами громадян-нерезидентів шляхом переведення на рахунки пов'язаних фізичних та юридичних осіб.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2024.4.4.4. Використання фіктивних суб'єктів господарювання для ВК

Держфінмоніторингом з урахуванням інформації правоохоронного органу, виявлено схему, яка була направлена на привласнення благодійних пожертв з використанням підконтрольних благодійного фонду та юридичних осіб.

Відомо, що **Благодійний фонд** через банківський сервіс залучав пожертви від **Громадян України** для закупівлі генераторів та продуктових наборів громадянам на деокупованих територіях.

Надалі благодійні пожертви було направлено на рахунки **Групи юридичних осіб** за генератори, продуктові набори та паливні талони. Останні своєю чергою були оформлені на **Організатора схеми**.

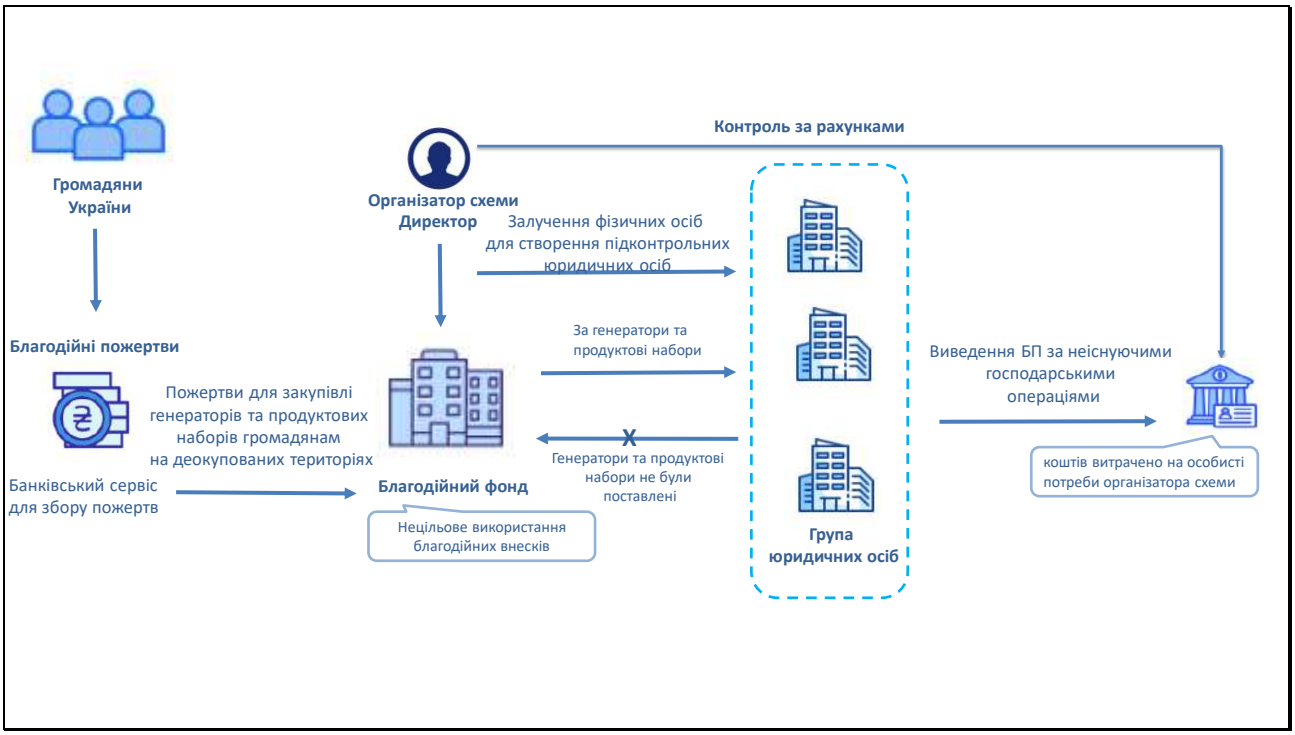
Встановлено, що громадяни з деокупованих територій не отримували генераторів та продуктових наборів.

А **Група юридичних осіб** не здійснювали господарських операцій з продажу продуктових наборів та генераторів.

Привертає увагу, що **Організатор схеми** за винагороду залучив фізичних осіб для створення підконтрольної **Групи юридичних осіб**.

Таким чином, **Організатор схеми** із залученням фізичних осіб реалізував схему заволодіння коштами громадян та їх відмивання.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2024.4.4.5. Відмивання коштів від прихованої підприємницької діяльності

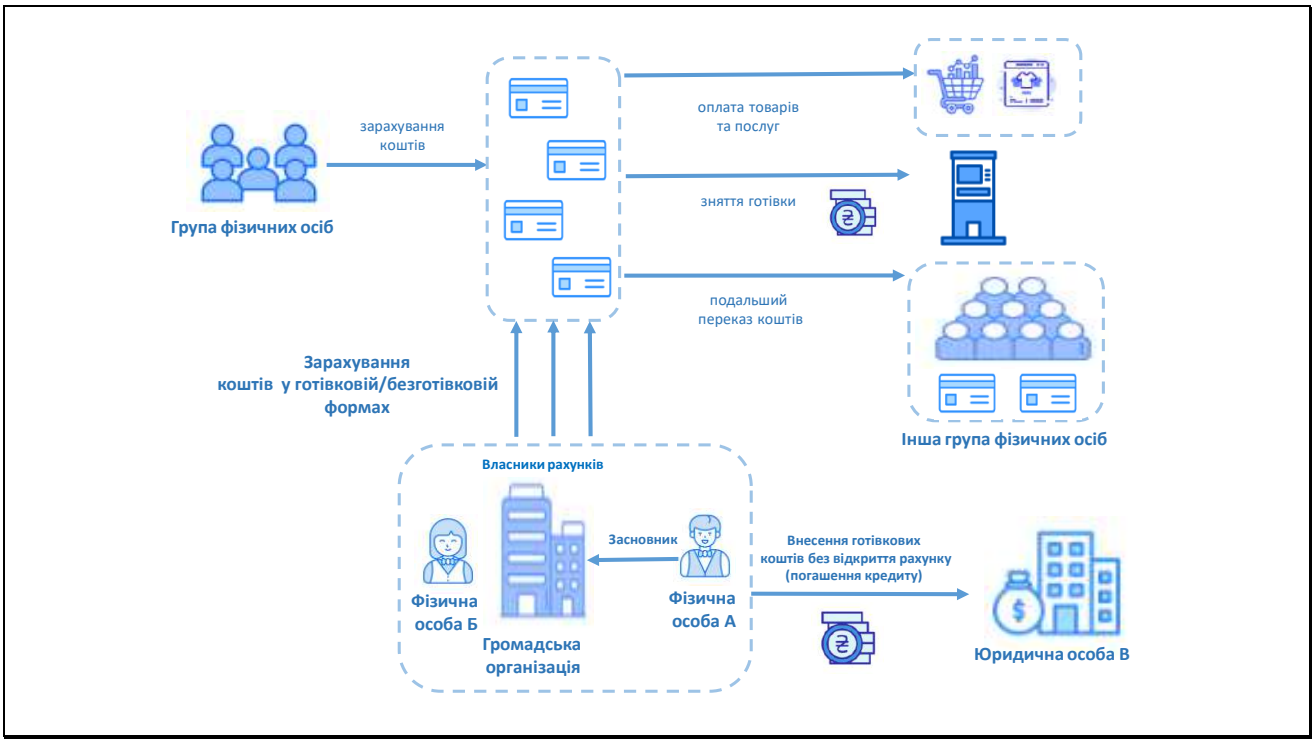
Держфінмоніторингом з врахуванням інформації, отриманої від правоохоронного органу встановлено, що рахунки **Фізичної особи А**, **Фізичної особи Б** та **Громадської організації** були використані для отримання доходів від прихованої підприємницької діяльності, у тому числі шахрайської діяльності, ймовірно пов'язаної із наданням послуг «реабілітації».

Так, **Фізичною особою А** засновано **Громадську організацію**, на рахунки якої, а також на власні рахунки **Фізичної особи А** та **Фізичної особи Б** зараховувались кошти від **Групи фізичних осіб** за перебування в реабілітаційному центрі їх родичів, яким необхідна допомога від алкогольної та наркотичної залежності.

Отримані кошти надалі перераховано на користь **Іншої групи фізичних осіб,** списано як оплату товарів та послуг, а також знято готівкою.

Також, **Фізичною особою А** вносилась готівка на користь **Юридичної особи В** як погашення кредиту.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2024.4.4.6. Відмивання привласнених благодійних внесків з використанням професійної мережі відмивання коштів

Держфінмоніторингом виявлено схему, яка була направлена на заволодіння чужими коштами шляхом обману чи зловживання довірою (шахрайство) та привласнення коштів державних установ.

Встановлено, що на власний рахунок **Настоятеля** та **Релігійної установи УПЦ МП** надходили кошти у вигляді благодійних пожертв від **Фізичних осіб – громадян України** на потреби придбання вугілля для обігріву **Релігійної установи**.

Частина благодійних пожертв використана для перерахування на **Компанію 1** за вугілля, а інша частина переказана на рахунки **Настоятеля** та використана ним на власні потреби.

Крім того, на рахунок **Компанії 1** також було зараховано кошти з рахунків **Державних установ**, в якості сплати за вугілля.

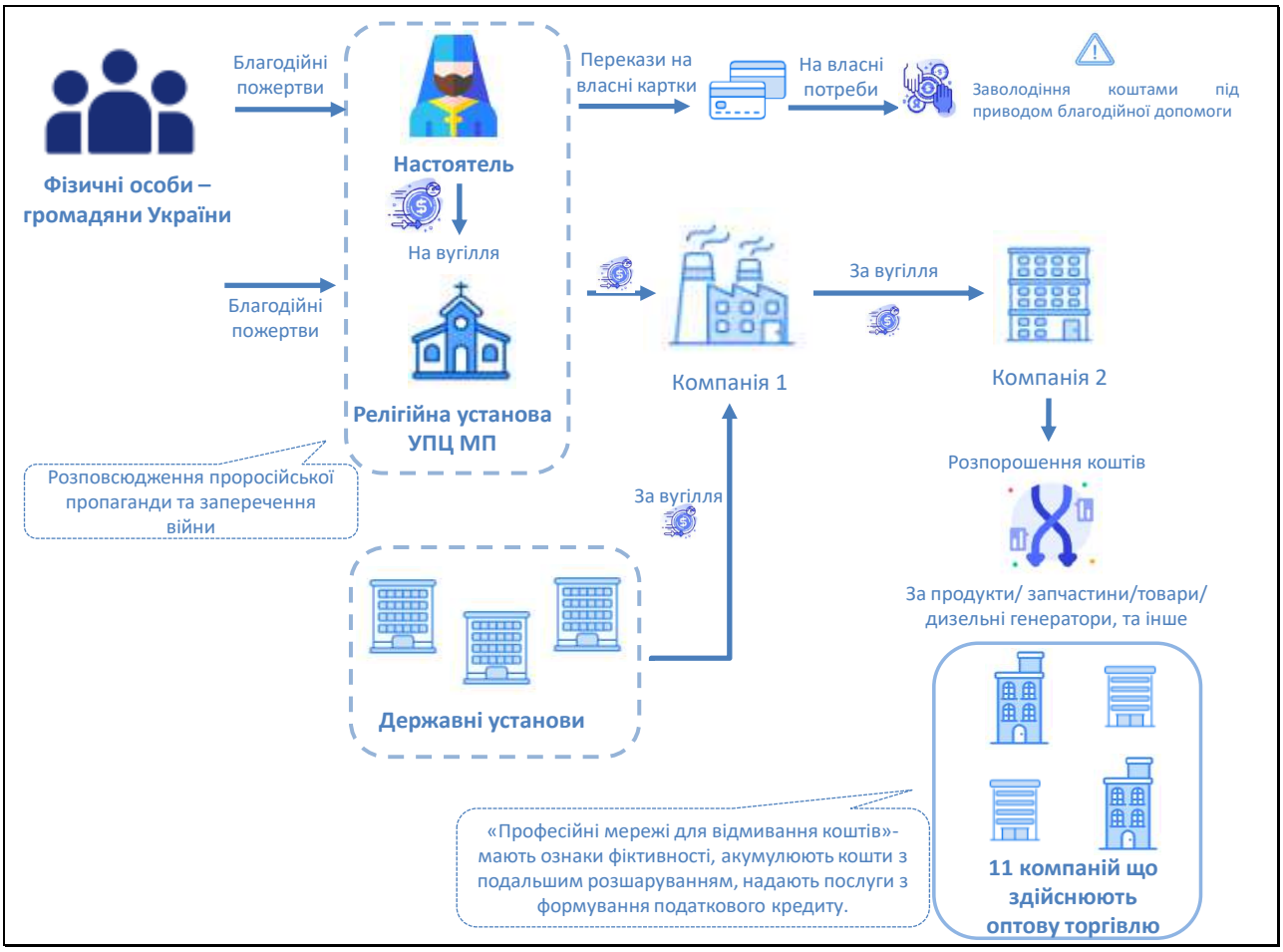
Надалі, зазначені кошти були переказані на користь **Компанії 2** як сплата за вугілля, якою кошти перенаправлено на користь **11 компаній**, що здійснюють оптову торгівлю, як оплата за продукти/запчастини/товари/ дизельні генератори тощо.

Також слід зазначити, що **Релігійна установа УПЦ МП** та її митрополит займалися розповсюдженням проросійської пропаганди.

Таким чином, виявлено схему заволодіння коштами благодійними пожертвами та привласнення коштів **Державних установ** та подальшу їх легалізацію через так звані **«професійні мережі для відмивання коштів» Компанію 1** та **Компанію 2**, що виконують функції транзитних підприємств,

мають ознаки фіктивності та акумулюють кошти на рахунках з подальшим розшаруванням на реальний сектор економіки для надання незаконних послуг з формування податкового кредиту.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2024.4.4.7. Привласнення коштів громадян під виглядом благодійних внесків

Держфінмоніторингом з урахуванням інформації, отриманої від правоохоронного органу, виявлено схему, яка була направлена на легалізацію коштів, отриманих внаслідок зловживання владою або службовим становищем шляхом незаконного використання благодійної допомоги та прихованої підприємницької діяльності.

Встановлено, що Колишній депутат міської Ради **Голова Громадської організації** разом зі знайомою йому **фізичною особою**, вступили у змову та здійснювали продаж пального пересічним громадянам, яке було попередньо придбане за благодійні внески для потреб територіальної оборони.

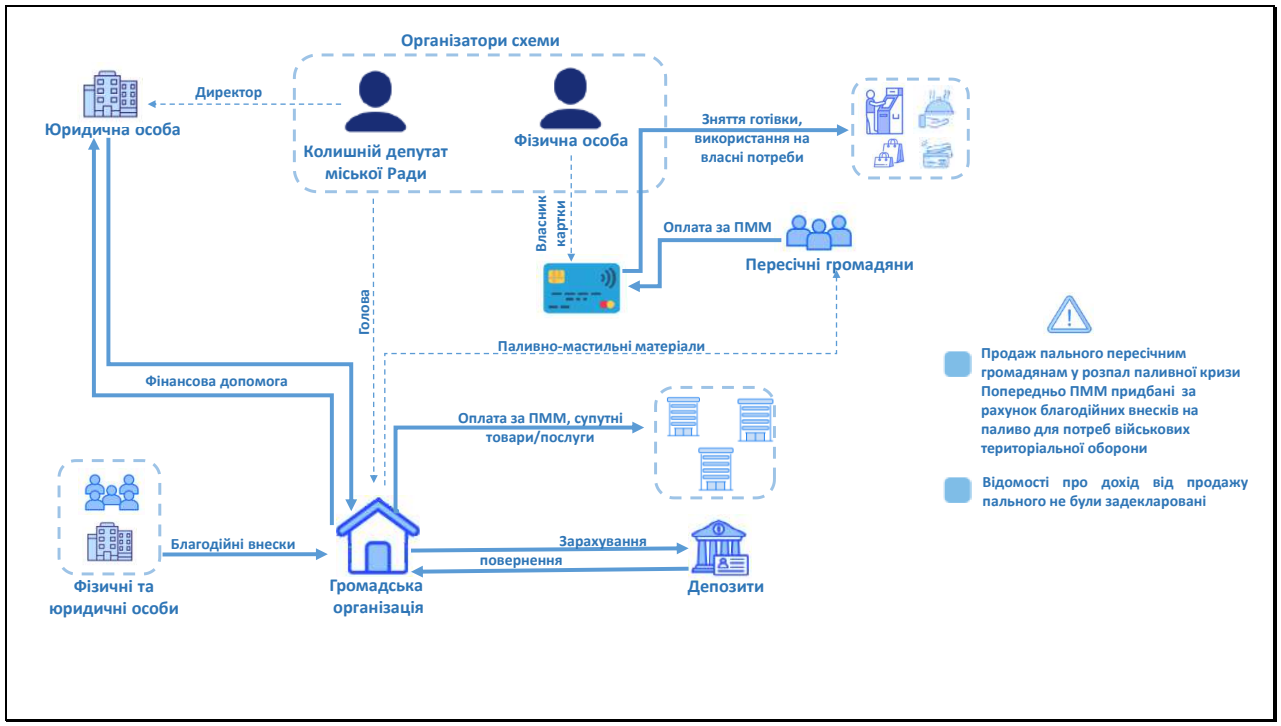
Зокрема, на рахунки **Громадської організації** надходили кошти як благодійні внески від фізичних та юридичних осіб, які мали бути спрямовані на придбання палива для потреб військових територіальної оборони. Натомість

лише половину з цих коштів було використано на оплату палива та супутніх товарів. Також кошти використовувалися на оплату товарів, робіт та послуг, циклічних операцій з розміщення та повернення депозитів, фінансової допомоги між **Громадською організацією** та пов'язаною з нею **Юридичною особою**.

Водночас під виглядом збору **Громадською організацією** благодійної допомоги, організаторами схеми залучено картку **фізичної особи**, на яку в період паливної кризи надходили кошти від значної кількості осіб як оплата за паливно-мастильні матеріали.

Отримані прибутки від продажу пального, були використано на власні потреби, частково зняті готівкою та розпорошено між власними платіжними картками.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2024.4.4.8. Використання афільованих суб'єктів господарювання для привласнення благодійних коштів та їх відмивання

Держфінмоніторингом з урахуванням інформації, отриманої від правоохоронного органу, виявлено схему, яка була направлена на привласнення та виведення грантів.

Відомо, що **Громадська організація** отримувала кошти виділені **Урядом Країни 1** для надання стипендії / фінансової допомоги учням /студентам.

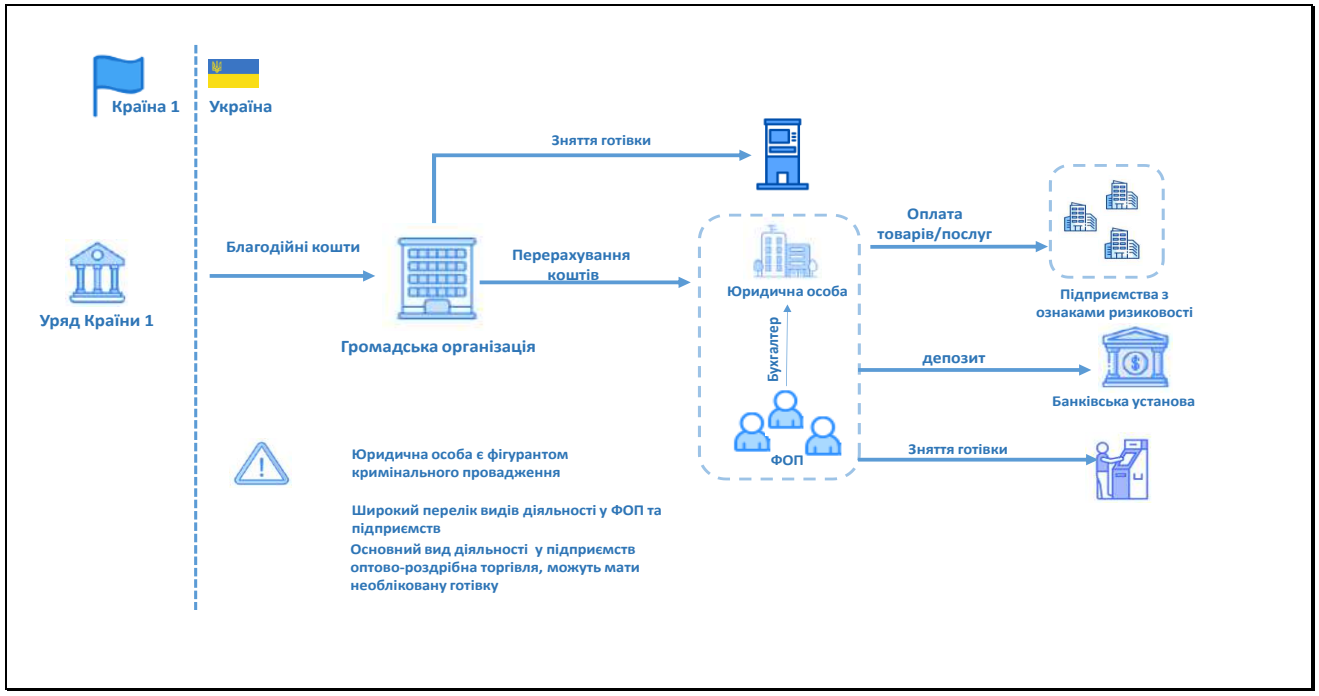
Встановлено, що основна частина **благодійних коштів** була використана **Громадською організацією** не за цільовим призначенням, а була **знята готівкою** та перенаправлена на користь **Юридичної особи** та **ФОП**ів які отримали цільові благодійні кошти без мети виконання своїх зобов'язань.

Слід зазначити, що один з **ФОП** також є бухгалтером **Юридичної особи**.

Надалі благодійні кошти частково перераховані на депозит з метою отримання неправомірного доходу, та перераховано на користь підприємств, основним напрямком діяльності яких, є оптово-роздрібна торгівля та які можуть мати необліковану готівку. Також підприємства мають ознаки створення юридичних осіб, що входять до схеми забезпечення та впровадження протиправного механізму діяльності, направленого на приховування джерел походження коштів, створення та впровадження схем з мінімізації сплати податків у значних розмірах, що може мати тяжкі економічні наслідки, а також є частиною легалізації коштів.

Крім того, **Юридична особа** є фігурантом кримінального провадження, за підозрою у заволодінні бюджетними коштами, підприємства та **ФОП**и мають широкий перелік видів діяльності, а одне з підприємств, на користь якого були зараховані благодійні кошти, визнано банкрутом.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2024.4.4.9. Заволодіння благодійних пожертв з використання НПО-клонів та фізичних осіб, підконтрольних одній особі

Держфінмоніторингом з урахуванням інформації, отриманої від правоохоронного органу, виявлено схему, яка була направлена на привласнення благодійних внесків.

З початку повномасштабної військової агресії росії **Фізична особа А** покинула територію України на підставі паспорта іноземної країни.

На території Країни 1 створив **Іноземну Благодійну організацію** з майже ідентичною до назви **Всеукраїнської Громадської організації**.

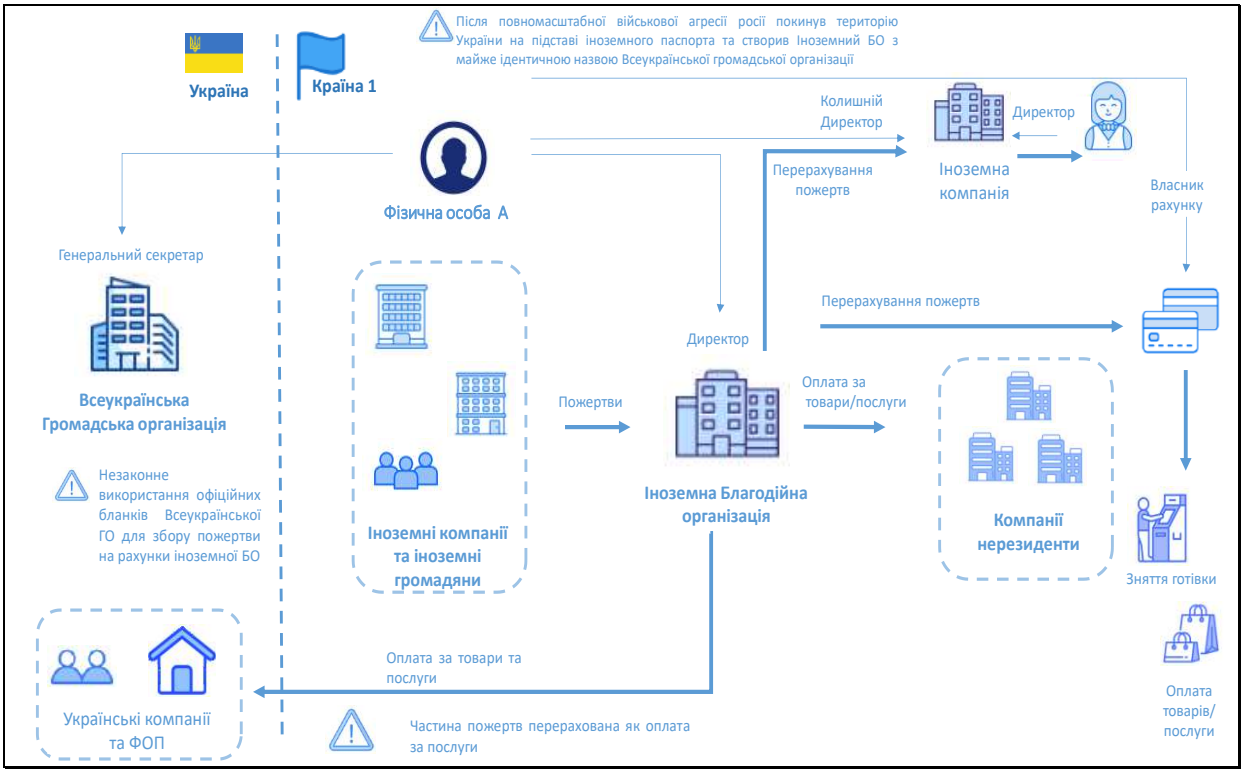
Відомо, що **Фізична особа А**, використовуючи офіційні бланки **Всеукраїнської громадської організації**, збирала пожертви на адресу **Іноземної Благодійної організації**.

Надалі, частину благодійних пожертв перераховано на користь юридичних осіб та ФОП, які знаходяться на території України, а також Компаніям-нерезидентам в якості оплати за товари/послуги. Частину пожертв направлено на рахунок **Іноземної компанії**, в якій **Фізична особа А** була директором. Також частину пожертв перераховано на рахунок **Фізичної особи А**.

В подальшому, **Фізичною особою А** частину коштів знято готівкою, а іншу частину витрачено для розрахунків за товари/послуги.

При цьому за весь період повномасштабного вторгнення на рахунки **Всеукраїнської громадської організації** не надходило жодних переказів від **Іноземної Благодійної організації**.

Правоохоронним органом здійснюється досудове розслідування.


Після повномасштабної військової агресії росії покинув територію України на підставі іноземного паспорта та створив Іноземний БО з майже ідентичною назвою Всеукраїнської громадської організації
Україна
Країна 1
Колишній Директор
Директор
Іноземна компанія
Перерахування пожертв
Власник рахунку
Фізична особа А
Генеральний секретар
Перерахування пожертв
Директор
Всеукраїнська Громадська організація
Пожертви
Оплата за товари/послуги
Іноземні компанії та іноземні громадяни
Іноземна Благодійна організація
Компанії нерезиденти
Незаконне використання офіційних бланків Всеукраїнської ГО для збору пожертви на рахунки іноземної БО
Зняття готівки
Оплата за товари та послуги
Оплата товарів/ послуги
Українські компанії та ФОП
Частина пожертв перерахована як оплата за послуги

РОЗДІЛ 4.5. ТРАНСКОРДОННЕ ВІДМИВАННЯ ДОХОДІВ

Ефективна зовнішньоекономічна діяльність є важливим фактором розвитку держав шляхом забезпечення надходження доходів від експортно-імпортних операцій, постачання різноманітних товарів та послуг, розвитку інноваційних виробництв. Визначено, що після початку великої війни Україна перебуває у надскладному становищі за всі роки незалежності: експорт товарної продукції скоротився майже вдвічі, а імпорт – втричі.

Війна внесла свої корективи в стратегічні питання міжнародної торгівлі, зокрема експорту та логістики. Відбулася динамічна переорієнтація зовнішньої торгівлі України на європейські ринки та нові логістичні маршрути, що суттєво пом'якшило обмеження, які наклало блокування агресором чорноморських морських портів. Проте, ця ситуація має і зворотний бік – скорочення або відсутність надходжень до банківських структур України валютного виторгу в повному обсязі.

За даними Національного банку України, обсяг експортної виручки, що надійшла в Україну за січень-червень 2024 року, перевершив результат за аналогічний період минулого року на 15,9%, або $3,3 млрд, тоді як розмір неповерненої валютної виручки тримається на колишньому рівні 7-8 млрд дол США.

Законодавчі зміни, які набули чинності в липні 2024 року передбачають посилений контроль за експортом зернових культур, вимогу реєстрації податкових накладних та впровадження нових митних правил тощо.

Проте, схеми вивозу продукції без надходження валютного виторгу залишались актуальними протягом поточного року. Також проблемними є схеми перерахування коштів за межі України без надходження товарів в повному обсязі, або надходження оплачених товарів неналежної якості – особливо в оборонному секторі.

Узагальнені типові приклади відмивання доходів в зовнішньоекономічній сфері наведено нижче.

Приклад 2024.4.5.1. Привласнення бюджетних коштів шляхом не виконання умов зовнішньоекономічних контрактів

Держфінмоніторингом з урахуванням інформації ПФР іноземних держав та правоохоронного органу виявлено фінансові операції, направлені на привласнення державних коштів іноземних компаній з ознаками фіктивності.

Встановлено, що **Державною установою** у сфері оборони було укладено зовнішньоекономічні договори з **Іноземною компанією** на постачання військової амуніції та здійснено 100% передоплату.

Типологічне дослідження «Ризики та загрози легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансування тероризму в умовах військової агресії російської федерації – 2024»

Товари військового призначення були поставлені неналежної якості за істотно завищеною вартістю та в неповній комплектації. Крім того, товари, згідно умов договорів та специфікацій до них, було поставлено з порушеннями термінів постачання та не в повному обсязі. При цьому, за даними банківської установи та митного органу інформація щодо митного оформлення ввезених товарів або повернення коштів на користь **Державної установи** від **Іноземної компанії** відсутня.

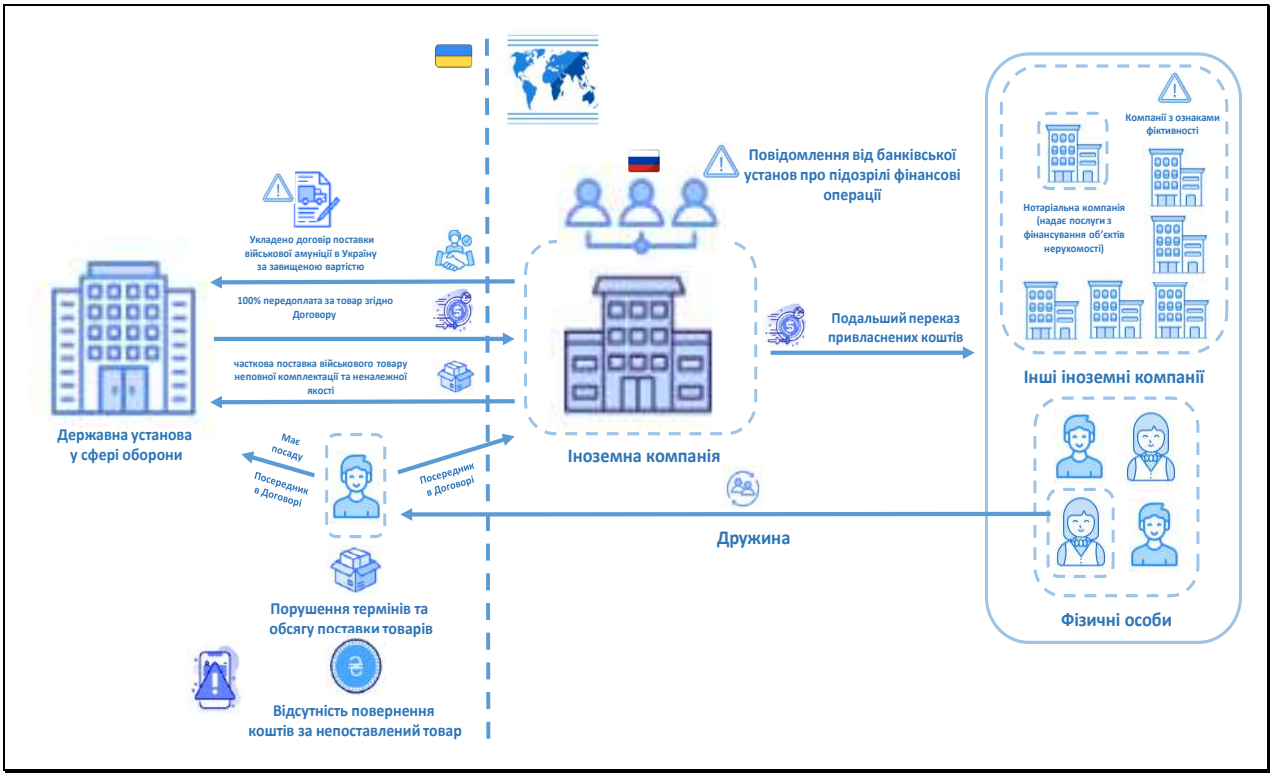
Встановлено, що надалі **Іноземною компанією** були здійснені перерахування **отриманих коштів** на користь інших іноземних компаній, серед яких є компанії з ознаками фіктивності (фігуранти розслідувань правоохоронних органів), а також компанія, яка надає послуги, пов'язані з фінансуванням в нерухомість, управлінням портфелем активів нерухомості.

Також встановлені перерахування коштів на користь ряду фізичних осіб, серед яких дружина **особи**, яка працює у **Державній установі** та виступала посередником при укладанні зовнішньоекономічних договорів.

Крім того, за даними з відкритих джерел, **Іноземна компанія** підконтрольна громадянам росії.

Таким чином, характер проходження фінансових потоків, починаючи з коштів отриманих від **Державної установи Іноземною компанією** за договорами по яких не здійснювалось постачання товарів та/або поставлявся товар неналежної якості та з порушенням термінів постачання, ймовірно спрямоване на привласнення державних коштів за допомогою **Іноземної компанії** та їх відмивання.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2024.4.5.2. Ухилення від сплати податків шляхом відшкодування ПДВ за експорт товарів, розрахунки за які на територію України не надійшли, з використанням посередників та зворотного імпорту

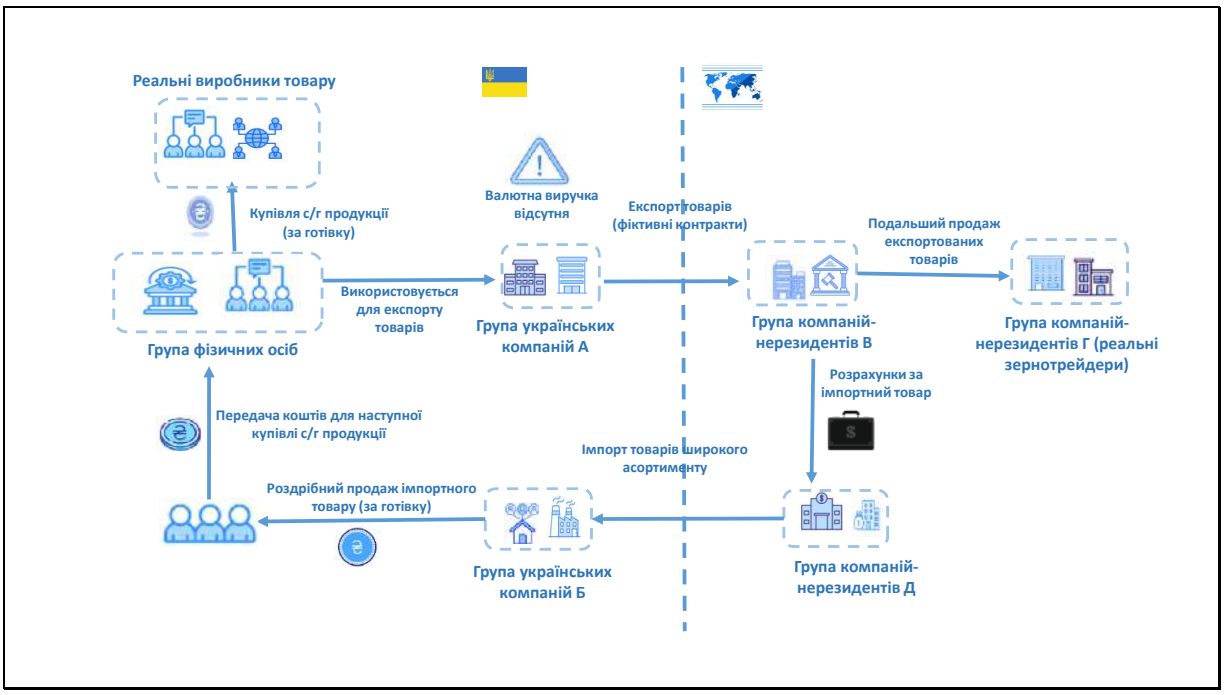
Держфінмоніторингом виявлено схему отримання юридичними та фізичними особами незаконних доходів від ухилення сплати податків при здійсненні експортно-імпортних операцій.

Встановлено, що **Група фізичних осіб** здійснювала на території України закупівлю сільськогосподарської продукції у **Реальних виробників** (переважно за готівку), експортувала її через **Групу українських компаній А** за спрощеною процедурою експорту на підставі контрактів, які можуть мати ознаки фіктивності, на користь **Групи компаній-нерезидентів В**, яка, в свою чергу, реалізувала зазначені товари на користь реальних зернотрейдерів – **Групу компаній-нерезидентів Г,** при цьому розрахунки відбувались за межами України.

Група компаній-нерезидентів В не перерахувала валютну виручку на користь **Групи українських компаній А** за експортований товар, проте використала кошти для розрахунків за товари широкого асортименту, які **Група компаній-нерезидентів Д** поставила в Україну на користь **Групи українських компаній Б**. Надалі зазначені товари реалізовано здебільшого за готівку на ринках, в інших місцях роздрібної торгівлі, отримані при цьому кошти передано **Групі фізичних осіб** для наступної закупівлі сільськогосподарської продукції.

Таким чином, **Групою невстановлених осіб** здійснено готівкові розрахунки з реальними українськими виробниками сільськогосподарської продукції за рахунок готівкових коштів, отриманих нею від продажу товарів широкого асортименту, які імпортовано в Україну. Метою зазначеної схеми є ухилення від сплати податків.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2024.4.5.3. Незаконне виведення коштів за межі України за фіктивними контрактами

Держфінмоніторингом з урахуванням інформації правоохоронного органу виявлено схему, пов'язану з наданням незаконних послуг з виведення коштів за межі України на користь **Іноземних компаній**, власниками яких є громадяни України, на підставі зовнішньоекономічних контрактів, без постачання відповідної продукції на територію України.

Встановлено, що **Групою компаній Б** (професійна мережа з відмивання коштів) було безпідставно перераховано кошти на користь **Іноземних компаній** під виглядом попередньої оплати за фактично непоставлений товар (промислове та електрообладнання, текстиль та взуття) згідно з укладеними фіктивними зовнішньоекономічними контрактами.

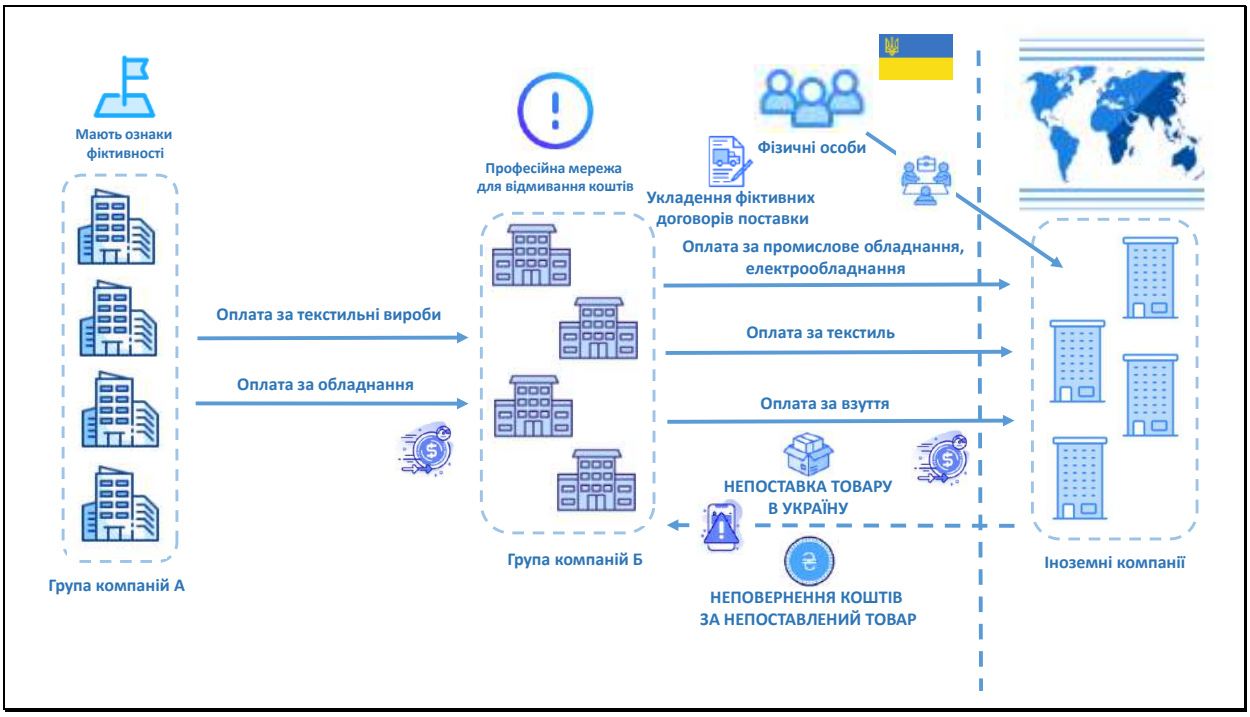
При цьому, зовнішньоекономічні контракти містять ознаки підробки (неоднакова висота та ширина літер, проміжків між словами, містяться помилки в тексті, печатка не має форми та відтиску, підписи учасників договору схожі на скопійовані фото).

Джерелом походження коштів були зарахування як оплата за текстильні вироби та обладнання від **Групи компаній А**, основними з яких є компанії з ознаками фіктивності (нещодавно зареєстровані компанії, мають спільний посадово-засновницький склад та адресу, незначний статутний капітал, однакову IP-адресу, за короткий проміжок часу існування компаній відбулася зміна КБВ та адреси).

Слід зазначити, що кошти за фактично непоставлений товар не було повернуто **Іноземними компаніями** на користь **Групи компаній Б**.

Зазначене може свідчити про здійснення схемних операцій, спрямованих на мінімізацію/ухилення від сплати податкового зобов'язання до державного бюджету, а також легалізації коштів, виведених за фіктивними зовнішньоекономічними договорами.

Правоохоронним органом здійснюється досудове розслідування.



РОЗДІЛ 4.6. ВИКОРИСТАННЯ ГОТІВКОВИХ КОШТІВ

Готівкові кошти створюють можливості для проведення непрозорих операцій поза межами фінансової системи. Особливо в умовах військової агресії внаслідок об'єктивних причин сфера використання готівки набуває значного поширення, оскільки, саме готівка є основним інструментом для ВК/ФТ. Більшість операцій із застосуванням готівки завжди розглядаються як такі, що містять високі ризики і потребують аналізу на всіх відкритих етапах проходження коштів.

Використання готівкових коштів для ФТ. В умовах військової агресії готівкові кошти можуть використовуватись для підтримки терористичних організацій через неформальні фінансові канали та контрабанду готівки.

Фізичне переміщення готівки є одним із способів, за допомогою яких терористи можуть переміщувати кошти в обхід контрольних заходів. У разі перехоплення транскордонного переміщення готівки, визначення походження і кінцевого призначення перехоплених коштів може бути ускладнено. Залучення невеликих обсягів готівки для ФТ також є чинником, який ускладнює виявлення та перехоплення таких активів.

В умовах відкритої збройної агресії з боку росії готівкові кошти можуть використовуватись для фінансування терористичних актів, диверсій, колаборційної та сепаратистської діяльності тощо. Крім того, набула поширення схема переведення в готівку коштів осіб, які знаходяться на тимчасово окупованих територіях, через рахунки (термінали) фіктивних фізичних осіб – підприємців.

Використання готівкових коштів для ВК. Доходи від незареєстрованої, прихованої підприємницької, забороненої, злочинної діяльності також значною мірою акумулюються в готівковій формі. Надалі, такі кошти можуть використовуватись як для подальшого фінансування незаконної діяльності та придбання матеріальних цінностей, так і для надання винагороди за незаконно надані послуги.

Також, враховуючи значну кількість внутрішньо переміщених осіб в Україні, поширене використання необлікованої готівки для виплати неофіційної заробітної плати.

Популярність використання готівки в різноманітних схемах, як і раніше, обумовлена складнощами її виявлення та відстеження переміщення між учасниками схеми.

Узагальнені типові приклади відмивання злочинних доходів, використовуючи готівку, наведено нижче.

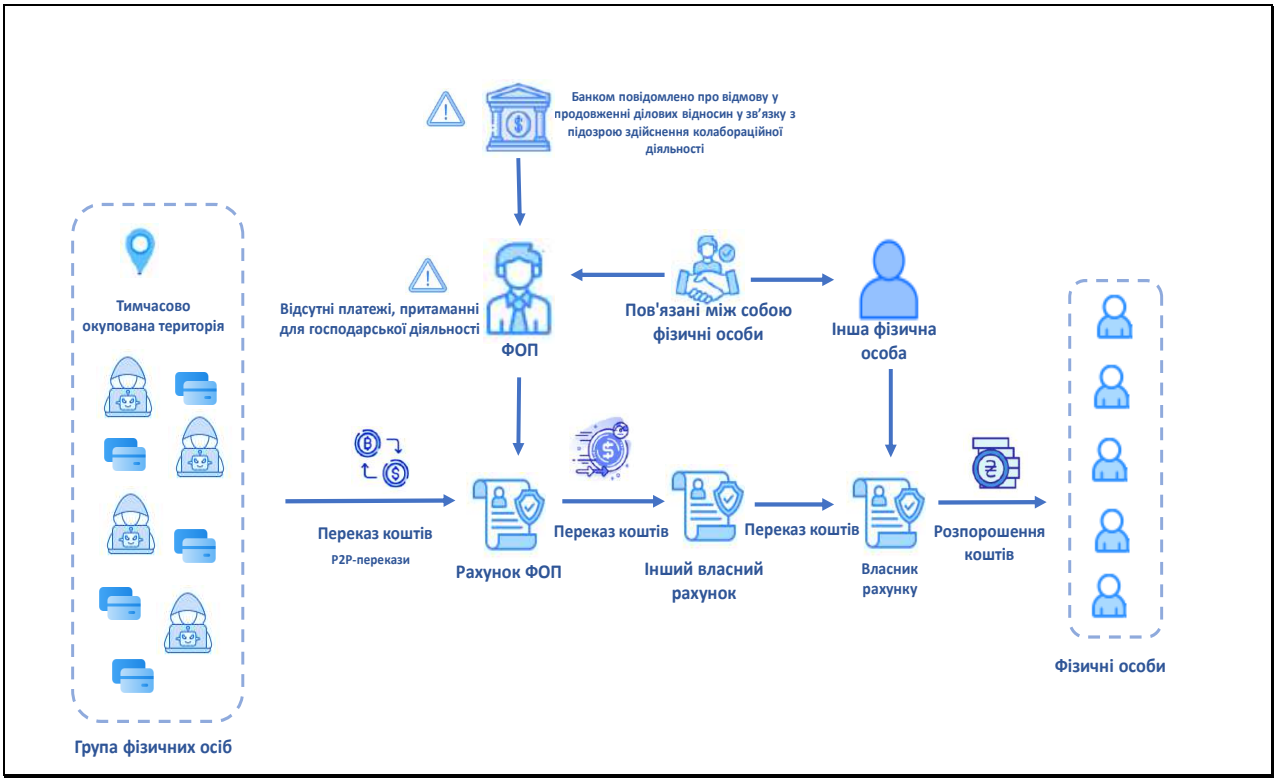
Приклад 2024.4.6.1. Конвертації безготівкової гривні у готівковий російський рубль на тимчасово окупованих територіях

Держфінмоніторингом виявлено схему фінансових операцій із використанням еквайрингових розрахунків через POS-термінал на тимчасово окупованій території, ймовірно, з метою конвертації гривні у готівку.

В ході аналізу встановлено, що на рахунок **ФОП** через транзитний рахунок перераховано кошти від **Групи фізичних осіб** – власників платіжних карток, зареєстрованих на тимчасово окупованих територіях, під виглядом оплати за товари чи послуги з подальшим перерахуванням на власний рахунок фізичної особи. При цьому можливо припустити, що таким чином **ФОП** надає послуги з отримання готівки, а також обмін безготівкової гривні на готівковий російський рубль.

Частину отриманих коштів надалі перераховано на користь **Іншої фізичної особи**, пов'язаної з **ФОП**, яка, своєю чергою, їх розпорошує на користь третіх фізичних осіб. Варто зазначити, що банківською установою відмовлено у продовженні ділових відносин з **ФОП** у зв'язку з підозрою у вчиненні колабораційної діяльності та посібництві державі-агресору.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2024.4.6.2. Ухилення від сплати податків та прихованого конвертування

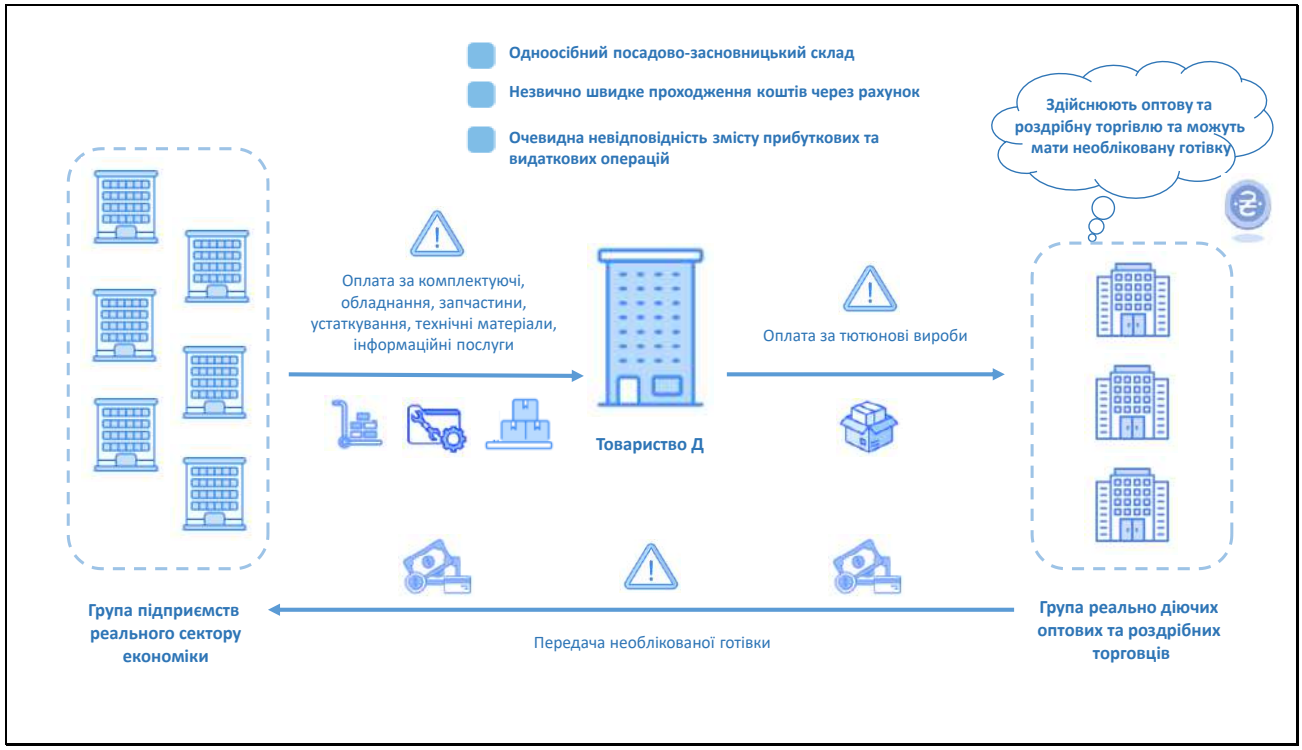
Держфінмоніторингом виявлено схему, пов'язану з наданням незаконних послуг групі компаній, щодо ухилення від сплати податків, легалізації доходів, зокрема, через «приховану конвертацію» безготівкових коштів в готівкові з використанням реально діючих оптових та роздрібних торговців.

Так, встановлено, що **Товариство Д** з ознаками фіктивності виконувало функцію транзитного підприємства для переміщення коштів та формування податкових накладних. На його рахунок зараховувались кошти від **Групи підприємств** різноманітного призначення в якості оплати за комплектуючі, обладнання, запчастини, устаткування, технічні матеріали, інформаційні послуги тощо. Надалі кошти перераховувались з іншими призначеннями в якості оплати за тютюнові вироби на користь **Групи реально діючих оптових та роздрібних торговців**, які можуть мати необліковану готівку.

По рахунку **Товариства Д** спостерігалось незвично швидке проходження коштів, а також очевидна невідповідність змісту прибуткових та видаткових операцій. Тобто, йде мова про ознаки загальновідомої схеми «товарів» у скрутках, що використовується для ухилення від сплати податків та відмивання коштів.

Тобто, **Товариство Д** надавало незаконні послуги з формування податкового кредиту підприємствам реального сектору економіки, сприяло ухиленню від сплати податків з використанням механізму «товарів» у скрутках та «прихованій конвертації» безготівкових коштів у готівку.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2024.4.6.3. Організація переведення безготівкових коштів у готівку

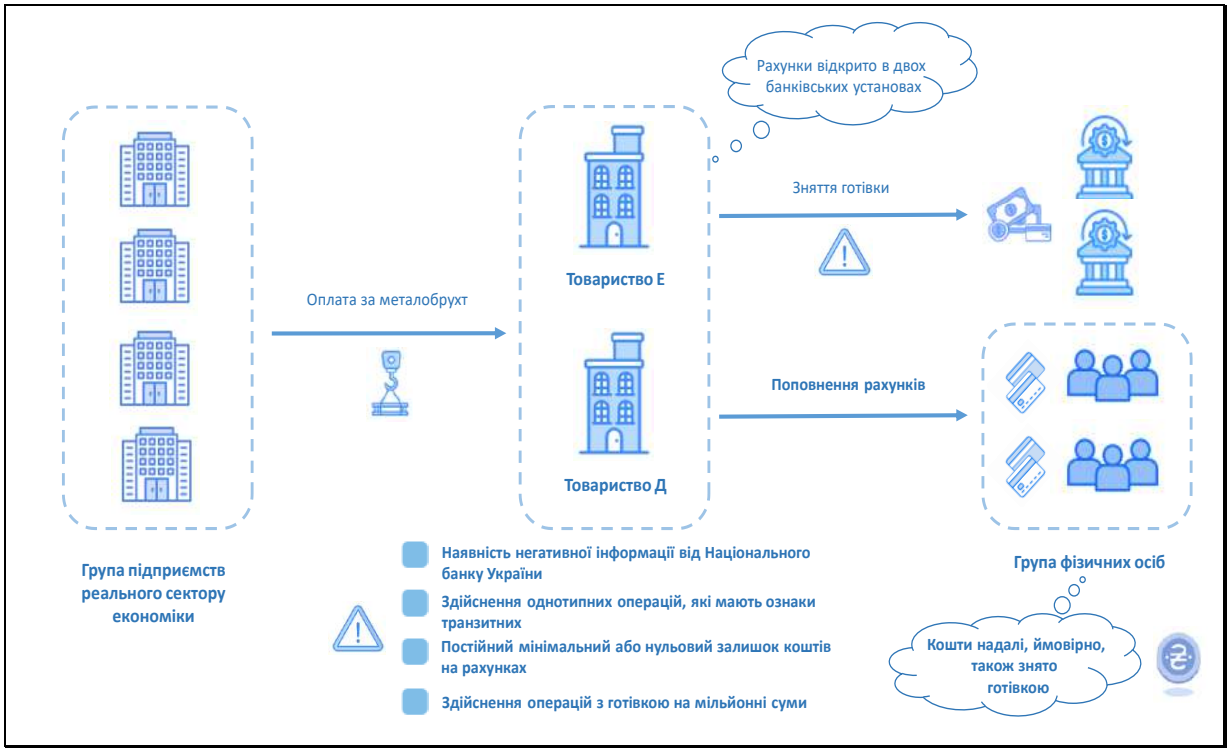
Держфінмоніторингом виявлено схему спрямовану на переведення безготівкових коштів у готівку. Так, Національним банком України надано інформацію щодо виявлення підозрілих операцій двох клієнтів – **Товариства Е** та **Товариства Д** при здійсненні нагляду за діяльністю банківської установи.

Держфінмоніторингом за результатами подальшого аналізу встановлено, що на рахунки **Товариства Е** та **Товариства Д**, відкриті у двох банківських установах, зараховувались кошти від **Групи підприємств** під виглядом оплати за металобрухт. Надалі значна частина коштів знімалась готівкою через каси банківських установ, а решта перераховувалась на особисті рахунки **Групи фізичних осіб**. З рахунків фізичних осіб безготівкові кошти надалі також переводились в готівку або перераховувались на рахунки фізичних осіб.

Привертає увагу, що по рахунках **Товариства Е** та **Товариства Д** проводились однотипні операції, які мають ознаки транзитних. При цьому при здійсненні операцій з готівкою на мільйонні суми спостерігався постійний мінімальний або нульовий залишок коштів на рахунках.

Тобто з використанням рахунків **Товариства Е** та **Товариства Д** та особистих рахунків **Групи фізичних осіб**, здійснюється переміщення коштів та формування валових витрат суб'єктів господарювання реального сектору економіки для ухилення від сплати податків та «конвертації» безготівкових коштів у готівку.

Правоохоронним органом здійснюється досудове розслідування.



РОЗДІЛ 4.7. ВІДМИВАННЯ ДОХОДІВ ВІД НЕЗАКОННОГО ЗАВОЛОДІННЯ КУЛЬТУРНИМИ ЦІННОСТЯМИ

Незаконний обіг культурних цінностей є загальносвітовою проблемою та, як відмічають експерти, набуває особливих масштабів в регіонах, що постраждали від збройних конфліктів та стихійних лих.

В нинішніх умовах російської агресії, збереження культурної спадщини є одним з найважливіших чинників забезпечення національної безпеки України, консолідації суспільства та формування спільної національної історичної пам'яті.

Незаконний обіг культурних цінностей охоплює крадіжки з музейних установ або приватних колекцій, розграбування археологічних пам'яток, виготовлення підробок, а також незаконне переміщення об'єктів матеріальної культури внаслідок війни.

Торгівля культурними цінностями найчастіше має міжнародний характер та може бути пов'язана з відмиванням злочинних доходів, організованою злочинністю та тероризмом. Для розрахунків використовуються як традиційні інструменти (готівка), так і більш прогресивні новітні технології (p2p-перекази, онлайн-платежі, криптовалютні перекази тощо).

В свою чергу, боротьба з незаконним обігом культурних цінностей вимагає специфічних знань та досвіду використання міжнародно-правових інструментів, у тому числі їх практичної реалізації.

Узагальнені типові приклади відмивання злочинних доходів від незаконного заволодіння культурними цінностями наведено нижче.

Приклад 2024.4.7.1. Незаконне заволодіння та переміщення за межі України, з метою подальшої реалізації, об'єктів матеріальної культури

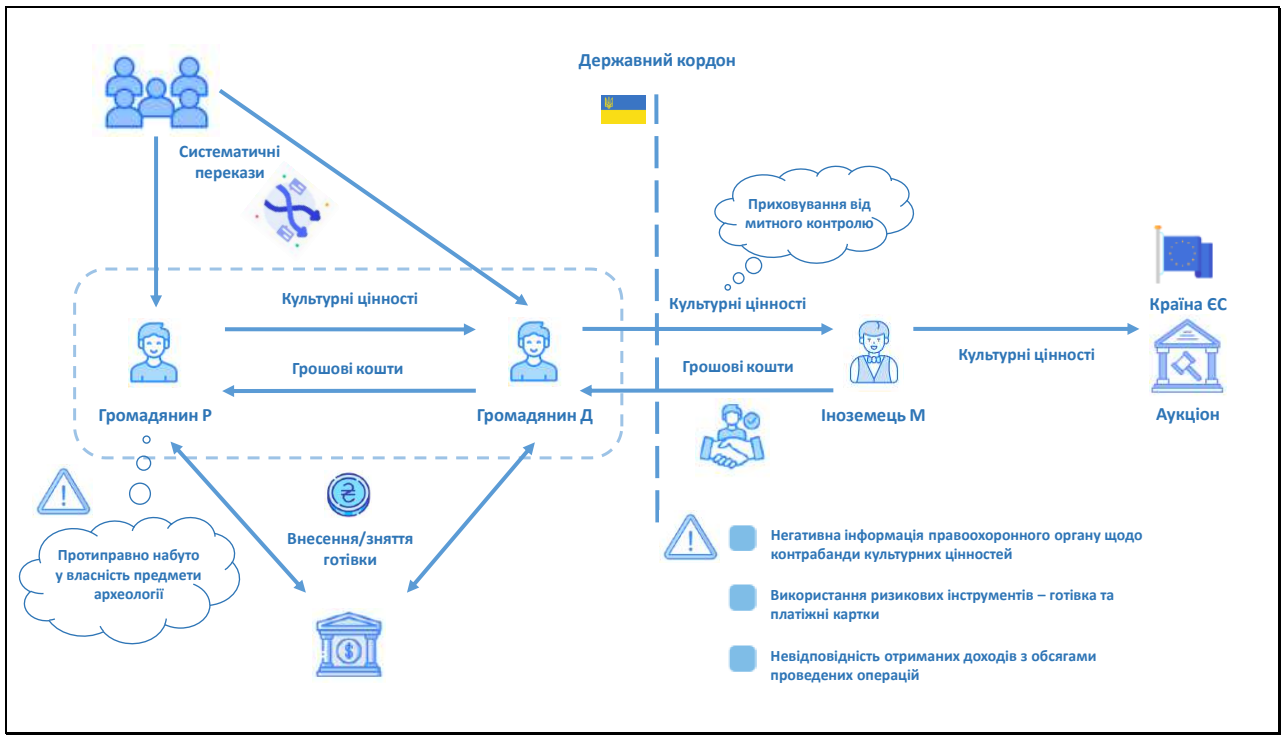
Держфінмоніторингом, з врахуванням інформації отриманої від правоохоронного органу, виявлено підозрілі фінансові операції **Групи фізичних осіб**, які причетні до незаконного заволодіння та переміщення за межі митного кордону України (з приховуванням від митного контролю) культурних цінностей.

За інформацією правоохоронного органу **Громадянином Р** протиправно, в порушення вимог чинного законодавства про охорону культурної спадщини, набуто у власність предмети археології. Надалі зазначені цінності через електронний аукціон були реалізовані **Громадянином Р** на користь **Громадянина Д**, який перетнув держаний кордон України та перемістив, з приховуванням від митного контролю, культурні цінності до країни Європейського союзу з подальшою реалізацією на користь **Іноземця М**.

Культурні цінності, надалі, були розміщені на іноземному аукціоні для подальшого перепродажу.

Держфінмоніторингом, за результатами аналізу виявлено відповідні фінансові потоки, зокрема пов’язані з отриманням коштів від значної кількості осіб з використанням різних платіжних систем, що може бути пов’язане з прихованим розрахунком за культурні цінності, а також внесенням/зняттям готівки. Обсяг таких операцій не відповідає офіційно отриманим/задекларованим доходам.

Правоохоронним органом здійснюється досудове розслідування.



РОЗДІЛ 4.8. ВІДМИВАННЯ ДОХОДІВ, ОТРИМАНИХ ВІД ШАХРАЙСЬКИХ ДІЙ ТА КІБЕРЗЛОЧИНІВ

У 2023-2024 році в Україні шахрайські дії та кіберзлочини залишаються важливою проблемою. Під час війни шахраї використовують вразливість громадян, їх складний психоемоційний стан та матеріальні труднощі.

Найбільш розповсюдженими залишається шахрайство при купівлі чи продажу товарів в Інтернеті, злам акаунтів в соціальних мережах, шахрайські інвестиційні проєкти, використання фішингових посилань, а також виманювання персональної та банківської інформації з використанням методів соціальної інженерії. При цьому жертвами шахраїв найчастіше стають найменш фінансово обізнані особи – молодь та особи похилого віку. Основною причиною шахрайства залишається соціальна інженерія, а саме збитки спричинені розголошенням клієнтами чутливих даних.

Отримані шахрайським шляхом кошти найчастіше транзитом проходять через рахунки значної кількості залучених осіб (дропів), а на кінцевому етапі переводяться в готівку або криптовалюту.

Узагальнені типові приклади відмивання злочинних доходів від шахрайських дій та кіберзлочинів наведено нижче.

Приклад 2024.4.8.1. Вимагання коштів групою осіб

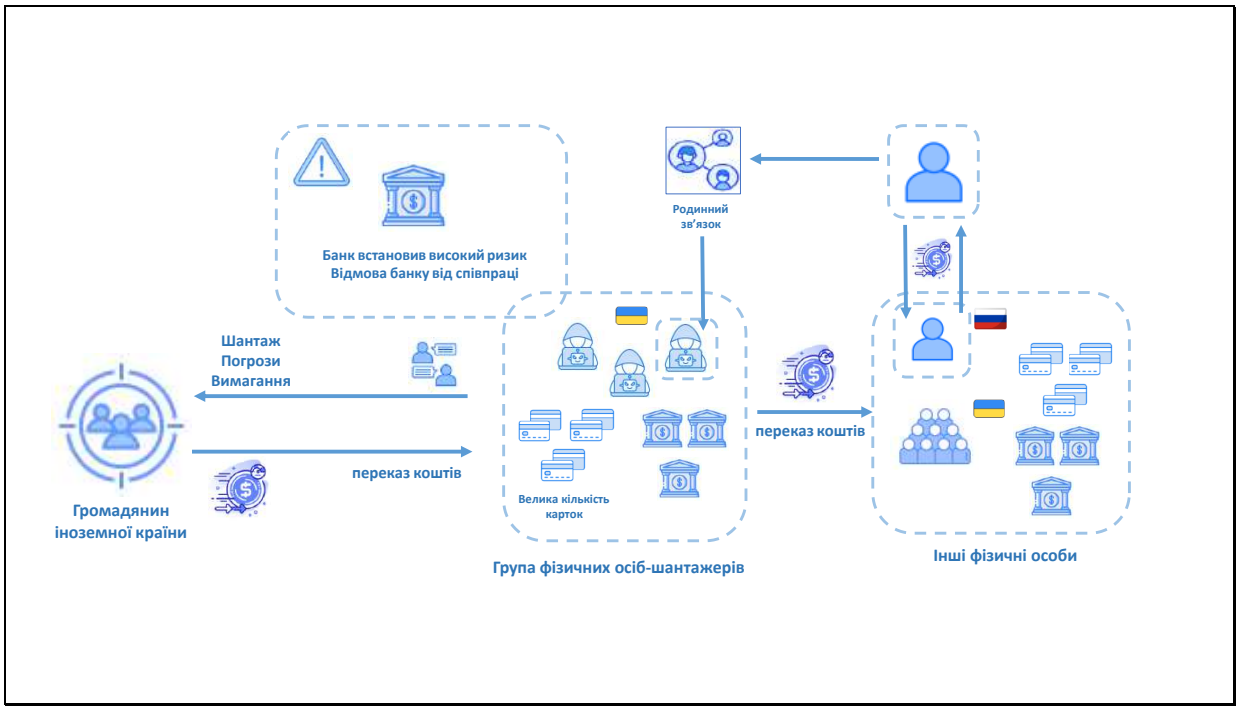
Держфінмоніторингом, з урахуванням інформації, отриманої від ПФР іноземних держав та СПФМ, виявлено шахрайську схему заволодіння коштами фізичної особи шляхом вимагання.

Під час аналізу встановлено, що **Громадянин** іноземної країни став жертвою шантажу та вимагання коштів з боку **групи фізичних осіб** – шантажистів, яке полягало у погрозах поширення його приватних фотографій публічно у випадку несплати коштів на платіжні картки, емітовані українськими банківськими установами. Крім того, шантажисти мали велику кількість рахунків, відкритих в банківських установах.

Під тиском шантажу **Громадянин** переказав кошти на карткові рахунки групи осіб. Згодом ці кошти були переведені на інші картки, одним із власників яких є громадянин росії, що проживає в Україні.

Встановлено, що **фізичні особи** проводили неодноразові перекази коштів на рахунки одного і того ж **уродженця росії**, а останній перерахував їх **особі**, яка є родичем одного з **групи фізичних осіб**.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2024.4.8.2. Шахрайство з використанням викрадених платіжних карток

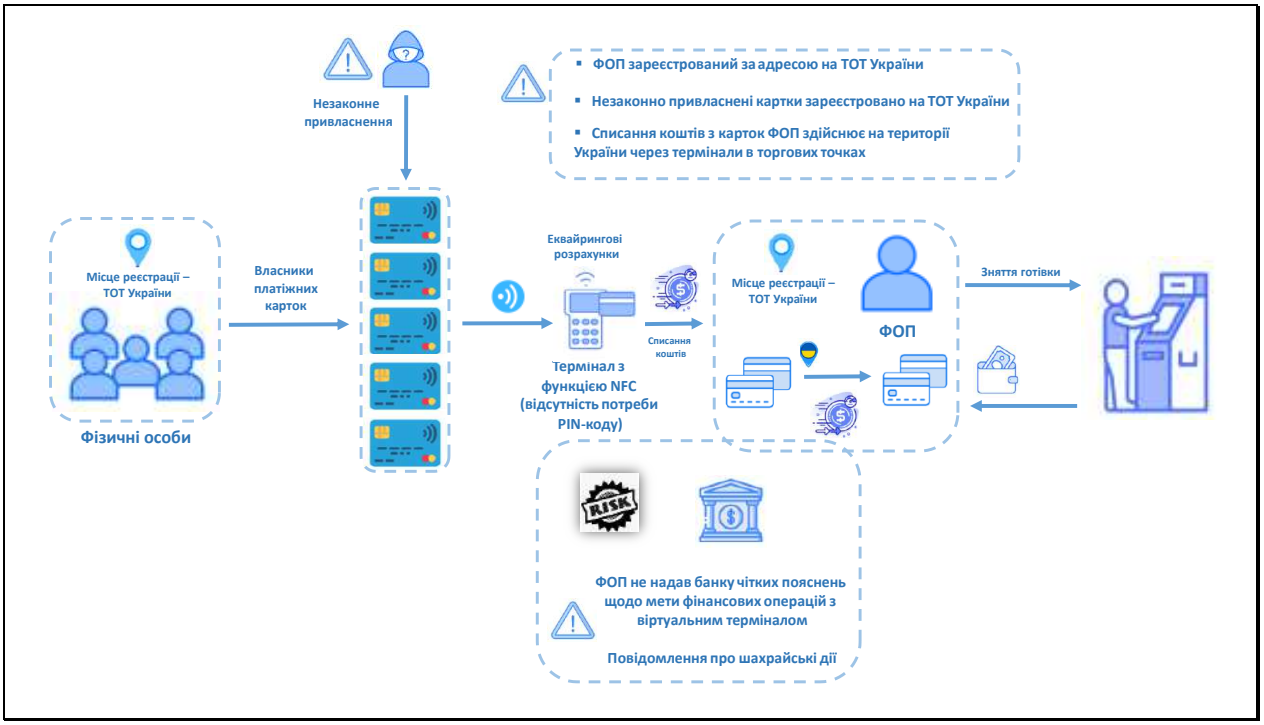
Держфінмоніторингом виявлено схему шахрайських фінансових операцій з викраденими платіжними картками осіб, що зареєстровані на тимчасово окупованих територіях, з метою їх привласнення та сприяння у відмиванні доходів, одержаних злочинним шляхом.

Встановлено, що з карток фізичних осіб було списано кошти за допомогою торгових точок **фізичної особи-підприємця**, зареєстрованої на тимчасово окупованій території України, які обладнані віртуальним терміналом, що має функцію NFC та дозволяє проводити оплати карткою без введення PIN-коду. Фінансові операції (спроба їх здійснення) зі списання коштів з рахунку проводились методом неодноразового підбору округлених сум, що свідчить про те, що особи не знали наявні залишки коштів на рахунках. Кошти зараховувались на рахунок **ФОП** у вигляді відшкодування (еквайрингові розрахунки) від фізичних осіб на великі, рівні суми з підбором суми оплати за короткий проміжок часу.

Фізичні особи - власники карток, з яких були проведені зазначені операції зі списання коштів, зареєстровані за місцем проживання на тимчасово окупованій території України. При цьому, **ФОП** на момент проведення зазначених фінансових операцій перебував за адресою на території підконтрольній Україні.

Надалі кошти, зараховані на рахунок **ФОП**, було перераховано на картковий рахунок, відкритий **ФОП**, для подальшого обготівковування. **ФОП** не надав банку чітких пояснень щодо мети проведення операцій з використанням віртуального терміналу.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2024.4.8.3. Шахрайське заволодіння державними коштами

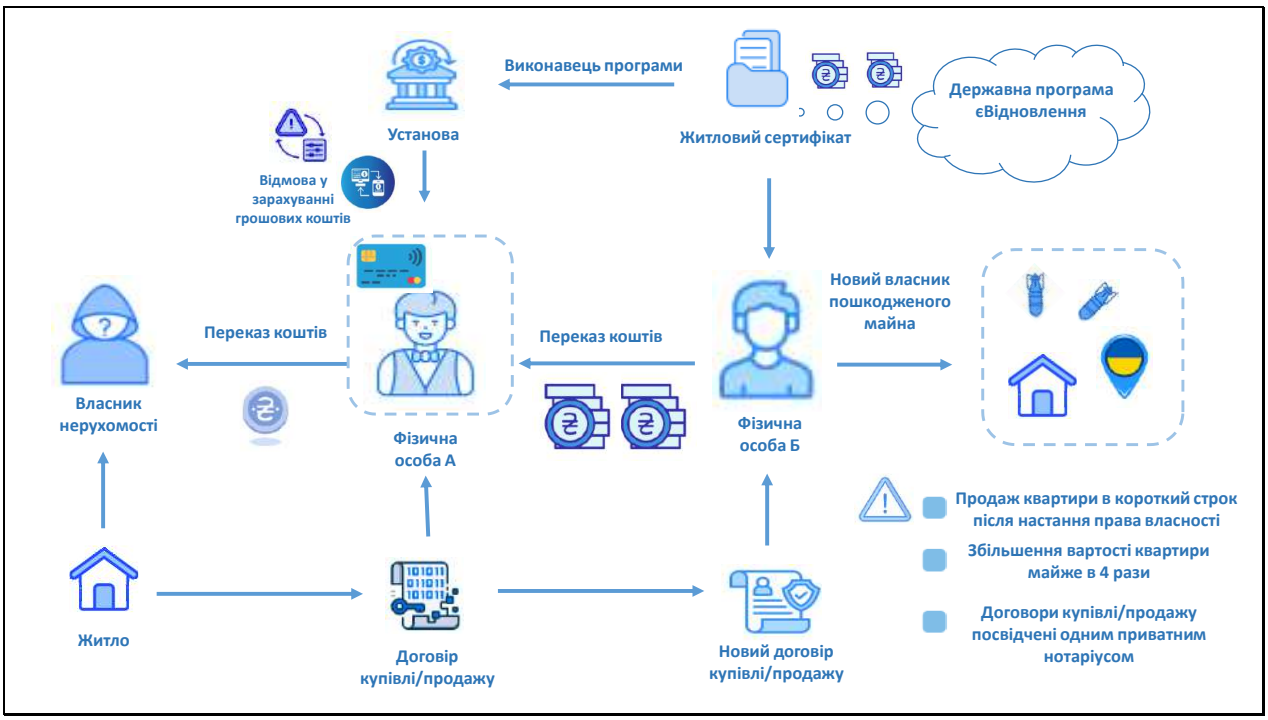
Держфінмоніторингом виявлено схему щодо спроби заволодіння державними коштами при здійсненні операцій з купівлі-продажу нерухомого майна за завищеною ціною.

Встановлено, що **Фізичною особою А** було придбано квартиру, яку через короткий проміжок часу (10 днів) було продано **Фізичній особі Б** за ціною, яка в 4 рази перевищує попередню вартість придбання. Варто зазначити, що обидва договори купівлі-продажу нерухомості посвідчені одним і тим же нотаріусом.

Відомо, що **Фізична особа Б** є учасником державної програми «єВідновлення» за кошти, передбачені державною програмою з відшкодування збитків за зруйноване чи пошкоджене житло внаслідок військових дій, та має житловий сертифікат на суму, зазначену в новому договорі купівлі-продажу нерухомості. Вартість квартири була завищена порівняно з ринковими цінами для отримання завищеної суми грошової компенсації.

Враховуючи наявність підозр у проведені сумнівних фінансових операцій, банківською установою було відмовлено у зарахуванні державних коштів на рахунок **Фізичної особи**.

Правоохоронним органом здійснюється досудове розслідування.



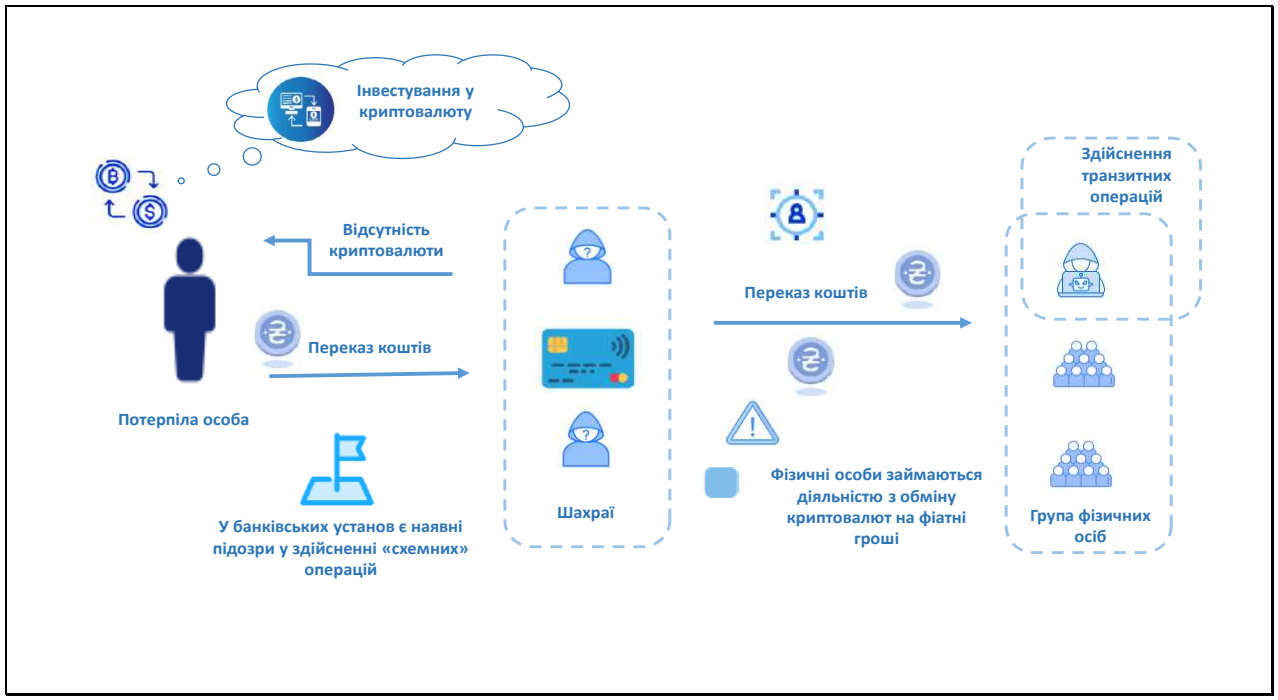
Приклад 2024.4.8.4. Шахрайство з використанням псевдоінвестування

Держфінмоніторингом з урахуванням інформації, отриманої від правоохоронного органу, виявлено схему шахрайського заволодіння грошовими коштами фізичної особи шляхом зловживання довірою з наступною їх легалізацією на користь ряду фізичних осіб.

Встановлено, що **Потерпіла особа** прийняла пропозицію невідомої особи заробити пасивний дохід шляхом інвестування коштів у криптовалюту та перерахувала кошти на карту, номер якої їй надали шахраї. Проте обіцяної криптовалюти не отримала.

Надалі кошти у день їх зарахування транзитом було перераховувано на рахунки **Групи фізичних осіб**, зокрема особі, яка раніше вже була залучена до здійснення транзитних фінансових операціях. За наявною інформацією ці фізичні особи займаються діяльністю з обміну криптовалюти на фіатні гроші, проте не мають офіційно задекларованих доходів.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2024.4.8.5. Шахрайство шляхом пропозиції отримання подарунка

Держфінмоніторингом з урахуванням інформації правоохоронного органу виявлено схему шахрайського заволодіння грошовими коштами фізичних осіб шляхом обману чи зловживання довірою під приводом надсилання коштовного подарунку при умові оплати митного збору.

Встановлено, що **Потерпілі особи** (громадяни України, пенсіонери) через особисті сторінки у соціальній мережі отримали від **Фізичної особи** – громадянина іноземної країни пропозицію отримати коштовний подарунок, проте для цього потрібно сплатити митний платіж.

Для можливості сплати митного платежу **Потерпілими особами** було перераховано кошти на картку, емітовану іноземним банком, на ім’я цієї **Фізичної особи**.

Встановлено, що пропозиція надійшла з соціальної сторінки особи, яка використовує підроблені світлини та має негативні відгуки від інших потерпілих осіб про випадки та спроби шахрайства, а саме: неодноразові прохання про допомогу з придбанням певних товарів або оплати логістичних витрат на відправку неіснуючих коштовних подарунків.

Правоохоронним органом здійснюється досудове розслідування.

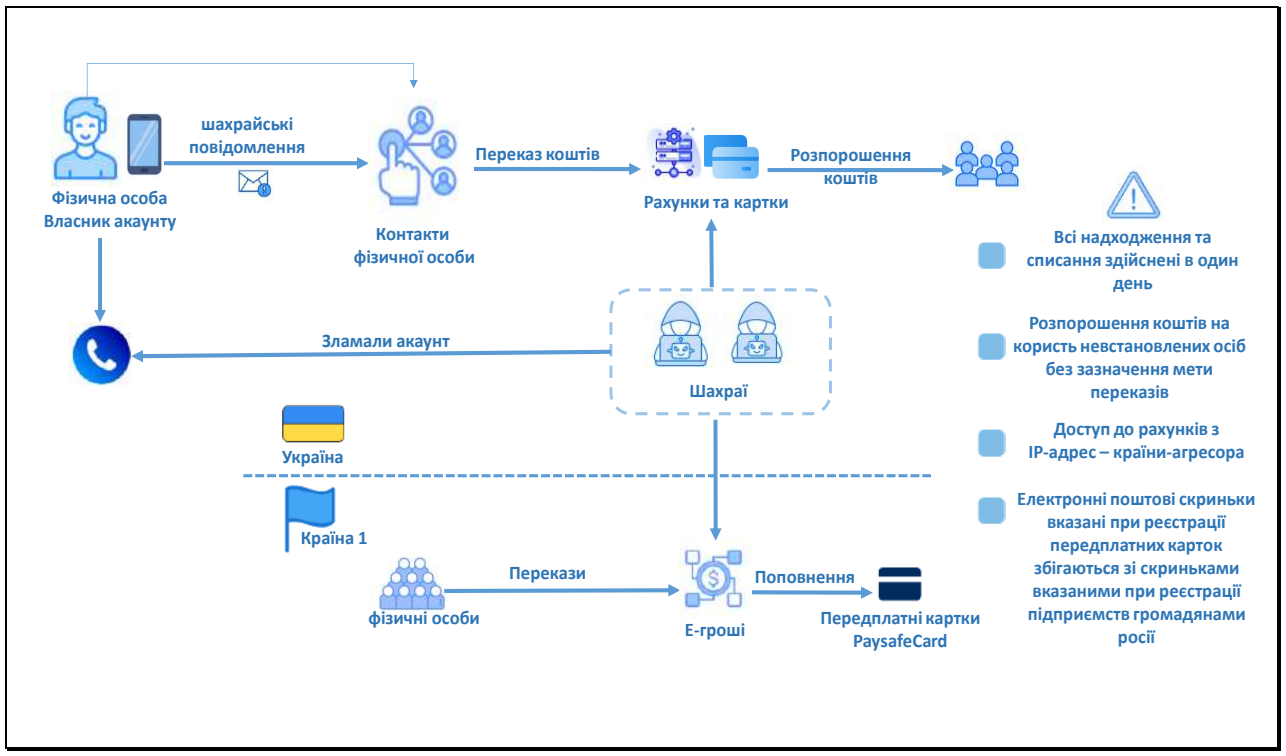
Приклад 2024.4.8.6. Шахрайство з викраденими даними

Держфінмоніторингом з урахуванням інформації, отриманої від ПФР іноземної держави, виявлено схему з шахрайського заволодіння коштами фізичних осіб та ймовірного фінансування тероризму.

Встановлено, що **Шахраї** зламали акаунт **Фізичної особи** та розіслали іншим **фізичним особи, що були у списку її контактів** повідомлення з проханням терміново позичити кошти. Протягом дня на рахунки **шахраїв** надходили кошти, які надалі того ж дня були розпорошені на користь невстановлених осіб без зазначення мети переказу.

Крім того, на рахунки **шахраїв** у Країні 1 надходили е-кошти від різних осіб з використанням міжнародних платіжних систем та надалі спрямовувались на поповнення **Передплатних карток PaysafeCard**. Деякі **Передплатні картки PaysafeCard** прив'язані до поштових скриньок, які зазначались при реєстрації індивідуальних підприємств громадянами російської федерації. Також, доступ до рахунків **шахраїв**, що відкриті в Країні 1, здійснювався через IP-адресу, яка знаходиться на території країни-агресора.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2024.4.8.7. Заволодіння грошовими коштами фізичних осіб з використанням дропів

Держфінмоніторингом виявлено ознаки підозрілої фінансової діяльності **Подружжя Н**, пов'язаної з проведенням схемних/транзитних операцій, використанням новітніх технологій/віртуальних активів, наявністю ознак «дропів», шахрайським заволодінням грошовими коштами фізичних осіб з наступною їх легалізацією шляхом переказу на платіжні картки інших банків.

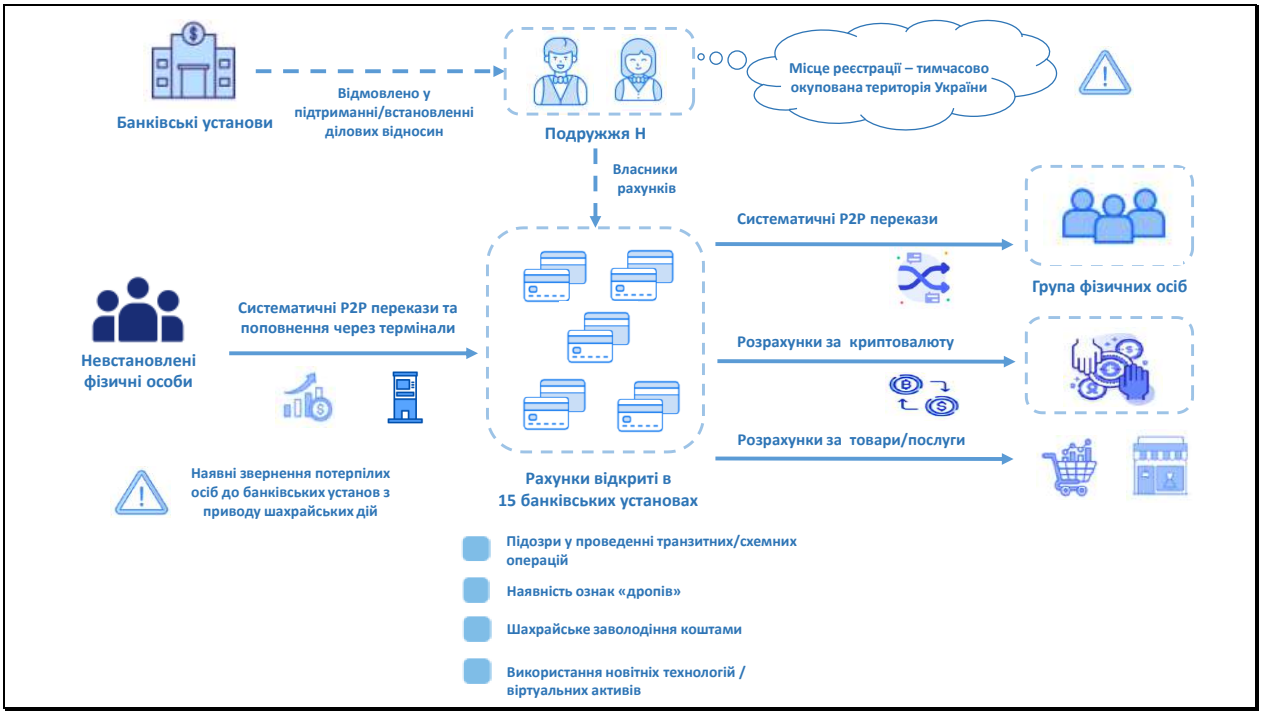
За інформацією ряду банківських установ, щодо підозрілої діяльності **Подружжя Н** надійшли звернення стосовно шахрайських заволодінь коштами фізичних осіб. Банками заблоковані рахунки клієнтів та відмовлено в підтриманні ділових відносин.

Привертає увагу, що кошти, отримані на рахунки, у тому числі шахрайським шляхом, розпорошувалися на різні картки невстановлених осіб, емітовані різними банківськими установами, використовувались для придбання криптовалюти, оплати товарів/послуг тощо.

У зв'язку з підозрілою діяльністю **Подружжя Н**, їм було відмовлено у підтримані/встановлені ділових відносин 15 банківськими установами.

Привертає увагу, що **Подружжя Н** зареєстровано на тимчасово окупованій території України.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2024.4.8.8. Шахрайське заволодіння коштами шляхом підміни реквізитів платіжного документа

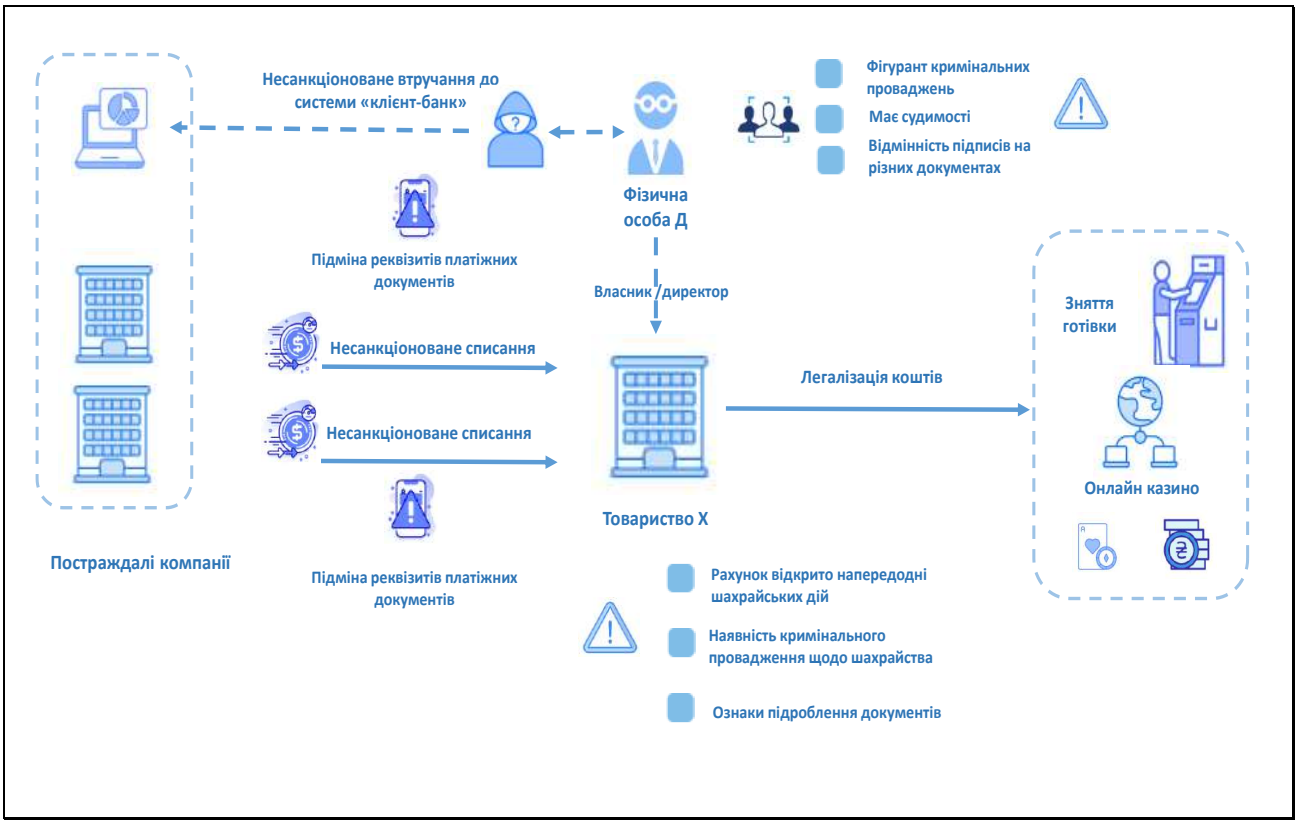
Держфінмоніторингом було виявлено схему шахрайських фінансових операцій, здійснених з метою заволодіння грошовими коштами юридичних осіб через несанкціоноване втручання у систему міжбанківських платежів «клієнт-банк» та зміну реквізитів платіжних документів.

Так, з рахунків постраждалих компаній через систему міжбанківських платежів «клієнт-банк» включаючи підміну реквізитів платіжних документів та підробку електронних підписів, відбулися несанкціоновані списання коштів на користь **Товариства Х**. Під час фінансового розслідування встановлено, що для заволодіння коштами було використано рахунок **Товариства Х**, відкритий напередодні вчинення шахрайських дій

Надалі незаконно отримані кошти легалізувались через оплату послуг на сайті онлайн-казино та подальше зняття готівки **Фізичною особою Д**, яка є власником/директором **Товариства Х**.

При цьому, **Фізична особа Д** має низку кримінальних справ та судимостей, зокрема за розбій, за незаконні операції з наркотиками, шахрайство та крадіжку). Крім того, виявлено ряд ознак (відмінність підписів на різних документах), які свідчать про можливість, що **Фізична особа Д** є лише номінальним власником **Товариства Х**, співпрацює або його документи використовуються невстановленими особами для здійснення незаконної діяльності.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2024.4.8.9. Шахрайське заволодіння коштами шляхом викрадення даних

Держфінмоніторингом виявлено шахрайську схему заволодіння коштами з використанням методу соціальної інженерії – «вішинг».

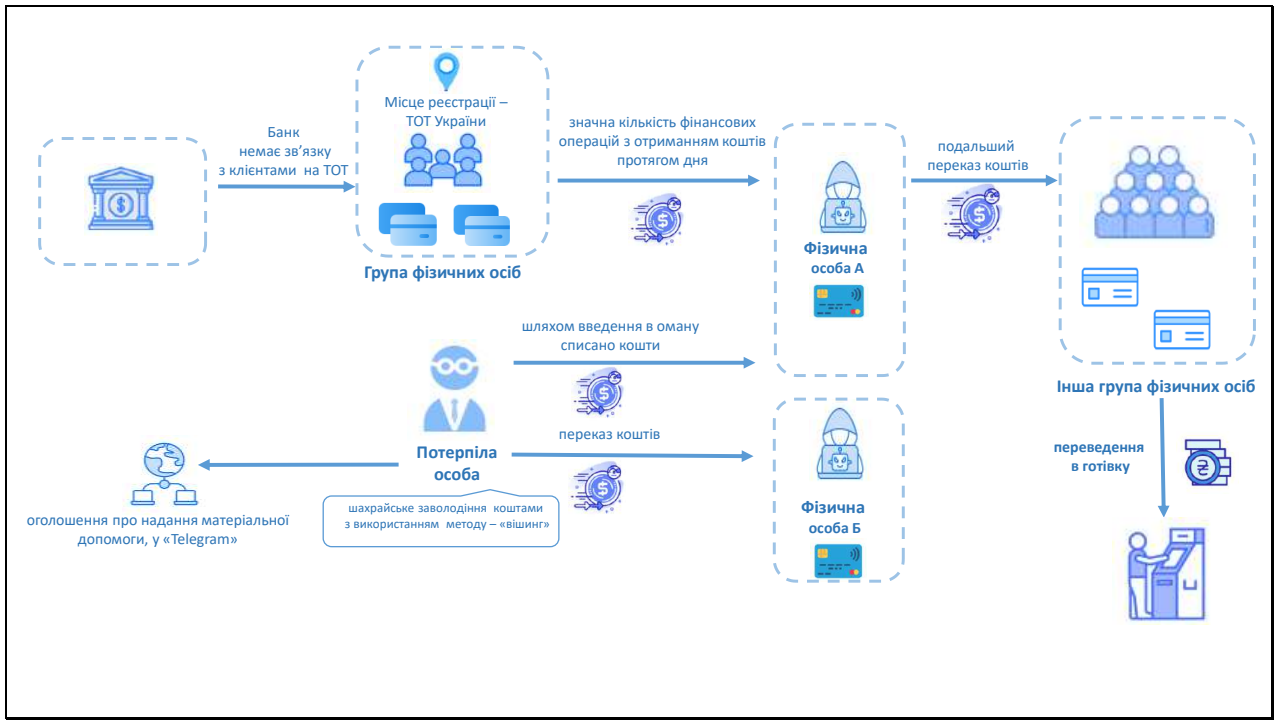
Потерпіла особа у «Telegram» знайшов оголошення про надання матеріальної допомоги та, перейшовши за посиланням у відповідних WEB-формах, вказав логін та пароль входу до свого онлайн-банкінгу.

Встановлено, що **Фізична особа А** та **Фізична особа Б** шляхом введення в оману **Потерпілу особу** заволоділи його коштами з наступною їх частковою легалізацією шляхом переказу на платіжні картки **Інших фізичних осіб**.

Також **Фізична особа А** в умовах воєнного стану отримала на власний рахунок протягом дня значну кількість переказів від **Групи фізичних осіб**, які зареєстровані на тимчасово окупованій території та з якими банк не має зв'язку.

Фізична особа А надалі перерахувала ці кошти **Іншій групі фізичних осіб**, ймовірно, для переведення в готівку.

Правоохоронним органом здійснюється досудове розслідування.



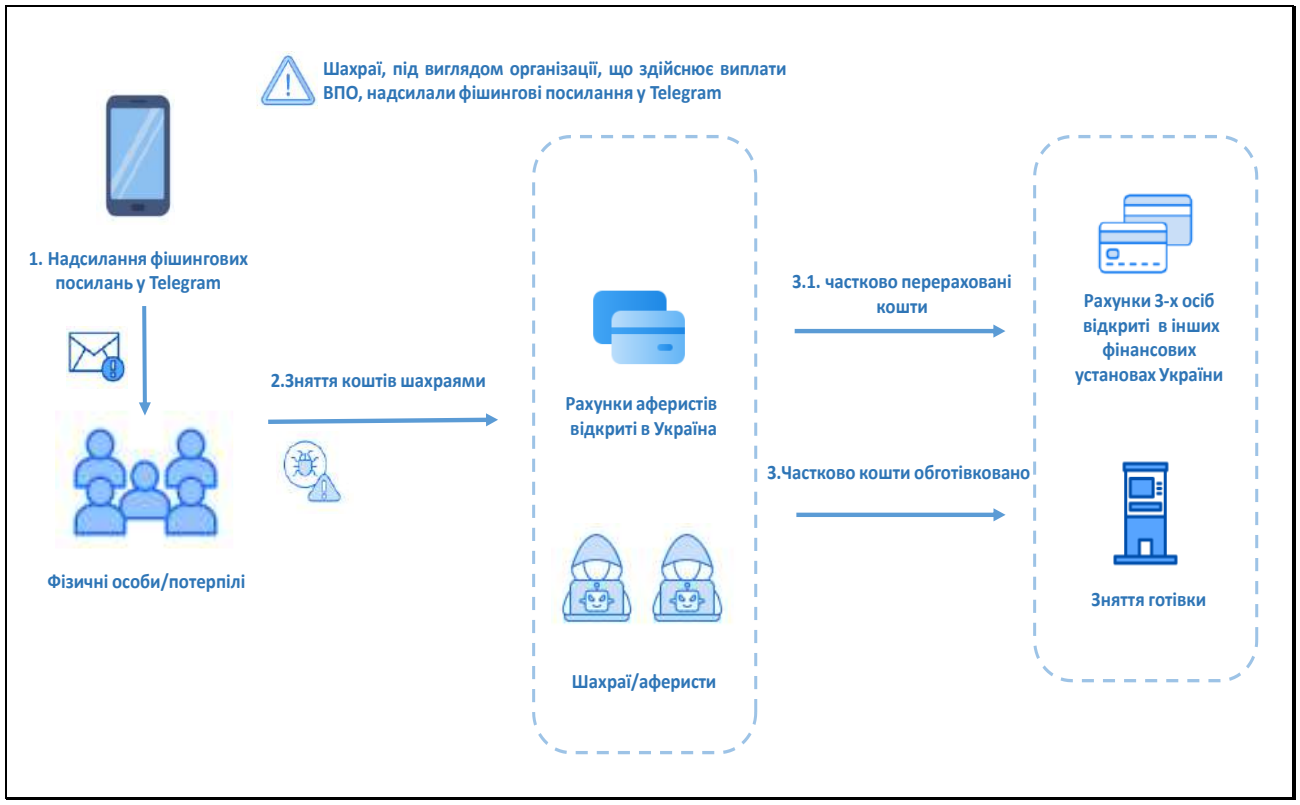
Приклад 2024.4.8.10. Шахрайське заволодіння коштами громадян шляхом викрадення даних

Держфінмоніторингом виявлено схему з шахрайського заволодіння коштами фізичних осіб, шляхом обману чи зловживання довірою.

Встановлено, що **Шахраї**, під виглядом організації, що здійснює виплати внутрішньо переміщеним особам, надсилали фішингові посилання від відомого банку у Telegram **Фізичним особам**. Перейшовши за отриманим посиланням, кошти з рахунків **Потерпілих** були зняті та перераховані на картки **Шахраїв**.

Надалі, **Шахраї** вищевказані кошти перераховували на картки третіх осіб в інші фінансові установи, частково зняли готівкою та списали для оплати товарів/послуг.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2024.4.8.11. Заволодіння коштами фізичних осіб, отриманими внаслідок проведення «псевдозборів»

За даними Державної податкової служби України, **Фізична особа** разом із спільниками оприлюднювали в соціальних мережах (Telegram, Instagram) «фіктивні» пости щодо проведення зборів на потреби Збройних сил України та на допомогу постраждалим громадянам.

Надалі отримані кошти, які надходили на банківські рахунки на ім'я головного фігуранта **Фізичної особи**, використовувалися не за цільовим призначенням, а саме: перераховувалися на власні рахунки, обготівковувалися та обмінювалися на валюту, придбавалися речі для власного користування, робилися ставки в інтернет-казино (типу «ROYAL JOKER», «Фавбет», «PIN-UP», «PARIK24», «FIRST» та інші), ставки на спорт (типу «Parimatch» та інші), придбання авто тощо.

Таким чином була організована схема по незаконному привласненню коштів гуманітарної допомоги, благодійних пожертв, з подальшою легалізацією (відмиванням) коштів, одержаних злочинним шляхом.

Правоохоронним органом здійснюється досудове розслідування.

РОЗДІЛ 4.9. ВІДМИВАННЯ ЗЛОЧИННИХ ДОХОДІВ ІЗ ВИКОРИСТАННЯМ ВІРТУАЛЬНИХ АКТИВІВ ТА ЧЕРЕЗ ГРАЛЬНИЙ БІЗНЕС

Ринок обігу віртуальних активів належить до високоризикованих сфер діяльності, які потребують особливої уваги контролюючих та правоохоронних органів.

Використання ВА в схемах ВК/ФТ. Перевагами використання віртуальних активів залишаються висока анонімність та швидкість переказу, як в межах країни, так і за кордон, децентралізація платежів, обмежене регулювання або його відсутність в деяких юрисдикціях.

Віртуальні активи продовжують використовувати для обходу санкцій, виведення коштів за кордон, фінансування терористичної діяльності, приховування доходів від незаконної діяльності, торгівлі зброєю, наркотиками та іншими забороненими речовинами.

Згідно з останніми даними Chainalysis та TRM Labs, типології відмивання доходів із використанням віртуальних активів охоплюють широкий спектр схем, які постійно трансформуються та залежать від технологічних рішень. Вони охоплюють кілька ключових сценаріїв, що відображають сучасні технологічні тенденції.

Наприклад:

- **використання міксерів та протоколів конфіденційності.** Міксери дозволяють приховувати джерела криптовалютних активів шляхом змішування транзакцій із коштами інших користувачів. Це ускладнює відстеження руху коштів;
- **використання крос-чейн мостів.** Крос-чейн транзакції дозволяють злочинцям переводити активи між різними блокчейнами, що ускладнює їхнє відстеження;
- **застосування криптобірж.** Більшість незаконних коштів переводяться у фіат через криптобіржі з низьким рівнем дотримання процедур AML та KYC;
- **використання стейблкоїнів.** Стейблкоїни стають популярними для незаконних операцій через їхню стабільність і можливість обходу традиційних фінансових систем;
- **зловживання NFT.** Неліквідні активи, такі як NFT, використовуються для маскування походження коштів через підставні угоди. Це дозволяє фіктивно збільшувати цінність активу і легалізувати доходи;
- **операції на платформах даркнету.** Оплата за незаконні товари чи послуги у даркнеті здійснюється криптовалютою. Попри закриття таких платформ, як Hydra, їхні функції поступово відновлюються через менші майданчики;

Типологічне дослідження «Ризики та загрози легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансування тероризму в умовах військової агресії російської федерації – 2024»

- **маскування у краудфандингових платформах. «Фейкові» збори.** Маскування злочинного походження коштів через платформи збору криптовалют, де прозорість менша, ніж у банківських рахунках. Криптовалюти використовуються для організації «фіктивних» благодійних кампаній, через які відмиваються незаконні кошти;
- **фіктивні токени.** Зловмисники створюють фіктивні токени чи платформи для збору інвестицій, маскуючи незаконні кошти під інвестиції;
- **крипто-банкомати**. Крипто-АТМ часто використовуються для переведення готівки у віртуальні активи. Значна кількість нелегальних операцій відбулася через ці термінали;
- **використання штучного інтелекту**. Додатки з використанням штучного інтелекту дозволяють забезпечити автоматизацію фінансових потоків. Використання ботів та алгоритмів для розподілу коштів через численні рахунки та сервіси.

Згідно з останніми даними Chainalysis та TRM Labs, тенденції у відмиванні грошей через криптовалюти у 2023–2024 роках демонструють кілька ключових змін:

- **падіння загального обсягу незаконних транзакцій**: Загальна вартість криптовалют, отриманих незаконними шляхами, знизилася з $31,5 млрд у 2022 році до $22,2 млрд у 2023 році. Головним чином через посилення санкцій та регуляторних заходів;
- **перехід від Bitcoin до інших блокчейнів**. Частка Bitcoin у незаконних транзакціях падає, тоді як Tron та Binance Smart Chain набули популярності серед злочинців;
- **зміна популярності криптоактивів серед злочинців**: Стейблкоїни стали домінуючим інструментом для незаконних операцій, особливо у випадках, пов’язаних із шахрайством і санкціями;
- **фокус на мостах і міксерах**: Зловмисники активно використовують крос-чейн мости та міксери для приховування джерела коштів;
- **російські криптоекосистеми.** Групи з росії домінують у таких сферах, як програми-вимагачі (69% доходів) та даркнет-торгівля. Активність таких груп пов’язана з підтримкою державних інтересів;
- **зловживання платформами стейблкоїнів для незаконних транзакцій**. Зростає загроза, оскільки такі активи пропонують стабільність і простоту транзакцій, зокрема в умовах ВК/ФТ та обходу санкцій.

Використання росією віртуальних активів. Віртуальні активи відіграють важливу роль у фінансуванні воєнних дій росії проти України, включаючи можливе використання для обходу санкцій та підтримки незаконних збройних угруповань.

Типологічне дослідження «Ризики та загрози легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансування тероризму в умовах військової агресії російської федерації – 2024»

Підтримка бойовиків на окупованих територіях України здійснюється шляхом збору коштів у криптовалюті через закриті мережі та сервіси, які часто працюють на платформі Tron або через міксери для приховування транзакцій.

FATF. У 2024 році FATF продовжила вдосконалювати глобальні стандарти для регулювання криптовалют і боротьби з відмиванням коштів у цьому секторі. FATF опублікувала п'яте оновлення Оцінки виконання стандартів для віртуальних активів (VA) і постачальників послуг віртуальних активів (VASPs). FATF акцентує увагу на ризиках, пов'язаних зі стейблкоїнами та децентралізованими фінансами (DeFi), які стають дедалі популярнішими у схемах відмивання коштів.

Узагальнені типові приклади відмивання злочинних доходів із використанням віртуальних активів та через гральний бізнес наведено нижче.

Приклад 2024.4.9.1. Незаконне заволодіння коштами фізичних осіб з використанням криптовалют та підроблених документів

Держфінмоніторингом, з урахуванням інформації, отриманої від ПФР іноземних держав, виявлено групу шахраїв, які діяли на території ЄС, використовуючи підроблені документи.

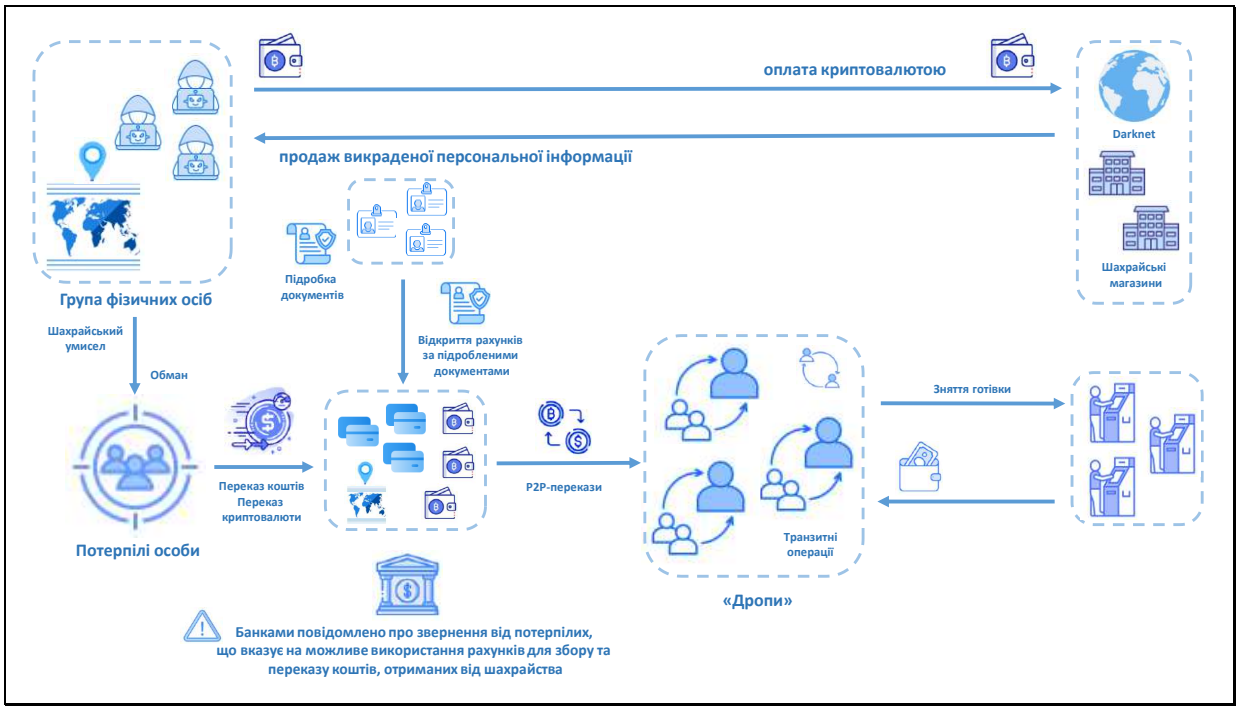
В ході аналізу встановлено, що **фізичні особи** придбавали викрадену персональну інформацію за криптовалюту на ринку Darknet та у шахрайських магазинах з використанням підроблених паспортів громадян України для виїзду за кордон.

Придбана персональна інформація надалі використовувалась **фізичними особами** для формування нових фіктивних документів, за якими вони відкривали рахунки у різних провайдерів платіжних послуг, що діють в країнах ЄС.

Щодо деяких фінансових операцій по відкритих рахунках **фізичних осіб** банками повідомлено про звернення від потерпілих, які є громадянами країн ЄС, що вказує на можливе використання цих рахунків для збору та переказу коштів, отриманих від інвестиційного шахрайства або шахрайства з авансовими платежами.

Для подальшого виведення коштів, отриманих в результаті шахрайської діяльності, **фізичні особи** залучали **«дропів»**, за допомогою яких здійснювалось обготівковування.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2024.4.9.2. Фінансування диверсійної діяльності

Держфінмоніторингом спільно з правоохоронним органом проводиться фінансове розслідування за фактом причетності фізичних осіб до диверсійної діяльності в Україні в умовах воєнного стану.

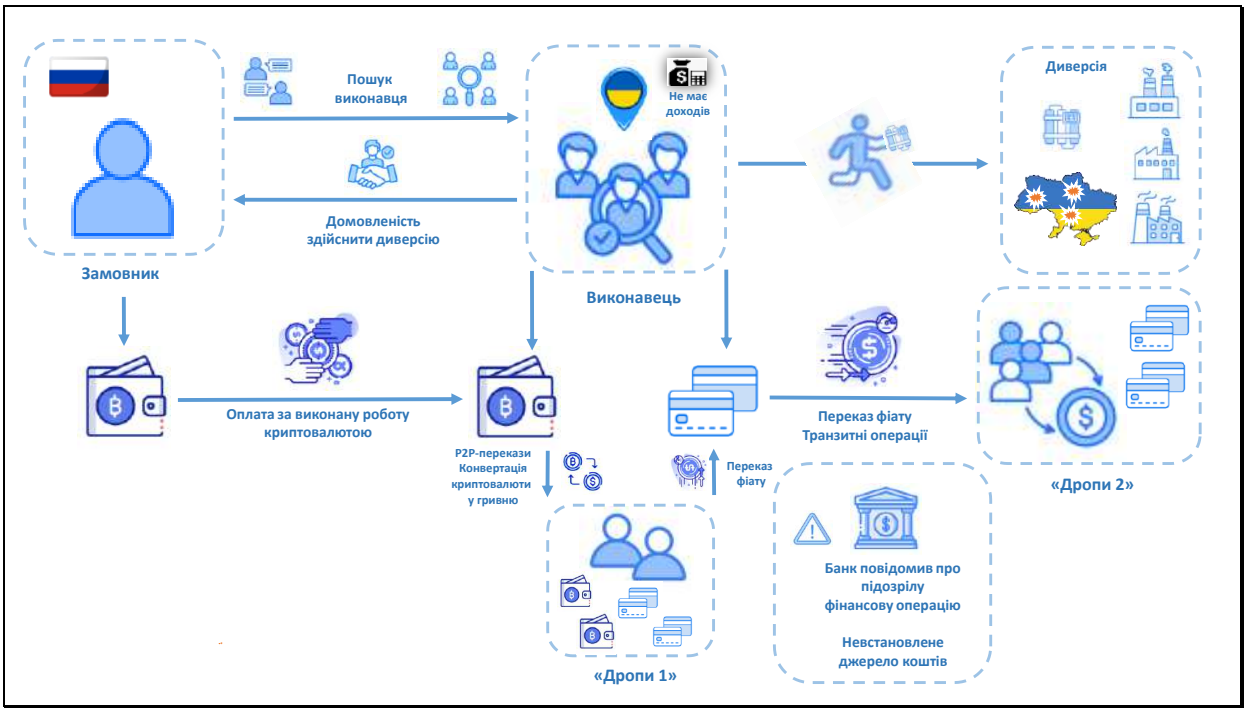
Встановлено, що **Замовник** (з громадянством росії) здійснював пошук осіб в Україні, які були здатні виконати диверсійну роботу з заподіяння шкоди об'єктам критичної інфраструктури України, яким ставив відповідні завдання.

Розрахунок за виконану роботу **Замовник** проводив у криптовалюті з власного криптогаманця на криптогаманець **Виконавця**, зареєстрований на криптовалютній біржі. Надалі криптовалюта з використанням p2p-переказів переводилась у гривню та перераховувалась на банківський рахунок **Виконавця**. Фіатні кошти було перераховано p2p-переказом на картки **«дропів 2»**.

Банківська установа, в якій обслуговується **Виконавець** злочину, повідомила про схемні фінансові операції, проведені на його рахунку на значну суму. При цьому, кошти, залучені для проведення фінансових операцій по рахунку, мають невстановлене походження, оскільки задекларованих доходів у **Виконавця** немає.

Таким чином, виявлено фінансові операції по відкритому рахунку **Виконавця** злочину, які пов'язані із зарахуванням коштів, є оплатою за вчинення кримінального правопорушення.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2024.4.9.3. Відмивання доходів з використанням послуг, вартість яких оцінити складно

Держфінмоніторингом, з урахуванням інформації правоохоронного органу, виявлено схему легалізації (відмивання) доходів від ухилення сплати податків у сфері грального бізнесу.

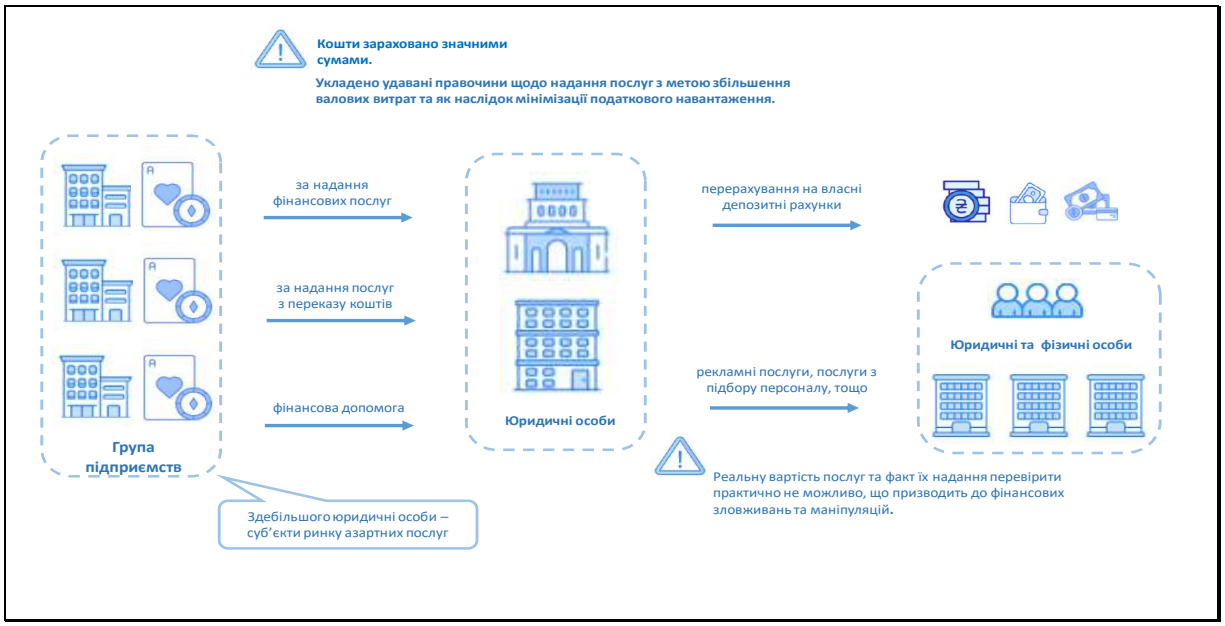
Встановлено, що від **Групи підприємств**, які переважно є суб'єктами ринку азартних послуг, на рахунки **Юридичних осіб**, значними сумами зараховуються кошти під виглядом оплати послуг з переказу коштів, фінансових послуг та надання фінансової допомоги.

Надалі кошти перераховуються на інші власні рахунки **Юридичних осіб**, у тому числі депозитні, а також на користь великої кількості юридичних та фізичних осіб, як оплата за послуги, вартість яких оцінити складно (рекламні послуги, послуги з підбору персоналу тощо).

Варто зазначити, що фінансові операції учасників, пов'язані із залученням для їх проведення ризикових інструментів, таких як надання фінансової допомоги, неконкретизовані та розмиті за змістом фінансові послуги, а також залучення обігових коштів для поповнення депозитних вкладів.

Є підстави вважати, що **Юридичні особи** укладали з суб'єктами ринку азартних послуг удавані правочини щодо надання послуг з метою збільшення валових витрат та як наслідок мінімізації податкового навантаження.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2024.4.9.4. Шахрайське заволодіння криптовалютними коштами

Держфінмоніторингом, з врахуванням інформації отриманої від правоохоронного органу, виявлено схему шахрайських фінансових операцій, здійснених з метою заволодіння грошовими коштами **Потерпілої особи** під виглядом обміну криптовалюти на грошові кошти.

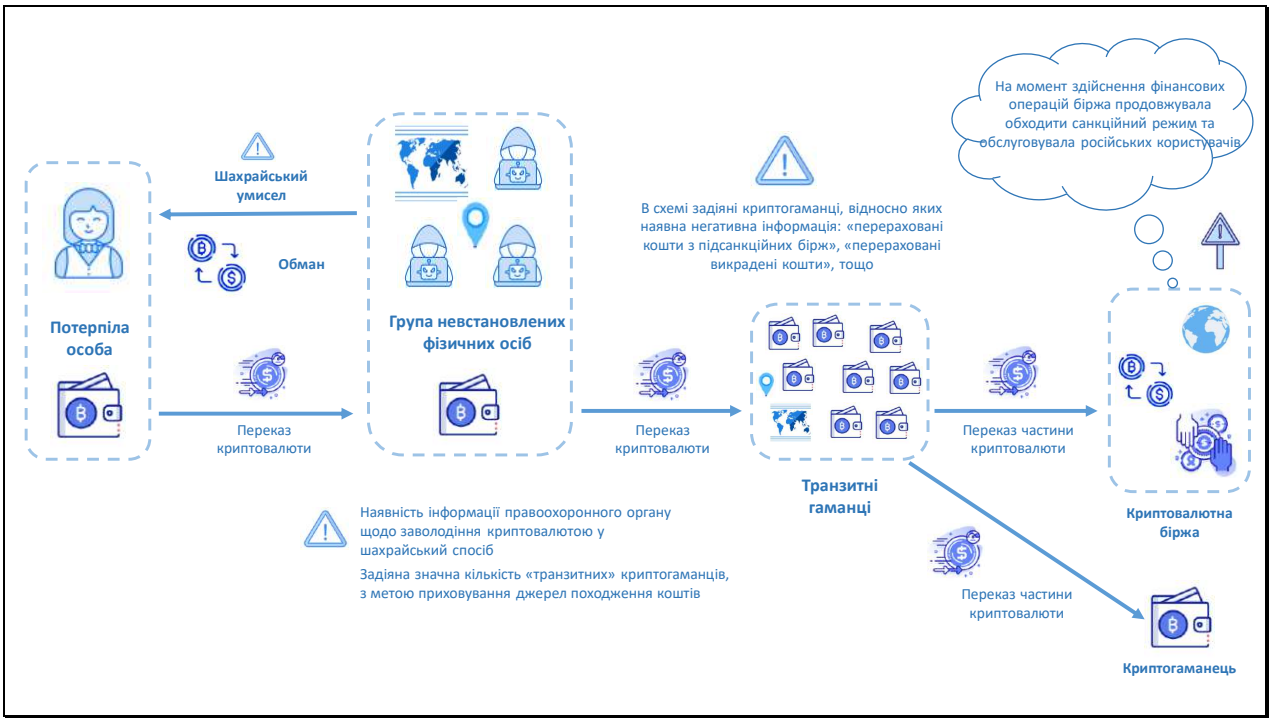
За інформацією правоохоронного органу, невстановлені **Фізичні особи** шляхом обману та незаконних фінансових операцій з використанням електронно-обчислювальної техніки під виглядом обміну криптовалюти на грошові кошти протиправно заволоділи криптовалютними активами **Потерпілої особи**.

Встановлено, що перерахування валюти з криптогаманця **Потерпілої особи** на інший криптогаманець було здійснено шахрайським способом.

За результатами аналізу руху криптовалюти встановлено, що частина отриманих у шахрайський спосіб коштів транзитом через значну низку адрес (криптогаманців) була перерахована на адресу **Криптовалютної біржі**.

Слід зазначити, що зазначена платформа, на момент здійснення фінансових операцій, продовжувала обходити санкційний режим та обслуговувала російських користувачів.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2024.4.9.5. Приховування доходів від здійснення діяльності нелегальних гральних платформ

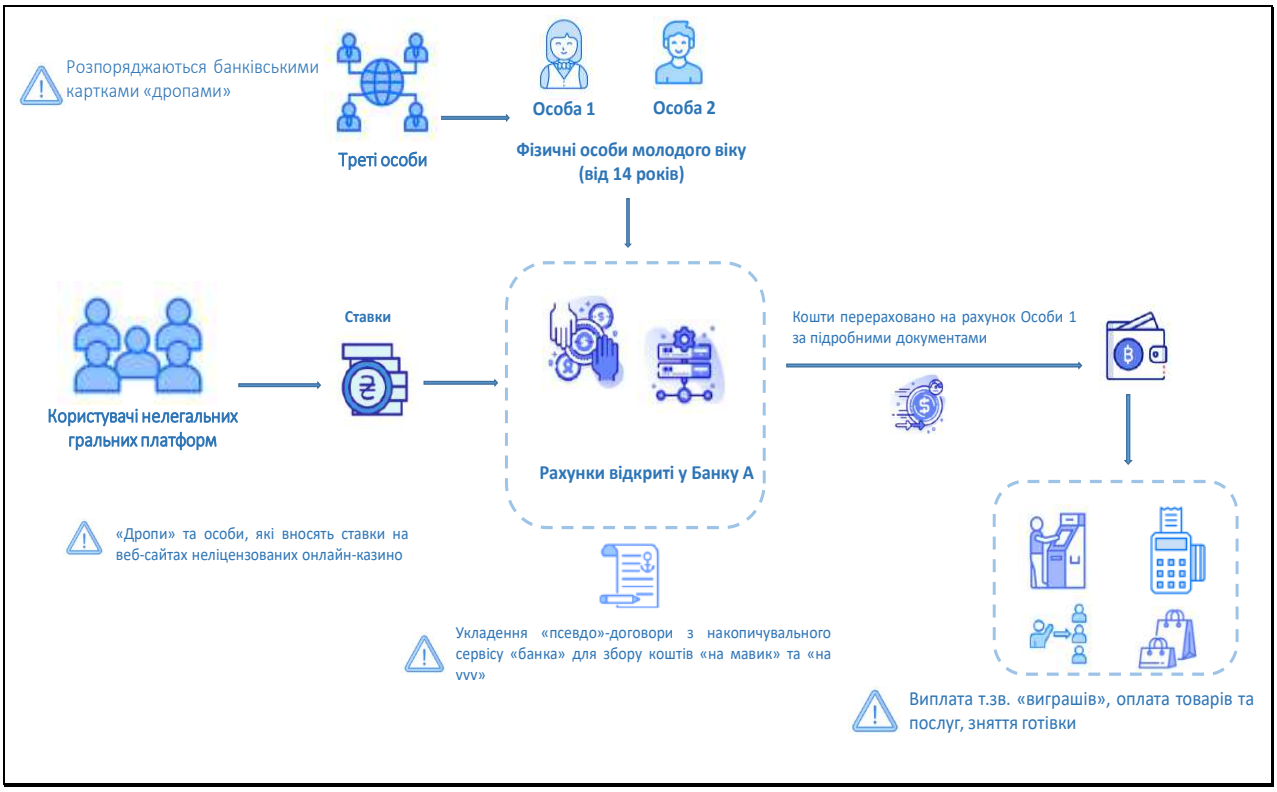
Держфінмоніторингом, з урахуванням інформації правоохоронного органу, виявлено схему незаконної діяльності за участю великої групи фізичних осіб молодого віку, яка може бути пов'язана із приховуванням доходів нелегальних гральних платформ.

Встановлено, що в розпорядженні **Третіх осіб** перебувають банківські картки «дропів» (зокрема, **Особи 1** та **Особи 2**), на які на регулярній основі зараховуються кошти від користувачів нелегальних гральних платформ.

Відомо, що дистанційно ймовірно **третіми особами** у **Банку А** з неповнолітньою (14 років) **Особою 1** укладено «псевдо»-договори з накопичувального сервісу «банка» для збору кошів «на мавик», «на vvv» («банки»).

Надалі кошти, отримані в результаті P2P переказів, перераховано на поточний рахунок **Особи 1** у **Банку А**, з якого проводиться виплата т.зв. «виграшів» на нелегальних гральних сайтах, легалізація вказаних коштів, шляхом придбання товарів та послуг на торгових майданчиках або обготівковування в банкоматах та касах банківських установ.

Правоохоронним органом здійснюється досудове розслідування.


Розпоряджаються банківськими картками «дропами»
Треті особи
Особа 1
Особа 2
Фізичні особи молодого віку (від 14 років)
Користувачі нелегальних грального платформ
Ставки
Рахунки відкриті у Банку А
Кошти перераховано на рахунок Особи 1 за підробними документами
«Дропи» та особи, які вносять ставки на веб-сайтах неліцензованих онлайн-казино
Укладення «псевдо»-договори з накопичувального сервісу «банка» для збору коштів «на мавик» та «на vvv»
Виплата т.зв. «виграшів», оплата товарів та послуг, зняття готівки

РОЗДІЛ 4.10. ВІДМИВАННЯ ДОХОДІВ ВІД ТОРГІВЛІ ЗБРОЄЮ, ЛЮДЬМИ ТА НАРКОТИЧНИМИ ЗАСОБАМИ

Торгівля людьми, зброєю та наркотичними засобами – трійка найбільш прибуткових злочинів в кримінальній сфері, що безумовно підсилює інтерес до них як окремих злочинців, так і організованих злочинних угрупувань.

Важко переоцінити негативний вплив цих злочинів на економічну стабільність в країні та на міжнародний імідж України у світі, особливо в умовах російської збройної агресії, коли Україна потребує значної міжнародної допомоги.

Схеми відмивання доходів від торгівлі людьми, зброєю та наркотичними засобами зазвичай є складними й заплутаними, із залученням значної кількості підставних осіб, транзитних та фіктивних компаній, в тому числі офшорних.

Для ускладнення виявлення джерел походження злочинних доходів використовуються розрахунки в криптовалюті та інших віртуальних активах, готівкові розрахунки, транзитні операції, в тому числі з використанням дропів.

Узагальнені типові приклади відмивання злочинних доходів від торгівлі людьми та наркотичними засобами наведено нижче.

Приклад 2024.4.10.1. Відмивання коштів, отриманих від торгівлі людьми (сурогатне материнство)

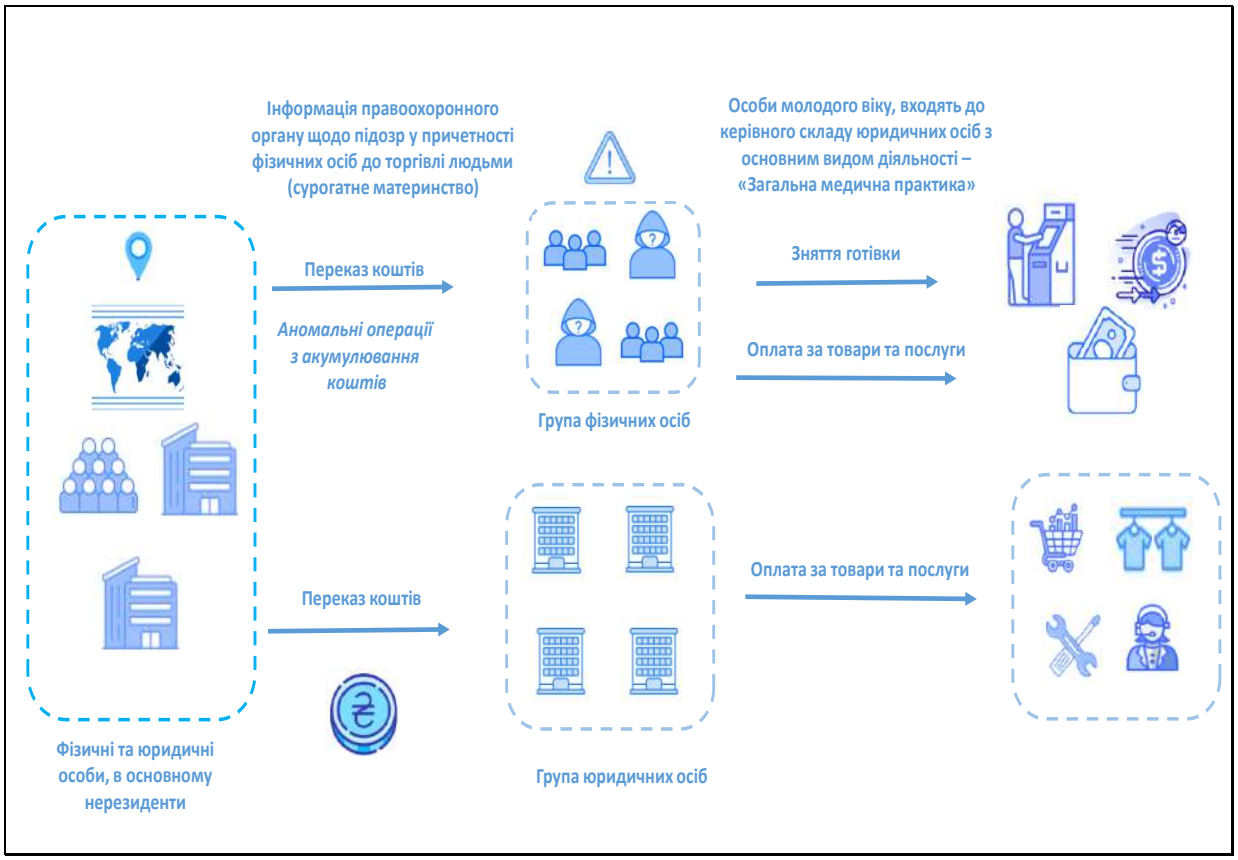
Держфінмоніторингом, з урахування інформації правоохоронного органу, виявлено підозрілі фінансові операції **Групи фізичних та юридичних осіб**, які можуть бути пов’язані зі злочинною діяльністю, ймовірно торгівлею людьми (сурогатне материнство).

Держфінмоніторингом виявлено аномальні фінансові операції, пов’язані з акумулюванням коштів на рахунках **Групи фізичних та юридичних осіб**, які попередньо були зараховані переважно від нерезидентів. Надалі кошти, в переважній більшості, знято готівкою або використано для оплати товарів, послуг, придбання нерухомості.

Фізичні особи, молодого віку, входять до керівного складу ряду підприємств з основним видом діяльності – «Загальна медична практика». За інформацією правоохоронного органу зазначені особи є організаторами схеми незаконного комерційного сурогатного материнства.

Характер проведених фінансових операцій може свідчити про використання особистих рахунків фізичних осіб для одержання та використання доходу від злочинної діяльності, ймовірно торгівлі людьми.

Правоохоронним органом здійснюється досудове розслідування.



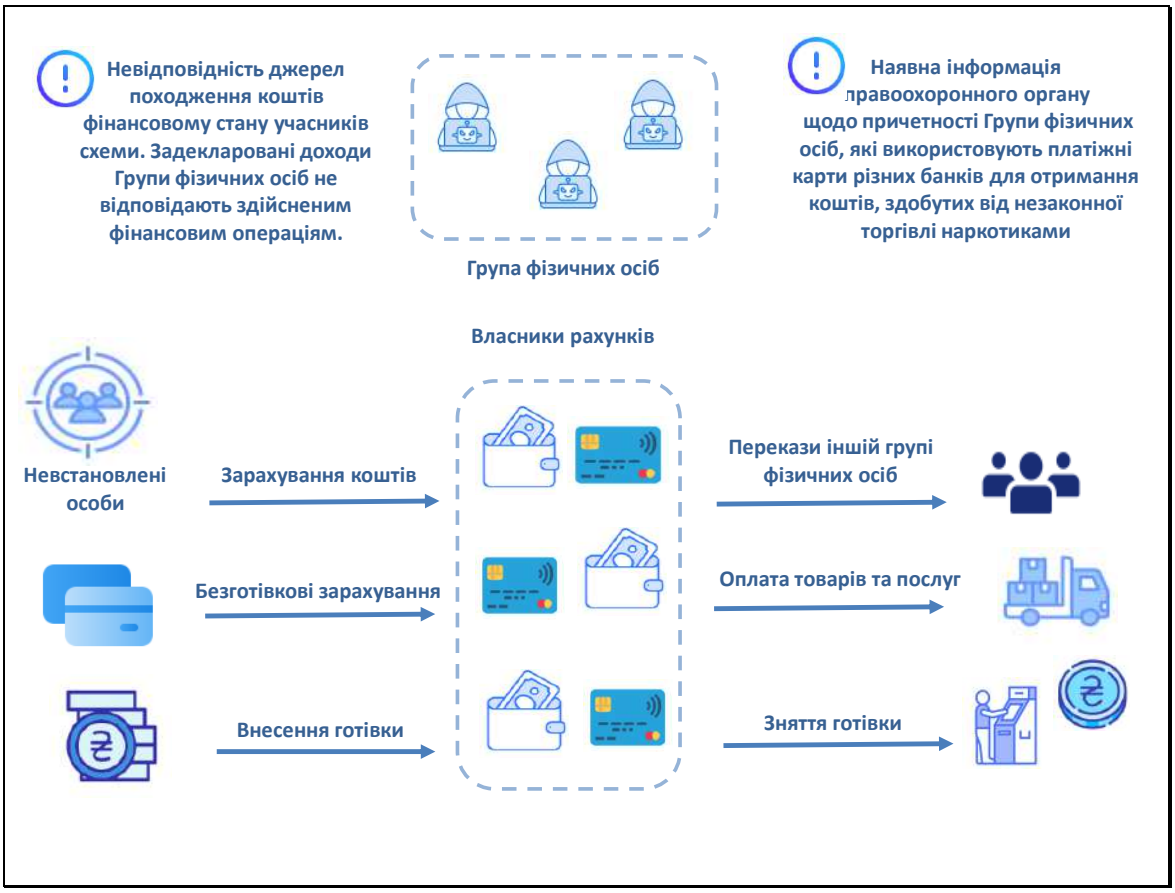
Приклад 2024.4.10.2. Відмивання коштів, одержаних від торгівлі наркотиками

Держфінмоніторингом, з врахуванням інформації, отриманої від правоохоронного органу, виявлено фінансові операції, пов'язані з акумулюванням коштів, отриманих від групи невстановлених осіб на карткових рахунках **Групи фізичних осіб**, відкритих у різних банках, що можуть бути пов'язані із вчиненням кримінального правопорушення, що стосується торгівлі наркотиками.

Так, по картах **Групи фізичних осіб** спостерігалося надходження значних сум коштів (як в готівковій, так і в безготівковій формах), які не відповідають офіційно задекларованим доходам та фінансовому стану учасників. Надалі кошти переважно перераховано іншій групі фізичних осіб, частково знято готівкою або списано як оплату за товари/послуги.

Фізичні особи мають ознаки дропів.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2024.4.10.3. Отримання злочинних доходів від продажу наркотичних засобів

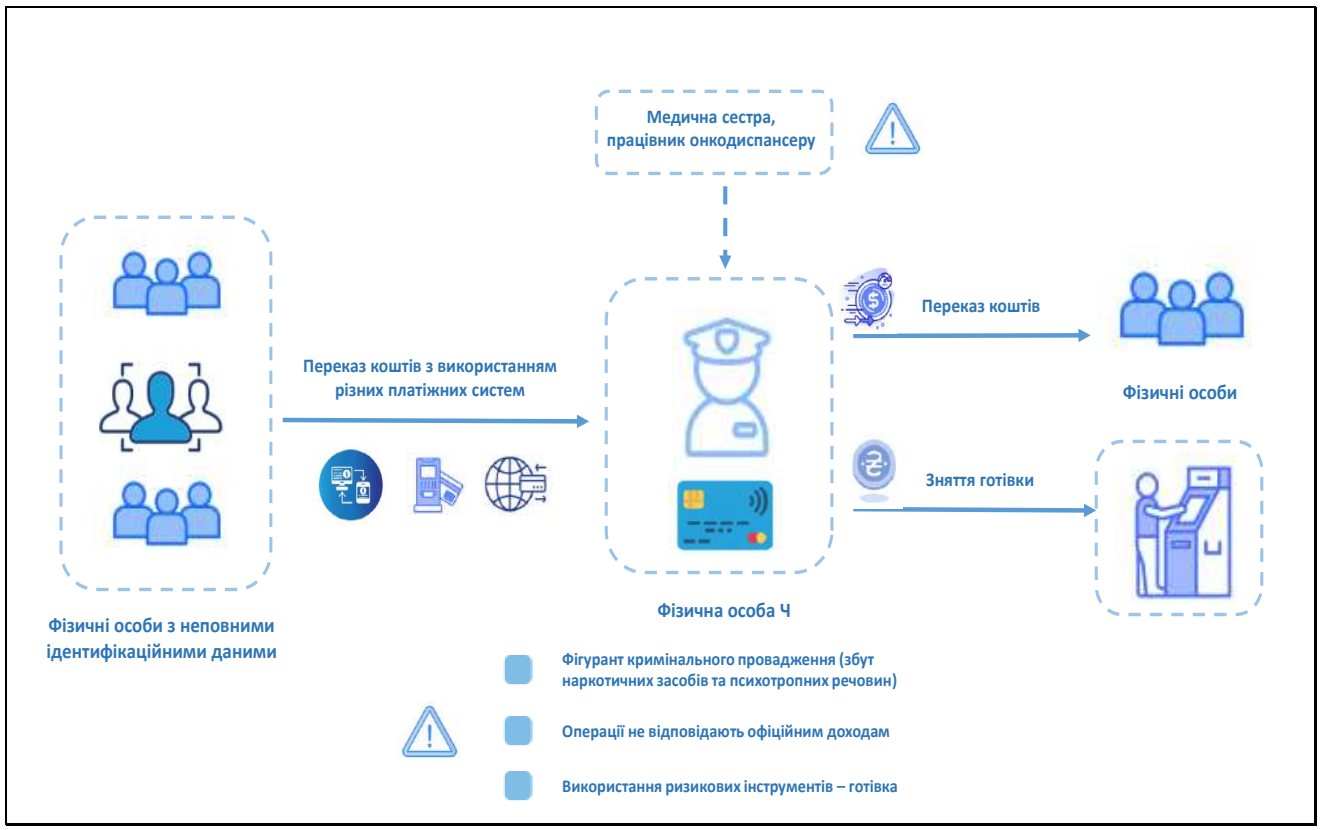
Держфінмоніторингом, виявлено підозрілі фінансові операції із поповнення банківської картки **Фізичної особи Ч**, які можуть бути пов'язані з реалізацією наркотичних засобів.

Так, встановлено, що **Фізична особа Ч,** яка є співробітником онкодиспансеру та обіймає посаду медичної сестри, отримує систематичні надходження на рахунок від **Фізичних осіб** з неповними ідентифікаційними даними через різні платіжні системи.

Надалі отримані кошти знімаються готівкою або перераховуються на користь ряду інших фізичних осіб. При цьому операції **Фізичної особи Ч** не відповідають офіційним доходам та не мають очевидної економічної чи законної мети.

Крім того, за наявною інформацією **Фізична особа Ч** є учасником кримінального провадження (збут наркотичних засобів та психотропних речовин).

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2024.4.10.4. Незаконне виготовлення та збут вогнепальної зброї та боєприпасів до неї з використанням підконтрольних осіб

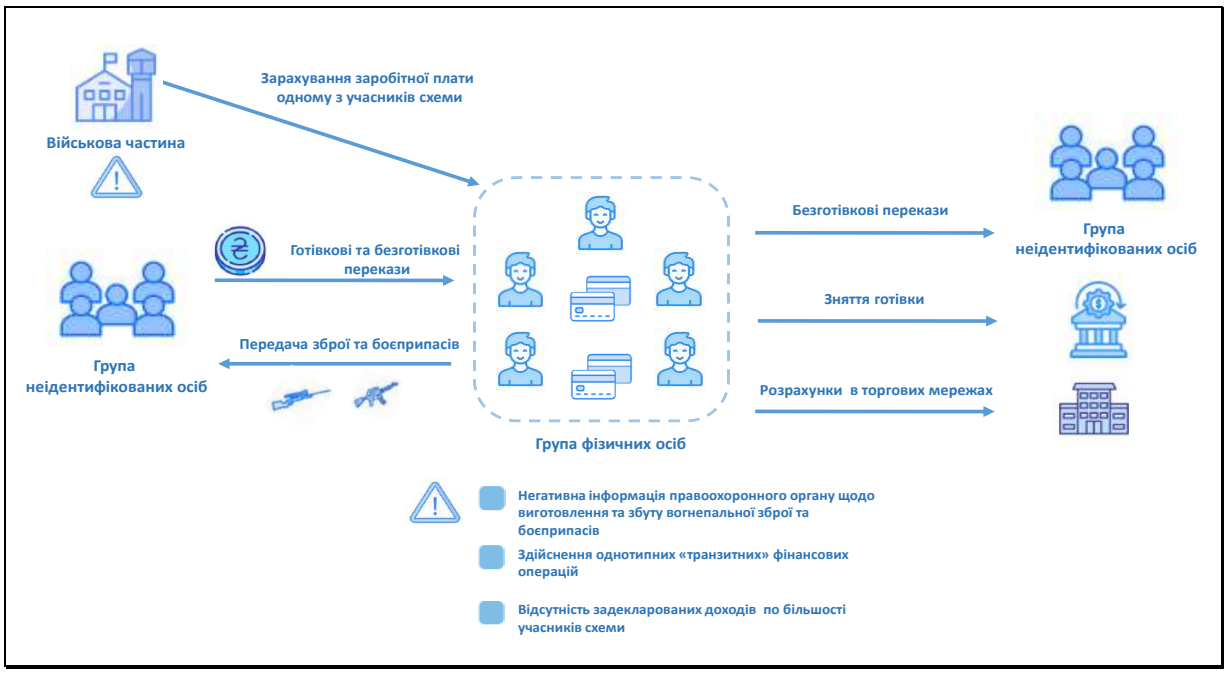
Держфінмоніторингом, з урахуванням інформації отриманої від правоохоронного органу, виявлено підозрілі фінансові операції **Групи фізичних осіб**, які причетні до незаконного виготовлення та збуту вогнепальної зброї та боєприпасів до неї.

За інформацією правоохоронного органу **Групою фізичних осіб**, з метою уникнення безпосереднього контакту з покупцями, розрахунок за реалізовану зброю здійснюється безготівково, шляхом переказу грошових коштів на банківські картки підконтрольних осіб.

Держфінмоніторингом, за результатами аналізу виявлено підозрілі фінансові операції учасників зазначеної схеми, зокрема пов'язані з отриманням готівкових та безготівкових переказів від групи неідентифікованих фізичних осіб. Надалі зазначені кошти перераховувались іншій групі неідентифікованих осіб, знімались готівкою або використовувались для розрахунків у торгівельних мережах за товари та послуги. При цьому інформація щодо задекларованого основного доходу по більшості учасників схеми відсутня.

При цьому на рахунок одного з учасників схеми зараховувано безготівкові перекази в якості заробітної плати від військової частини.

Правоохоронним органом здійснюється досудове розслідування.


Військова частина
Зарахування заробітної плати одному з учасників схеми
Готівкові та безготівкові перекази
Передача зброї та боєприпасів
Група неідентифікованих осіб
Група фізичних осіб
Безготівкові перекази
Зняття готівки
Розрахунки в торгових мережах
Група неідентифікованих осіб
Негативна інформація правоохоронного органу щодо виготовлення та збуту вогнепальної зброї та боєприпасів
Здійснення однотипних «транзитних» фінансових операцій
Відсутність задекларованих доходів по більшості учасників схеми

РОЗДІЛ V. ОСНОВНІ ІНСТРУМЕНТИ, ІНДИКАТОРИ ТА СПОСОБИ ЗЛОЧИНІВ ВІЙНИ ТА ВК/ФТ

Війна залишається ключовим фактором дестабілізації економіки та безпеки, сприяючи зростанню тіньової економіки, посиленню контрабанди, поширенню схем ВК та міжнародної злочинності.

Сучасні тенденції свідчать про активізацію діяльності злочинних груп.

Злочинці активно адаптуються до нових викликів, використовуючи криптовалюту, цифрові платформи та різноманітні канали для приховування незаконної діяльності, що ускладнює моніторинг та контроль національних і міжнародних правоохоронних органів.

Втрата Україною контролю над тимчасово окупованими росією територіями ускладнює моніторинг незаконної діяльності, та фактично перетворила ці регіони на осередки нелегальних операцій, які підривають економічну стабільність та загрожують безпеці країни й європейському регіону.

Операції високого ризику.

Операції високого ризику в сучасному фінансовому середовищі мають чіткі ознаки та категорії, які можуть сигналізувати про незаконну діяльність.

До основних груп таких операцій належать:

а) **фінансування тероризму –** група операцій чи операція, що пов’язана з цільовим направленням коштів або ресурсів на підтримку терористичних організацій чи окремих осіб. В Україні законодавче визначення фінансування тероризму міститься у статті 258-5 КК України.

В загальному значенні «фінансування тероризму» передбачає надання або збирання коштів, майна чи інших матеріальних ресурсів із розумінням, що вони будуть використані для підтримки терористичної діяльності. Такі дії включають фінансування організації, підготовки або вчинення терористичних актів, залучення осіб до терористичної діяльності, забезпечення функціонування терористичних груп чи організацій, а також будь-яку іншу форму підтримки, спрямовану на реалізацію терористичних планів чи діяльності, зокрема забезпечення матеріальної бази, логістики або пропагандистських кампаній;

Типологічне дослідження «Ризики та загрози легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансування тероризму в умовах військової агресії російської федерації – 2024»

б) **операції з бюджетними коштами** – нецільове використання (розкрадання) бюджетних коштів за рахунок завищення ціни, поставки товарів низької якості, або за відсутності поставок;

в) **шахрайство** – заволодіння коштами фізичних осіб шляхом введення в оману, маніпулюванням, зловживання довірою, підробкою документів;

г) **операції НПО** – фіктивна благодійна діяльність, нецільове використання (привласнення) благодійної допомоги. НПО можуть бути використані як інструмент для здійснення незаконних операцій, включаючи ВК/ФТ.

Розуміння основних інструментів, індикаторів та способів вчинення злочинів є ключовим для ефективної протидії ВК та ФТ. Виявлення операцій високого ризику, аналіз підозрілих фінансових транзакцій та діяльності учасників дозволяють своєчасно ідентифікувати нелегальну діяльність на ранніх етапах, встановлювати коло учасників, джерела походження нелегальних доходів і їх подальше використання.

В сучасних умовах протидія ВК та ФТ вимагає ретельного моніторингу фінансових операцій та впровадження передових технологій. Використання інструментів штучного інтелекту, аналізу великих даних, автоматизованих систем перевірки транзакцій та моніторингу поведінки клієнтів дозволяє оперативно виявляти підозрілі схеми. Інноваційний підхід до аналізу ризиків та застосування високотехнологічних рішень є ключовими елементами у боротьбі з фінансовою злочинністю та тероризмом.

Систематизація знань про механізми вчинення злочинів і визначення ключових елементів схем ВК/ФТ має фундаментальне значення для ефективної боротьби з фінансовою злочинністю. Вона сприяє розробці більш точних стратегій моніторингу, забезпечує профілактику злочинів та дозволяє зміцнити національну і міжнародну безпеку.

Інструменти. Визначають технічні та організаційні засоби, які використовують злочинці для здійснення незаконних операцій. Вивчення інструментів допомагає зрозуміти, як та через які механізми здійснюються злочини.

Індикатори. Це основа для виявлення підозрілих фінансових операцій та поведінки. Вони є важливим елементом у розробці алгоритмів моніторингу, дозволяючи автоматизованим системам ідентифікувати аномалії у транзакціях або діях учасників фінансових процесів.

Способи. Розкривають характерні методи та стратегії, які використовують зловмисники.

Сукупний аналіз цих категорій дозволяє створити ефективні механізми для оцінки ризиків, вдосконалити методи фінансового моніторингу та підвищити рівень безпеки національних і міжнародних фінансових систем.

5.1. Основні інструменти у виявлених схемах ВК та ФТ

За результатами дослідження встановлено наступні основні інструменти, що використовувались у типових схемах ВК/ФТ:

Реєстраційні та структурні маніпуляції

- перереєстрація компаній за «законодавством» окупаційної влади та використання рахунків в фінансовій установі іншої країни;
- використання фіктивних суб'єктів господарювання та компаній-нерезидентів;
- залучення підставних осіб, номінальних власників, складної структури власності;
- ребрендинг підсанкційних суб'єктів;
- використання компаній-клонів;
- використання компаній, що надають послуги, подібні до «Агентства інтернет-досліджень» тощо;

Використання підставних осіб та афілійованих компаній

- залучення пов'язаних фізичних осіб-підприємців;
- залучення підконтрольних суб'єктів господарювання;
- залучення широкого кола фізичних осіб для здійснення фінансових операцій;
- наявність ймовірних родинних зв'язків між основними учасниками схеми;

Фінансові маніпуляції

- використання значної кількості рахунків одним клієнтом;
- проведення операцій по рахунках на незвично великі суми, що не притаманні ризик-профілю клієнта;
- використання платіжних систем, до яких застосовано санкції;
- поповнення передплатних карток PaysafeCard;
- надання послуг через професійні мережі з відмивання коштів;

Торгівельні маніпуляції та логістика

- відсутність постачання товарів при 100% передоплаті;
- підміна (заміна) номенклатури товарів;
- змішування сировини різних виробників;
- використання третіх країн для розрахунків з рф;
- здійснення транзитних операцій, залучення компаній-транзитерів;

- використання компаній з метою імпорту на територію країни-агресора виробничого обладнання, яке використовується для виробництва військових товарів;
- завищення/заниження вартості товарів/робіт/послуг/лотів;
- розрахунки та поставки товарів через офшорні юрисдикції;
- контрабанда товарів;
- використання «скруток» та «зустрічних потоків»;
- співпраця з країнами високого ризику (зокрема рф, рб, Північна Корея, Іран);
- неповернення валютної виручки;

Цифрові маніпуляції та кіберзагрози

- створення фейкових акаунтів (підроблені веб-сайти);
- створення ідентичних сайтів в різних юрисдикціях;
- використання шкідливих програм (програми-вимагачі);
- викрадення даних;
- злом акаунтів користувачів;
- несанкціоноване втручання в роботу електронних банківських систем;

Маніпуляції з криптовалютами

- надання послуг з переведення криптовалюти у готівку через криптообмінники, які працюють на тимчасово окупованих територіях;
- використання неліцензованих p2p-майданчиків та позабіржових обмінників (OTC-обмінників), які працюють поза регульованими платформами;
- співпраця з підсанкційними криптобіржами;

Використання фізичних осіб

- залучення «дропів»;
- залучення «кеш-кур'єрів»;

Гральний бізнес

- поповнення ігрових акаунтів через рахунки фізичних осіб на неліцензованих онлайн ігрових платформах;
- виведення незаконних доходів грального закладу під виглядом зарплат працівникам або переказ коштів фізичним особам-підприємцям;

Маніпуляції інформацією та шахрайство

- використання ботоферм для викривлення інформації;
- використання підроблених документів, у т.ч. паспортів;
- підміна реквізитів платіжних документів, використання «міскодінгу»;
- соціальна інженерія (вішинг);

Фінансові операції та афілійованість у зонах конфліктів

- отримання та відправлення переказів до або з зон конфліктів;
- залучення компаній (які співпрацювали з релігійними організаціями, що підтримують агресію росії) та мають зв'язки із зонами конфлікту;

Маніпуляції з інвестиціями та цінними паперами

- псевдоінвестування;
- купівля-продаж «сміттєвих» цінних паперів;

Незаконна діяльність

- незаконні правочини;
- використання гуманітарної допомоги для продажу;

Також, встановлено інструменти, які в комплексі з індикаторами підозрілості використовуються у протиправних схемах.

- використання платіжних терміналів та банкоматів;
- зарахування на карткові рахунки через провайдерів послуг з переказу електронних грошей;
- придбання елітних автомобілів та інших дороговартісних активів;
- використання готівки;
- надання/повернення фінансової допомоги/позик;
- надання благодійної допомоги;
- використання НПО;
- здійснення/повернення інвестицій;
- виплата дивідендів;
- подарунки родичів;
- купівля-продаж майнових прав;
- використання послуг інтернет-еквайрингу;
- операції з криптовалютою (віртуальними активами);
- використання суб’єктів грального бізнесу;
- виплата «виграшів».

5.2. Індикатори підозрілості учасників

За результатами дослідження встановлено наступні основні індикатори підозрілості учасника, що використовувались у типових схемах відмивання злочинних доходів та фінансування тероризму:

Фінансування війни

- особа, пов'язана з незаконним збройним формуванням;
- особа, яка підозрюється у вчиненні воєнних злочинів, державній зраді, колабораційній діяльності, злочинах проти основ національної безпеки України, проти життя та здоров'я особи, злочинах проти власності та інших злочинах визначених КК України;
- реєстрація фізичних осіб з непідконтрольних територій як ФОП з метою отримання терміналів для проведення обмінних операцій, в т.ч. обміну валют на валюту країни-агресора;
- використання спільних девайсів декількома суб'єктами господарювання;
- використання рахунків виробників продукції, виробничі потужності яких знаходяться на окупованих територіях;
- причетність до релігійної організації, що пропагандує підтримку тероризму, екстремізму чи війни;

Санкції

- щодо особи прийнято рішення про застосування санкцій;
- особа сприяє обходу санкційного режиму;
- щодо особи наявна інформація про співпрацю з підсанкційними біржами;

Політичні партії

- причетність до політичної партії забороненої в Україні через просування проросійських наративів;

Релігійні організації

- причетність до релігійної організації забороненої в Україні;

НПО

- фінансові операції НПО не відповідають їх профілю діяльності;
- витрачання коштів НПО без формування відповідної звітності про їх використання;
- у відкритих джерелах відсутня інформація про гуманітарні проєкти (ініціативи, цілі збору, тощо);

Учасник операцій

- фізичні особи володіють значною кількістю банківських рахунків (платіжними картками) потребу в яких не можуть пояснити;

- соціальний статус учасника не відповідає фінансовим операціям. Особи, які належать до соціально вразливих верств населення (студенти, пенсіонери) або отримують соціальну допомогу тощо. Особи зі спеціальним статусом (малозабезпечені, жебраки), або молодого (до 20 років), або похилого (після 75 років) віку;
- неповнолітня особа (14-18 років), яка може бути залучена до незаконної діяльності, зокрема до виконання злочинних дій за фінансову винагороду, таких як підпали, передача конфіденційної інформації чи інші протиправні дії, і водночас вразлива до маніпулювання свідомістю з боку агресора проти України;
- фізичні особи проживають на тимчасово окупованих територіях;
- виробничі потужності знаходяться на тимчасово окупованій території;
- участь в операціях значної кількості фізичних осіб;
- особа володіє чи розпоряджається статками, джерела набуття яких неможливо підтвердити;
- в джерелах походження коштів зазначається інформація щодо отриманих виграшів;
- криптобіржа, яка здійснює діяльність під виглядом єдиного бренду, але зареєстрована окремими юридичними особами;
- учасниками операції є підконтрольні суб'єкти господарювання;

КБВ, посадові особи

- невідповідність КБВ;
- номінальні посадові особи, власники;
- фізичні особи є кінцевими бенефіціарними власниками чи входять до посадово-засновницького складу великої кількості юридичних осіб;
- засновником/керівником, ФОП є особа, яка належить до соціально вразливих верств населення (студенти, пенсіонери, особи, які отримують соціальну допомогу тощо), особи зі спеціальним статусом (малозабезпечені, жебраки), особи молодого віку (до 20 років) або похилого (після 75 років);
- незначний досвід роботи юридичної особи (період діяльності), дата та місце реєстрації;
- засновником/керівником є особа відносно якої наявна негативна інформація (судимість, вживання наркотиків, причетність до корупційних злочинів тощо);
- одноосібний посадово-засновницький склад;
- непрозора структура власності;
- засновником/керівником є особа яка зареєстрована та проживає на непідконтрольній Україні території;
- корпоративне володіння суб’єктами господарювання (стратегічними підприємствами) громадянами росії та білорусі;

- опосередкований контроль за діяльністю суб'єкта господарювання з боку представників росії та білорусі через третіх осіб;
- використання пов'язаних осіб для реєстрації компаній;

Господарська діяльність учасника

- новостворений суб'єкт підприємницької діяльності;
- незначний статутний капітал;
- відсутність найманих працівників або наявність незначної кількості працівників, що не відповідає масштабам заявленої діяльності;
- юридична особа часто здійснює зміну назви або засновницько-посадовий склад;
- юридична особа часто здійснює адресу реєстрації та місця знаходження, назв компаній та основних видів діяльності;
- відсутність основних засобів, виробничих потужностей, складських приміщень та інших активів;
- ліквідація суб'єкта господарювання одразу після здійснення платежу;
- не є виробником товарів;
- відсутність ліцензій або дозволів на види діяльності, що вимагають обов'язкового ліцензування або дозволів;
- відсутність орендних платежів, якщо суб'єкт господарювання не може надати підтвердження про використання власної території або спільних приміщень для здійснення діяльності;
- реєстрація за місцем масової реєстрації;
- наявність значної кількості рахунків в різних банківських установах;
- наявність значної кількості посередників;
- відсутність деталізації в торгових угодах;

Кримінальна історія

- клієнт або його контрагенти є фігурантами кримінальних проваджень;
- учасниками операцій є громадяни з кримінальним минулим;

Негативна інформація щодо учасника

- щодо особи отримано звернення від фізичних або юридичних осіб, фінансових посередників, або інших суб'єктів про шахрайські дії клієнта (за умови наявності пов'язаних фінансових операцій та інших документів чи фактів які можуть бути використані при формуванні підозр);
- залучення шахраїв, які прикриваються волонтерською діяльністю;
- отримання чи виявлення інформації щодо особи, яка причетна до розкрадання бюджетних коштів та/або вчинення корупційних діянь;
- щодо особи наявна інформація про співпрацю з даркнет майданчиками;
- імітування офіційних урядових сайтів, використання логотипів державних установ іншими особами;

Відкриті джерела

- наявність негативної інформації щодо особи у відкритих джерелах;

Податки

- наявність податкового боргу;
- відсутність задекларованих доходів та сплачених податків;
- ухилення від сплати податків та обов'язкових платежів;
- по рахунках клієнта не сплачуються платежі, притаманні звичайній господарській діяльності;
- відсутність нарахувань та виплати заробітної плати працівникам;

Документи

- документи містять суттєві помилки, суперечності або ознаки підробки;
- ненадання клієнтом первинних документів (договорів, контрактів тощо), які пояснюють суть фінансових операцій;
- надання клієнтом сумнівних документів щодо походження подарунків від родичів.

Бюджет

- здійснення бюджетних закупівель без проведення тендеру.

5.3. Індикатори підозрілості фінансових операцій (діяльності)

За результатами дослідження встановлено наступні основні індикатори підозрілості фінансових операцій (діяльності), що використовувались у типових схемах відмивання злочинних доходів та фінансування тероризму:

Фінансування війни

- фінансові операції, пов'язані з діяльністю незаконних збройних формувань або з суб'єктами країни-агресора;
- еквайрингові операції на тимчасово окупованих територіях;
- здійснення операцій особами, які організовують, забезпечують та провокують військову агресію з боку росії;
- незвичні перекази коштів підприємствами, що знаходяться на окупованих територіях;
- транскордонні перекази до країни, про яку відомо, що вона підтримує (є нейтральною) збройну агресію росії;
- здійснення фінансових операцій на користь компаній-нерезидентів, які мають засновницькі або бізнесові зв'язки з суб'єктами росії, білорусі та інших агресорів;
- фінансові операції, пов'язані з виведенням коштів на рахунки компаній країни-агресора;
- операції з ресурсами, що походять з тимчасово окупованих територій (корисні копалини, метали, руда, зерно тощо);
- операції з культурними цінностями, що походять з тимчасово окупованих територій;

Санкції

- використання банківських карток підсанкційних банків;

НПО

- подрібнення та структурування фінансових операцій, проведення фінансових операцій без належного пояснення суті таких операцій, проведення сумнівних фінансових операцій з використанням новітніх технологій (електронні гроші, криптоактиви);
- здійснення фінансової операції з виплати електронних переказів, у яких відсутня повна інформація про ініціатора або отримувача переказу;
- необґрунтований переказ коштів на користь осіб, пов'язаних з НПО;
- фінансові операції мають заплутаний характер;
- відсутність конкретизації платежів під час залучення коштів та при подальшому їх переказі;
- здійснення НПО фінансових операцій з призначенням платежів, що не стосуються благодійної діяльності;
- переказ коштів НПО на користь юридичних осіб, діяльність яких не відповідає суті фінансової операції (виду діяльності);

- здійснення переказів за послуги, вартість яких необґрунтована;

Загальні індикатори

- значні суми перерахувань за надані послуги, вартість яких важко оцінити (агентські та рекламні послуги; послуги з підготовки документів, досліджень, з пошуку роботи тощо);
- відсутність оплати за отримані від нерезидентів товари;
- відсутність операцій притаманних звичайній господарській діяльності (виплата заробітної плати, сплата податків і зборів, оренда плата тощо);
- значний обсяг фінансових операцій з надання / отримання фінансової допомоги;
- використання професійних мереж відмивання коштів для обходу санкцій;
- дроблення платежів між одними і тими ж учасниками фінансових операцій в один день;
- використання для доступу до он-лайн банкінгу різних осіб з одних і тих же IP-адрес;
- характер фінансових операцій по рахунках, відкритих у різних банківських установах є схожим;
- відсутність або малоінформативність вебсайту;
- використання посередників в угодах;
- використання захищених безіменних рахунків;
- значний обсяг розрахунків за поштові відправлення;
- неодноразові фінансові операції за договорами відступлення прав вимоги (переведення боргу);
- анонімне переміщення коштів;

Неповнолітні особи

- наявність регулярних переказів великих сум, які перевищують звичайні потреби неповнолітньої особи. Часте поповнення рахунку неповнолітньої особи великими сумами, які не відповідають доходам родини та/або значно вищі за звичайні витрати на освіту, побут або дозвілля за віком особи;
- перекази, які проходять на значні суми через рахунок неповнолітнього та негайно пересилаються іншим одержувачам;

Бюджет

- розпорошення коштів клієнтом, які отримані від державних підприємств та інших суб'єктів, що фінансуються з державного та місцевих бюджетів, на суб'єктів з ознаками проведення підозрілої діяльності;
- відсутність розрахунків за товар, який в подальшому має бути поставлений на державне підприємство;

- фінансування бізнесу за рахунок коштів отриманих від продажу товарів, які надійшли від державного підприємства;

Корупція

- здійснення фінансових операцій з дороговартісними активами членами сімей високопосадовців та/або афільованими з ними особами;
- отримання/надання членами сімей високопосадовців та/або афільованими з ними особами значних коштів за послуги;

Транскордонні операції

- сума перерахованих коштів за кордон, значно перевищує вартість отриманих товарів;
- регулярне отримання коштів з-за кордону, без очевидної мети проведення таких фінансових операцій;
- участь у фінансових операціях пов'язаних компаній - нерезидентів;
- транзитний характер руху товарів через країни високого ризику;
- фінансові операції, пов'язані з виведенням коштів на рахунки офшорних компаній;
- відсутність оплати за отримані від нерезидентів товари;
- операції пов'язані з виведенням коштів на користь нерезидентів, які не мають відповідних ресурсів (працівників, приміщення та обладнання) для виконання умов контракту;
- здійснення міжнародних постачань з подальшою переуступкою боргу нерезидентам інших країн;
- здійснення/повернення інвестицій, виплата дивідендів, купівля-продаж майнових прав, відступлення прав вимог з метою незаконного виведення коштів;

Кримінальна історія

- звернення постраждалих осіб до правоохоронних органів;
- учасник фінансової операції оголошений правоохоронним органом у розшук;
- наявність інформації про відкрите кримінальне провадження чи судове переслідування учасника фінансової операції;

Не співпрацює з СПФМ

- учасник фінансової операції не надає пояснення щодо фінансових операцій та наявні ознаки щодо приховування джерел походження коштів;
- після звернення СПФМ щодо надання документів та пояснень відкликав платіж та закрив рахунок;

Підробка

- наявність фактів щодо підробки або фальсифікації офіційних документів;

Транзит

- транзитне проходження безготівкових коштів за рахунком (протягом короткого проміжку часу). Вхідний та вихідний залишок після проходження коштів за рахунком є мінімальним та/або нульовим;
- невідповідність отриманих доходів з обсягами проведених фінансових операцій;
- спонтанні обороти по рахунках особи (значні за обсягами обороти або повна відсутність оборотів);
- великі щоденні обороти коштів з незначним сальдо на початок та кінець дня;

Готівка

- необґрунтоване в значних розмірах використання готівки для розрахунків;
- циклічний необґрунтований рух готівкових коштів за рахунком клієнта;
- багаторазові зарахування готівкових коштів на карткові рахунки від невстановлених осіб;
- внесення готівки з сумнівних джерел (не підтверджених);
- проведення в значних обсягах фінансових операцій з готівкою, що не пов’язані з основним видом діяльності клієнта;
- фізичне переміщення готівки (кеш-кур’єри);
- зняття готівки або внесення на рахунки в різних країнах суб’єктами із зон конфліктів;
- фінансові операції з суб'єктами, які здійснюють торгівлю за готівку;

Призначення платежу

- нерозкриття інформації в призначенні платежу щодо підстав та мети переказу коштів;
- очевидна невідповідність призначень прибуткових та видаткових операцій за фінансовими операціями клієнта;
- зарахування та переказ коштів здійснюється з однаковим призначенням платежу із залученням широкого кола фізичних осіб без очевидної мети таких операцій;
- призначення платежу не відповідає звичній діяльності юридичної особи або фізичної особи-суб’єкта підприємницької діяльності;

Наявність ресурсів для ведення господарської діяльності

- відсутність обов’язкових платежів на рахунках суб’єктів підприємницької діяльності та юридичних осіб, які притаманні звичайній господарській діяльності (оренда, комунальні послуги, податки, збори тощо);

ФО з фіктивними учасниками

- використання новостворених суб'єктів господарювання або суб'єктів господарювання з ознаками «фіктивності» (клони);
- коригування дій учасників фінансових операцій («фіктивних» учасників) з єдиного центру прийняття рішення;

ФО з фіктивними іноземними компаніями

- наявні ознаки «фіктивності» іноземної компанії (компанії клону);
- кінцевим бенефіціарним власником іноземної компанії є громадян України відносно якого наявна інформація про вчинення економічних злочинів;

Невідповідність ФО

- фінансові операції клієнта не відповідають ризик профілю клієнта;
- структуровані платежі;
- платежі без найменування конкретного товару/послуги;
- придбання високовартісних активів із непідтверджених джерел;
- проведення фінансових операцій, які не мають очевидної мети;
- проведення фінансових операцій зі значною кількістю контрагентів (невідповідність діяльності учасників операцій, розпорошення активів з метою приховування фінансових потоків);
- проведення необґрунтовано великої кількості операцій з використанням рахунків, у т.ч. карткових;
- здійснення операцій з переказу на картки великої кількості фізичних осіб (A2C) без деталізації призначень платежів;
- проведення необґрунтовано великої кількості операцій або на значні суми між фізичною особою та суб'єктами грального бізнесу;
- здійснення операцій з готівкою, обсяг яких не відповідає офіційно задекларованим доходам;
- фінансові операції не мають законних джерел походження коштів;
- аномальний сплеск проведення фінансових операцій по рахунках;
- проведення фінансових операцій пов'язаних з торгівлею корисними копалинами без наявності дозволів та ліцензій на їх видобуток або не підтвердження джерела таких копалин;
- мета переказів є неочевидною або носить незвичний характер;
- отримання великої кількості платежів на свої рахунки від систем, що забезпечують проведення онлайн-платежів, за умови відсутності діяльності, пов'язаної з онлайн-маркетингом/аукціонами, або подібної діяльності;

ФО пов'язаних осіб

- проведення сумнівних фінансових операцій між групою юридичних осіб, які розташовані за адресами масової реєстрації;

- проведення сумнівних фінансових операцій між групою фізичних та/або юридичних осіб, які розташовані за спільними адресами чи мають інші спільні риси;
- фінансові операції, проведені між учасниками, які пов’язані між собою спільним посадово-засновницьким складом та метою їх операцій є маскування джерел походження коштів;
- використання афілійованих банківських установ для розрахунків;

Шахрайство

- фінансові операції клієнта пов’язані з шахрайством;

Гральний бізнес

- використання карток фізичних осіб для поповнення ігрових аккаунтів незаконних казино в мережі Інтернет та інших неліцензованих платіжних сервісах;
- перерахування коштів на рахунки значної кількості суб’єктів господарювання, які працюють під нібито одним брендом онлайн казино (представники), у т.ч. за кордон;

Криптовалюта

- здійснення розрахунків за фінансовими операціями криптовалютою;
- транзитне перерахування коштів між криптогаманцями;
- фінансові операції клієнта з придбання криптовалюти мають сумнівне джерело походження.

5.4. Найпоширеніші способи легалізації (відмивання) злочинних доходів

За результатами дослідження встановлено наступні основні способи легалізації (відмивання) злочинних доходів:

Бюджет, корупція

- перерахування коштів від державних установ та бюджетних організацій на користь юридичних осіб, які не є виробниками відповідної продукції, з метою завищення вартості контракту;
- заволодіння бюджетними коштами державної компанії з подальшим придбанням коштовної елітної нерухомості через ряд пов'язаних компаній-нерезидентів, що мають ознаки фіктивності;
- заволодіння бюджетними коштами шляхом здійснення шахрайських дій з об'єктом нерухомого майна;
- перерахування бюджетних коштів на користь юридичних осіб з сумнівною репутацією з подальшим перерахуванням на їх власні рахунки та на користь суб'єктів господарювання, призначення яких не відповідає їх профілю діяльності;
- виведення коштів з комунального підприємства під виглядом придбання майнових прав на житло для соціально-незахищених верств населення, з подальшим перерахуванням коштів за кордон на користь фіктивних компаній, та на користь оптових та роздрібних торговців алкогольною та тютюновою продукцією з метою прихованої конвертації безготівкових коштів у готівку;
- виведення коштів з державного підприємства шляхом придбання у компанії-нерезидента через посередників, обладнання за значно завищеною ціною, з подальшим розпорошенням різниці від реальної вартості, зокрема, на користь компаній пов'язаних з громадянином російської федерації який використовує власну мережу компаній для відмивання злочинних доходів;
- перерахування бюджетних коштів на користь суб'єкта господарювання, задіяного в схемах, пов'язаних з ухиленням від сплати податків, підробкою документів з подальшим їх перерахуванням за кордон на користь отримувача, пов'язаного з країною-агресором;
- надання коштів отриманих від корупційних діянь родичам за кордоном для придбання ними дороговартісних авто, ювелірних виробів, нерухомості та прибуткового бізнесу;
- виведення коштів з державних підприємств підконтрольних РЕР, шляхом оплати підприємствами послуг на користь пов'язаних з РЕР осіб, з подальшим обготівковуванням коштів та придбанням активів;
- зарахування значної суми коштів на користь юридичної особи від групи компаній підконтрольних одній особі з метою надання неправомірної вигоди представнику судової влади через третіх осіб;

Благодійна діяльність

- отримання громадською організацією грантових коштів з подальшим їх обготівковуванням та розпорошенням між пов'язаними особами;
- збір коштів з громадян на вулиці, особами одягненими у військову форму, від імені попередньо створеного ними благодійного фонду з патріотичною назвою, з подальшим використанням коштів на власні потреби;
- збір благодійним фондом пожертв від громадян України для закупівлі генераторів та продуктових наборів громадянам деокупованих територій, з подальшим переведенням коштів на особисті потреби організатором схеми;
- продаж пального пересічним громадянам, попередньо придбаного громадською організацією за рахунок благодійних внесків для потреб територіальної оборони, з подальшим зняттям прибутку готівкою та забезпечення власних потреб;
- збір коштів з фізичних осіб через громадську організацію за перебування їх родичів в реабілітаційних центрах з подальшим обготівковуванням коштів та забезпечення власних потреб учасників схеми;
- надходження благодійних пожертв від фізичних осіб та державних установ для обігріву релігійної установи, з яких частково привласнені настоятелем на власні потреби та частково в подальшому легалізовані через «професійні мережі для відмивання коштів»;
- створення особою за кордоном благодійної організації, з майже ідентичною назвою громадської організації очолюваною ним раніше в Україні, з метою подальшого збору пожертв, використовуючи бланки української громадської організації та отриманням коштів на власні потреби;
- збір коштів європейською благодійною організацією з подальшим їх перерахуванням через пов'язаних між собою українських суб'єктів господарювань та благодійних організацій на іншу групу фізичних та юридичних осіб з призначенням платежів, що не стосується благодійної діяльності;

ЗЕД

- перерахування валюти за межі України без фактичного постачання товару або часткового постачання товару неповної комплектації та неналежної якості;
- оформлення фіктивних зовнішньоекономічних контрактів з експорту готової продукції та не отримання валютної виручки;
- імпорт та подальша реалізація товарів російського походження або товарів, які виготовлені з сировини російського походження, з використанням «транзитних» іноземних компаній з ознаками фіктивності;

Готівка

- організація еквайрингових розрахунків через POS-термінал на тимчасово окупованій території з метою конвертації пенсійних виплат,

отриманих громадянами України, які проживають на тимчасово окупованій території, у готівкові російські рублі;

- переведення в готівку безготівкових коштів, отриманих як оплата за металобрухт, через рахунки юридичних осіб та групи підконтрольних фізичних осіб;
- «прихована конвертація» безготівкових коштів у готівку з використанням механізму «скрутки» товарів із залученням реально діючих оптових та роздрібних торгівців, які можуть мати необліковану готівку;
- вивезення готівкових коштів з України із залученням кеш-кур'єрів, з подальшим декларуванням готівки за кордоном та придбанням автомобілів, внесенням коштів на власні рахунки та на користь підконтрольних компаній;

Переуступка прав вимог, цінні папери

- переуступка права вимоги «штучно» створеного боргу за поставленим товаром та його погашення без фактичної оплати (зарахування зустрічних однорідних боргових зобов'язань між сторонами) під виглядом передачі у власність «сміттєвих» цінних паперів, частки у статутному капіталі підприємства з ознаками фіктивності;
- збір коштів на рахунки фізичних та юридичних осіб, отриманих у якості міжнародних переказів без документального підтвердження, з подальшим інвестуванням їх у нерухомість, отриманням готівки та використанням на власні потреби;

Шахрайство

- заволодіння коштами фізичних осіб (людей похилого віку) шляхом злому сторінки у соціальній мережі;
- шахрайське заволодіння коштами шляхом несанкціонованого втручання до системи «клієнт-банк» з подальшим зняттям готівки та переведенням коштів на користь онлайн казино;
- заволодіння коштами фізичних осіб, шляхом несанкціонованого доступу до телефону та масової розсилки повідомлення з проханням позичити кошти, які в день надходження на користь шахраїв розпорошувалися на невстановлених осіб;
- привласнення коштів потерпілих в результаті переходу по фішингових посиланнях з подальшим зняттям коштів готівкою, переказом на інші власні картки;

Криптовалюта, гральний бізнес

- заволодіння коштами фізичної особи під виглядом інвестицій у криптовалюту;
- шахрайське заволодіння грошовими коштами фізичних осіб шляхом обману чи зловживання довірою з подальшим розпорошенням на картки невстановлених осіб та придбанням криптовалюти;

- шахрайське заволодіння криптовалютними активами постраждалої особи з подальшим переказом через транзитні криптогаманці на користь криптовалютної біржі, яка обходила режим санкцій та обслуговувала російських користувачів;
- зарахування коштів від користувачів нелегальних гральних платформ на банківські картки «дропів»;
- використання суб'єктами грального бізнесу рахунків підставних юридичних та фізичних осіб з метою ухилення від сплати податків та переведення безготівкових коштів у готівку, шляхом сплати за неконкретизовані та розмиті за змістом послуги, вартість та факт надання яких неможливо перевірити;

Торгівля зброєю, наркотиками

- готівкові та безготівкові зарахування від неідентифікованих осіб на рахунки групи фізичних осіб, які причетні до незаконного виготовлення та збуту вогнепальної зброї та боєприпасів до неї, з подальшим транзитом коштів іншим особам, переведенням в готівку та придбанням товарів/послуг;
- підозрілі зарахування, які можуть бути пов'язані з реалізацією наркотичних засобів, на картковий рахунок фізичної особи – працівника медичного закладу, з подальшим перерахування іншим особам та частковим переведенням в готівку;
- використання карткових рахунків фізичних осіб для проведення фінансових операцій з коштами, здобутих від незаконного обігу наркотичних та психотропних препаратів;

Культурні цінності

- незаконне заволодіння та переміщення за межі України, з метою подальшої реалізації об'єктів матеріальної культури.

5.5. Найпоширеніші способи фінансування війни та тероризму

До найпоширеніших способів фінансування війни та тероризму можливо віднести наступні:

Перекази

- перерахування коштів особами з країн з підвищеною терористичною загрозою та осіб, причетних до терористичної діяльності, через міжнародні системи грошових переказів на користь фізичних осіб за послуги;
- здійснення грошових переказів на користь осіб, які мають проросійську позицію, є колаборантами, коригувальниками вогню, агітаторами «руського міра», пропагують російські наративи, виправдовують військову агресію та заперечують тимчасову окупацію частини території України тощо;
- проведення регулярних переказів коштів від підконтрольних громадянам росії компаній-нерезидентів та російських рахунків напередодні та під час вторгнення росії в Україну на користь компанії, керівником та власником якої виступає уродженець росії;
- отримання неповнолітніми особами коштів за підпал автомобілів військовослужбовців України та/або передачу інформації спецслужбам росії;

Благодійна діяльність

- збір грошової (благодійної) допомоги для надання коштів бойовикам через афілійовані структури (НПО) та фізичних осіб під «фейкові» благодійні проєкти з використанням соцмереж;

Колаборaційна діяльність

- перерахування коштів особою-колаборантом, за корпоративні права підприємства, що належить пов’язаній з ним особі, яка в свою чергу здійснює контроль за діяльністю автозаправних станцій, дохід від яких може бути направлений агресором на фінансування повномасштабної війни;
- внесення особою-колаборантом та членами його сім’ї готівкових коштів у значних обсягах, ймовірно від колаборaційної діяльності, з подальшим придбанням елітної нерухомості, дороговартісних автомобілів, оплати навчання дітей за кордоном;
- колаборaційна діяльність та отримання незаконних доходів від діяльності телеграм-каналу, на якому розміщувались персональні дані громадян України, в тому числі військовослужбовців, отримані внаслідок несанкціонованого втручання в роботу закритих реєстрів державних органів;

Тимчасово окуповані території

- здійснення еквайрингових операцій на тимчасово окупованих територіях через термінали українських банків;

- фінансування підприємством, перереєстрованим за законодавством росії, робіт з підготовки російських бойовиків та ремонту військової техніки збройних сил росії на тимчасово окупованій території України;

КБВ

- перерахування коштів на користь компаній-нерезидентів з різних країн, бенефіціарні власники яких пов'язані з росією/білоруссю;

Дропи

- отримання грошових коштів для здійснення диверсійної діяльності на об'єктах критичної інфраструктури України з використанням карток фізичних осіб з ознаками «дропів»;

Криптовалюта, гральний бізнес

- переказ криптовалюти від різних фізичних осіб, у т.ч. від громадян росії, на криптовалютний гаманець фізичної особи, яка є студентом, не працює, не отримує постійного доходу, в якості оплати незаконної діяльності;
- використання доходів, отриманих від онлайн казино та операцій з криптовалютами, для фінансування незаконної діяльності;
- придбання фізичною особою з подвійним громадянством, криптовалюти з подальшим спрямуванням її через транзитні криптогаманці на криптогаманець проросійської групи;
- використання послуг «інтернет-еквайрингу» для зарахування коштів від гравців азартних ігор, з подальшим перерахуванням через рахунки юридичних осіб та групи підконтрольних фізичних осіб, у т.ч. на користь онлайн казино за кордоном, бенефіціарними власниками яких є представники країни-агресора;

Обхід санкцій

- виплата дивідендів, повернення позик та інвестицій українськими компаніями на користь громадян російської федерації через довірених осіб та родичів громадян росії, які формально виступали бенефіціарними власниками українських компаній, з метою приховування реальних бенефіціарів та подальшим придбанням високоліквідних активів за кордоном;
- придбання підприємством в автосалоні автомобілів преміумкласу з подальшим їх переоформленням на підставних фізичних осіб та переміщенням через країни ЄС та СНД для збуту на території росії;
- укладання зовнішньоекономічних контрактів з іноземними компаніями-прокладками, які пов'язані з росією.

ВИСНОВОК

Збройна агресія росії проти України створила комплексний набір викликів, які охоплюють широкий спектр загроз, пов'язаних із злочинами, відмиванням доходів та фінансуванням тероризму. Росія активно використовує різноманітні схеми, обходить міжнародні санкції, застосовує сучасні технології (криптовалюту), а також вдається до кіберзлочинів та корупційних дій як інструментів ведення гібридної війни.

Головною загрозою для України є агресія з боку Росії та діяльність злочинців, які займаються відмиванням коштів. Основні загрози та ризики включають: фінансування тероризму, захоплення росією активів, корупційні злочини, залучення НПО до незаконної діяльності, транскордонне відмивання коштів, використання готівки в схемах ВК, незаконний обіг культурних цінностей, шахрайство та кіберзлочинність, використання віртуальних активів в незаконній діяльності, а також торгівлю зброєю, людьми та наркотичними засобами, професійних «відмивачів коштів».

Злочинці постійно вдосконалюють свої методи в схемах ВК/ФТ, адаптуючи їх до сучасних реалій. Глобалізація процесів підвищує їх масштаб і складність, вимагаючи швидких та інноваційних підходів до протидії.

Особливо тривожним є залучення вразливих груп населення, зокрема неповнолітніх осіб.

У 2024 році спостерігається еволюція схем відмивання коштів, зокрема активізація діяльності так званих професійних «відмивачів коштів» як глобального тренду. Ці особи або організації спеціалізуються на наданні послуг з легалізації доходів, отриманих злочинним шляхом, а також на виконанні інших незаконних фінансових операцій. Ключовим елементом їхніх схем є залучення підставних осіб, так званих «дропів», для проведення транзакцій або відкриття рахунків, що ускладнює процес ідентифікації кінцевих бенефіціарів.

Держфінмоніторинг, як фінансова розвідка, активно протидіє ризикам, фінансовим злочинам та фінансування тероризму, зміцнюючи фінансову безпеку країни.

Результати дослідження мають практичне значення для проведення аналізу, розслідувань, виявлення та оцінки ризиків, клієнтського моніторингу, регуляторних заходів і вдосконалення стратегій та законодавства з ПВК/ФТ/ФРЗМЗ.

ПОПЕРЕДНІ ТИПОЛОГІЧНІ ДОСЛІДЖЕННЯ

Попередні типологічні дослідження Держфінмоніторингу забезпечують розуміння змін та трансформацій у типологіях ВК/ФТ/ФРЗМЗ. Ці дослідження висвітлюють методи, схеми та інструменти, що використовуються для незаконної фінансової діяльності.

Типологічні дослідження мають практичне значення:

- суб'єкти первинного фінансового моніторингу використовують ці дані для підвищення ефективності внутрішніх процедур та моніторингу.
- суб'єкти державного фінансового моніторингу використовують для розуміння тенденцій та схем;
- правоохоронні та розвідувальні органи отримують актуальні схеми для розслідування фінансових злочинів.

Зміни в законодавстві значно посилили аналітичні спроможності Держфінмоніторингу та як наслідок зробили типологічні дослідження більш комплексними, актуальними та ефективними.

Фінансування тероризму. Протягом 2014, 2017, 2022, 2023 та 2024 років особлива увага Держфінмоніторингом приділялася дослідженню актуальних загроз, пов'язаних із фінансуванням тероризму, зокрема у контексті військової агресії та посилення санкційного тиску.

Перелік типологічних досліджень Держфінмоніторингу

Рік	Тематичний напрямок	Тема типологічного дослідження
2024	ВК/ФТ	«Ризики та загрози легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансування тероризму в умовах військової агресії російської федерації – 2024»
2023	ВК/ФТ	«Ризики та загрози легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансування тероризму в умовах військової агресії російської федерації»
2022	ВК/ФТ	«Фінансування тероризму та отримання кримінальних доходів від вчинення інших злочинів в умовах військової агресії російської федерації»
2021	загальна	«Актуальні методи, способи, інструменти легалізації (відмивання) злочинних доходів та фінансування тероризму (сепаратизму)» (2021 рік)
2020	податки	«Відмивання доходів від податкових злочинів»
2019	бюджет	«Відмивання доходів від привласнення коштів і майна державних підприємств та інших суб'єктів, які фінансуються за рахунок державного та місцевих бюджетів»

Типологічне дослідження «Ризики та загрози легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансування тероризму в умовах військової агресії російської федерації – 2024»

Рік	Тематичний напрямок	Тема типологічного дослідження
2018	бенефіціари	«Ризики використання суб'єктів з непрозорою структурою власності у схемах відмивання кримінальних доходів»
2017	готівка	«Ризики використання готівки»
2017	ФТ	«Ризики тероризму та сепаратизму»
2016	корупція	«Відмивання доходів, отриманих від корупційних діянь»
2015	загальна	«Типові інструменти, способи та механізми розміщення і відмивання кримінальних доходів»
2014	ФТ	«Актуальні методи, способи та фінансові інструменти фінансування тероризму та сепаратизму»
2013	кібер	«Кіберзлочинність та відмивання коштів»
2012	загальна	«Актуальні методи і способи легалізації (відмивання) доходів, одержаних злочинним шляхом, та фінансування тероризму»
2011	готівка	«Використання готівки у схемах відмивання злочинних доходів»
2010	небанки	«Типології легалізації (відмивання) доходів, одержаних злочинним шляхом, через небанківські фінансові установи із залученням коштів та інших активів громадян
2009	готівка	«Властивості та ознаки операцій, пов'язаних з відмиванням коштів шляхом зняття готівки. Тактичне дослідження та практичне розслідування»
2008	нерухомість	«Типології легалізації (відмивання) доходів, одержаних злочинним шляхом, через ринок нерухомого майна»
2007	цінні папери	«Типології легалізації (відмивання) доходів, одержаних в результаті здійснення фінансових операцій з неліквідними цінними паперами»
2006	загальна	«Типології легалізації (відмивання) доходів, одержаних злочинним шляхом, в 2005-2006 роках»
2005	загальна	«Типології легалізації злочинних коштів в Україні в 2004 - 2005 роках»

ДОДАТОК. ІНСТРУМЕНТИ, ТЕХНОЛОГІЇ, РЕСУРСИ ДЛЯ КОНТРОЛЮ ТА МОНІТОРИНГУ

1. АНАЛІТИЧНІ ІНСТРУМЕНТИ ТА АНАЛІТИЧНІ ПЛАТФОРМИ

Аналітичні інструменти та аналітичні платформи забезпечують аналіз даних, виявлення ризиків та допомагають у протидії фінансовим злочинами.

Технічні рішення суттєво еволюціонують, стаючи більш інноваційними, адаптивними та інтегрованими, що відповідає викликам розвитку технологій, збільшення обсягів даних та зростання складності фінансових злочинів.

Інтелектуальні технології. Сучасні рішення використовують потужності штучного інтелекту (ШІ), машинного навчання та автоматизації, що дозволяє значно прискорити процес аналізу, підвищити точність прогнозів і забезпечити прийняття обґрунтованих рішень у реальному часі.

Інтеграція даних. Інтеграція даних із різних джерел, таких як глобальні бази даних, відкриті джерела та санкційні списки, у поєднанні з можливостями ШІ сприяє більш ефективному моніторингу ризиків та виявленню підозрілих фінансових операцій (підозрілих транзакцій).

Адаптивність. Значення аналітичних інструментів та платформ полягає у їхній здатності забезпечувати гнучкість, інтерактивність та адаптивність до нових викликів у сфері фінансових злочинів та до нових регуляторних вимог.

Фактично вони виступають основою для забезпечення прозорості, безпеки та дотримання глобальних регуляторних стандартів.

Основні напрямки розвитку:

- **автоматизовані системи перевірки клієнтів (KYC).** Мінімізація ризиків помилкової ідентифікації. Аналіз даних з державних реєстрів, відкритих джерел тощо;
- **інтеграція санкційних списків**. Перевірка клієнтів та їх транзакцій на відповідність санкційним спискам, виявлення осіб, які обходять санкції через складні фінансові схеми;
- **відкриті джерела (OSINT). В**икористання відкритих даних (з публічних реєстрів, засобів масової інформації, соціальних мереж та інших джерел) дає змогу збирати додаткову інформацію про клієнтів та учасників операцій. Виявляти потенційні ризики, які не відображені у наявних базах даних;
- **впровадження ризикових моделей.** Такі моделі повинні враховувати унікальні характеристики клієнтів та їхню взаємодію з фінансовою системою. Використання поведінкових даних сприяє запровадженню точних моделей оцінки ризиків, враховуючи динаміку дій клієнтів;

- **автоматизовані системи моніторингу транзакцій.** Моніторинг та аналіз конкретних фінансових операцій клієнта для виявлення підозрілих транзакцій. Моніторинг передбачає використання алгоритмів виявлення аномалій у транзакціях відповідно до індикаторів, фільтрацію за правилами, такими як сума операції, країна, учасники тощо;
- **динамічний моніторинг транзакцій у реальному часі.** Передбачає загальний контроль фінансових потоків та охоплює постійне спостереження за всіма транзакціями в системі в реальному часі. Забезпечує оперативне виявлення та реагування на аномалії, що можуть свідчити про шахрайство, ВК або інші підозрілі дії. Динамічний моніторинг передбачає автоматизовані оповіщення та блокування транзакцій у разі виявлення загроз та може використовувати результати роботи автоматизованих систем перевірки транзакцій;
- **сценарний аналіз із використанням ШІ**, який здатний прогнозувати потенційні загрози та моделювати майбутні ризики;
- **інтеграція даних із криптовалютних платформ** для формування ризиків. Інформація з криптовалютних бірж та блокчейнів забезпечить: виявлення зв'язків між криптовалютними гаманцями та нелегальними операціями; відстеження транзакцій у криптовалютах для ідентифікації підозрілих потоків коштів;
- **розширення можливостей автоматизації звітності**, що спрощує підготовку регуляторних звітів і забезпечує відповідність глобальним стандартам.

Для забезпечення ефективного фінансового моніторингу та управління ризиками СПФМ використовують сучасні інструменти та підходи, які включають:

<u>скорингові моделі</u>

Моделі запобігання ризикам використовуються для виявлення клієнтів із ознаками сумнівності на етапі встановлення ділових відносин. Оцінка ризиків за типами клієнтів: враховує особливості юридичних осіб, фізичних осіб та ФОП, а також операційну історію та географічні зв'язки.

<u>розроблені матриці розрахунку рівня ризику публічних осіб</u>

Застосовування матриці розрахунку рівня ризику публічних осіб дозволяє оцінити репутаційні та фінансові ризики клієнтів.

Ключові елементи матриці ризику розрахунку рівня ризику публічних осіб можуть бути:

<u>Посада та рівень політичної значущості</u>. Оцінка клієнтів за їхнім статусом (національний чи міжнародний рівень впливу) та аналіз пов'язаних осіб (членів сім'ї, близьких партнерів);

Фінансова діяльність**.** Виявлення джерел доходів для визначення їхньої прозорості. Оцінка походження активів, зокрема, великих фінансових потоків.

Географічні ризики. Аналіз країни походження або основної діяльності клієнта, зокрема, юрисдикцій із підвищеним рівнем корупції або ризиком фінансових злочинів.

Репутаційні фактори. Моніторинг відкритих джерел (OSINT), новин та інших публікацій та санкційних списків дозволяє виявляти інформацію про минулі випадки корупції, шахрайства чи інших ризикових дій, забезпечуючи всебічну оцінку репутації та потенційних загроз, пов'язаних із клієнтом.

Динаміка фінансової активності. Аналіз змін у транзакціях чи поведінці клієнтів, особливо публічно значущих осіб (PEP), дозволяє ідентифікувати аномалії, такі як раптове збільшення обсягів операцій або використання нових напрямків. Врахування рівня ризику PEP включає оцінку їхньої репутації, джерел доходів та можливих зв'язків із корупційними чи ризикованими діями.

скринінгові моделі виявлення потенційно високоризикових клієнтів

Ці моделі значно підвищують ефективність фінансового моніторингу, мінімізують ризики співпраці з неблагонадійними клієнтами та забезпечують відповідність регуляторним вимогам у сфері ПВК/ФТ.

Скринінгові моделі дозволяють швидко ідентифікувати осіб із підозрілою репутацією, зв'язками із кримінальними угрупованнями чи іншими ризиковими суб'єктами. Вони використовують фільтри та алгоритми для оцінки клієнтів за низкою показників, таких як країна походження, сфера діяльності, історія транзакцій та взаємозв'язки. Такі моделі передбачають перевірку інформації щодо клієнтів (ім'я, адреса, вид діяльності) у різних базах даних.

різноманітні звіти та власні сценарії відбору підозрілих фінансових операцій (діяльності)

Такі звіти та власні сценарії відбору підозрілих фінансових операцій є одним із інструментів фінансового моніторингу, що дозволяє систематизувати дані, аналізувати транзакції та ідентифікувати потенційно ризикові дії клієнтів.

Правила відбору фінансових операцій можливі за наступними полями: дата здійснення операцій, призначення платежу, сума, рівень встановленого ризику, країна, інформація щодо типу рахунку тощо. СПФМ також проводять сценарний аналіз, який охоплює дослідження загального руху активів та аналіз окремих фінансових операцій клієнтів у динаміці.

СПФМ інтегрують до своїх аналітичних систем додаткові дані про учасників операцій та іншу інформацію, що суттєво розширює обсяг доступних для аналізу відомостей.

Використання автоматизованих систем

В умовах війни, викликаної агресією росії, виявлення фінансових операцій, що підлягають моніторингу, стає ще більш критичним завданням.

Використання автоматизованих систем, які включають аналіз критеріїв ризику та індикаторів підозрілості, дозволяє своєчасно ідентифікувати операції, пов'язані з фінансуванням незаконних збройних формувань.

Це допомагає виявляти обходи санкцій та інші ризикові дії, що підривають економічну та національну безпеку України, забезпечуючи ефективне виконання завдань СПФМ в умовах підвищених загроз.

Приклад реквізитів для встановлення сценарію відбору підозрілих фінансових операцій (діяльності) клієнта

Сценарій відбору підозрілих фінансових операцій клієнта базується на аналізі профілю особи та його фінансової діяльності, що відхиляється від звичайного поведінкового профілю або містить ознаки, притаманні типологіям ВК/ФТ.

Щодо профілю та фінансових операцій клієнта:

зв'язки з агресором

- наявність зв'язків з країнами, які причетні до військової агресії проти України;

загальна інформація про клієнта

- регулярні зміни у реєстраційних документах, включаючи часті зміни адреси чи назви компанії;
- країна реєстрації клієнта. Наприклад, до таких юрисдикцій належать країни, що внесені до списків FATF як зони з високим ризиком, або ті, які мають репутацію офшорних зон з низьким рівнем фінансової прозорості;
- розмір статутного капіталу суб'єкта господарювання, оскільки розмір може бути критерієм ризику, якщо він суттєво занижений порівняно із заявленою діяльністю чи масштабом фінансових операцій, що може свідчити про фіктивність компанії, відсутність реальних фінансових ресурсів або її використання для непрозорих операцій і транзитних схем;
- вид діяльності суб'єкта господарювання;

- кількість працівників суб’єкта господарювання як відповідність масштабам та характеру заявленої діяльності;
- період діяльності юридичної особи/вік фізичної особи, оскільки короткий період існування компанії чи молодий вік особи можуть свідчити про недостатній досвід, низький рівень репутації або навіть створення суб’єкта виключно для участі у схемах відмивання коштів чи інших непрозорих операціях;

інформація про власників та управлінців

- інформація про кінцевого бенефіціарного власника, посадово-засновницький склад суб’єкта господарювання та їх участь в інших юридичних особах (резидентність);
- інформація про зміни кінцевого бенефіціарного власника та посадово-засновницького складу суб’єкта господарювання;

юридичні аспекти

- наявність інформації про відкриті кримінальні провадження з розслідування злочинів у сфері господарської діяльності щодо власника істотної участі/контролера або юридичної особи, її керівників та/або представників;
- історія судових рішень щодо клієнта;

задекларована фінансова інформація

- використання особою необґрунтованої кількості банківських установ для проведення фінансових операцій та здійснення діяльності. За виключенням банків із високим рівнем цифровізації що може бути поясненням використання різних функціональних мобільних додатків;
- розмір доходів та сплачені податки суб’єкта господарювання;
- потенційна сума (оборот) коштів, що може бути використаний суб’єктом господарювання за допомогою послуги (продукту);
- оцінка відповідності заявленої діяльності фактичній операційній активності (за даними звітності чи зовнішніх джерел);

господарська діяльність

- наявність виробничих потужностей/торговельно-складських приміщень, інших активів, необхідних для ведення задекларованої господарської діяльності суб’єкта господарювання;

географічні та зовнішньоекономічні аспекти

- взаємодія з особами чи компаніями із санкційних списків;
- взаємодія з особами чи компаніями із високоризикових юрисдикцій;
- дані про взаємодію з суб’єктами, які зареєстровані в офшорних зонах;

технологічні аспекти

- використання криптовалютних гаманців та участь у криптовалютних транзакціях;

- ідентифікація криптовалютних гаманців, пов’язаних із нелегальними транзакціями;

відкриті джерела (OSINT)

- залученість особи до сумнівних дій, що можуть вплинути на його репутацію та підвищити ризик за даними із відкритих джерел інформації (OSINT);

аналіз цифрових слідів: електронні адреси

- необґрунтоване використання однієї електронної адреси кількома особами може свідчити про спробу приховати справжніх бенефіціарів чи зв’язки між суб’єктами. Така практика часто вказує на фіктивність компаній, номінальне керівництво або контроль одного власника над кількома організаціями. Використання однієї адреси для різних суб’єктів господарювання може створювати ризик шахрайських дій, порушення регуляторних норм або участі у схемах відмивання коштів;
- використання доменів електронних адреси, які можуть бути пов’язані із сервісами розташованими у ризикових або підозрілих географічних зонах. Наприклад, домени, зареєстровані в країнах із високим ризиком корупції чи причетних до військової агресії;
- використання тимчасових або анонімних доменів (наприклад, @mailinator.com, @protonmail.com) може свідчити про спроби уникнути ідентифікації;

аналіз цифрових слідів: IP-адрес

- необґрунтоване використання інструментів для анонімізації транзакцій, таких як VPN або Tor. Приховування реального розташування;
- невідповідність IP-адреси заявленій локації клієнта або часте використання IP-адрес із різних країн. Регулярне переміщення за даними IP-адрес між різними географічними зонами без очевидної причини.

Щодо фінансових операцій клієнта:

структурування та уникнення моніторингу

- спроби структурувати фінансових операцій для обходу порогових значень особою для уникнення моніторингу транзакцій;
- велика кількість однотипних транзакцій за короткий період (наприклад, багато переказів невеликих сум із метою структуризації операцій);

баланс та рух коштів

- значний дисбаланс між кредитовими та дебетовими операціями (наприклад, великі обсяги вхідних коштів без відповідного руху на вихід);
- постійний «нульовий» баланс наприкінці дня за рахунком, що може вказувати на транзитний характер операцій;
- різке збільшення активності на рахунку та проходження за рахунком значних сум після тривалого періоду низької активності;

сутність операцій

- проведення систематично фінансових операцій суб'єктом господарювання без зазначення суті платежу в полі призначення платежу. Наприклад, без посилань на відповідні договори чи конкретні зобов'язання;

контрагенти та пов'язані рахунки

- наявність фінансових операцій із рахунками інших осіб, які часто асоціюються з підозрілими операціями, фігурують у розслідуваннях або внесені до переліку заблокованих чи зупинених, а також щодо яких наявна негативна інформація;

фінансова діяльність неповнолітніх осіб

- проведення операцій на значні суми, які не можуть бути обґрунтовані статусом неповнолітньої особи;
- наявність регулярних переказів великих сум, які перевищують звичайні потреби неповнолітньої особи. Часте поповнення рахунку неповнолітньої особи великими сумами, які не відповідають доходам родини та/або значно вищі за звичайні витрати на освіту, побут або дозвілля за віком особи;
- перекази, які проходять на значні суми через рахунок неповнолітнього та негайно пересилаються іншим одержувачам;
- використання рахунку неповнолітньої особи для тимчасового зберігання коштів у значних розмірах.

Для виявлення фінансових операцій, які можуть бути пов'язані з ВК/ФТ/ФРЗМЗ, СПФМ дедалі частіше використовують сучасні програмні комплекси.

Ці системи базуються на автоматизованих алгоритмах і сценаріях, що дозволяють ідентифікувати підозрілі операції на основі заданих критеріїв.

Програмні рішення B2:FinMon, АБС SCROOGE, САБ SrBank та AML.Point пропонують інструменти для автоматизації фінансового моніторингу. Зазначений перелік програмних рішень може бути доповнений відповідно до розвитку ринку ІТ-продуктів в Україні у сфері фінансового моніторингу.

Такі рішення мають забезпечувати своєчасне та повне виконання обов'язків СПФМ, сприяючи ефективному управлінню ризиками ВК/ФТ/ФРЗМЗ.

2. ПУБЛІЧНІ ІНФОРМАЦІЙНІ РЕСУРСИ КОНТРОЛЮЮЧИХ (ДЕРЖАВНИХ) ОРГАНІВ ТА ПРИВАТНИХ ОРГАНІЗАЦІЙ

У сучасних умовах автоматизація збору та аналізу даних з відкритих джерел стала важливим елементом для забезпечення прийняття ефективних управлінських рішень.

Для мінімізації ризиків ВК/ФТ/ФРЗМЗ суб'єкти первинного фінансового моніторингу активно інвестують в інформаційні та комунікаційні технології, що забезпечують стійкість до загроз, підвищують ефективність роботи та зміцнюють довіру клієнтів.

У 2024 році акцент робиться на розширенні можливостей автоматизованих інструментів і використанні новітніх технологій для отримання найбільш релевантної інформації. Сучасні технології вже дозволяють проводити пошук та аналіз даних із відкритих джерел для тисячі значень за один клік. Це досягається завдяки інтеграції інноваційних рішень, які забезпечують високу швидкість обробки інформації, масштабованість та автоматизацію процесів.

Отримання даних із відкритих джерел є невід'ємною складовою ефективного аналізу схем ВК/ФТ/ФРЗМЗ. Такий підхід до збору інформації дозволяє значно покращити аналітичні процеси, забезпечуючи глибше розуміння ризиків, виявлення аномалій та створення дієвих рішень для протидії фінансовим злочинам.

Збір інформації OSINT. Базовим напрямком збору інформації OSINT залишається використання пошукових систем, спеціалізованих баз даних та аналітичних платформ, що дозволяють ефективно опрацьовувати великі обсяги даних і отримувати релевантну інформацію.

Вибір системи залежить від цілей OSINT, а для кращих результатів варто комбінувати кілька пошукових платформ.

Для широкого пошуку ефективно використовувати глобальні пошукові системи, такі як Google, Bing чи DuckDuckGo, а для регіональних запитів доцільно звертатися до спеціалізованих платформ, орієнтованих на локальний контент. Спеціалізовані завдання виконують Shodan, а для конфіденційності варто обирати StartPage або DuckDuckGo. Пошук стає значно ефективнішим завдяки застосуванню пошукових операторів, спеціалізованих функцій і

плагінів, які дозволяють отримувати максимально релевантні результати з мінімальними зусиллями.

Держфінмоніторинг регулярно виявляє публічні інформаційні джерела для отримання додаткової інформації. Корисні посилання наводяться у типологічних дослідженнях відповідно до їх тематики.

Актуальні відкриті джерела, що стосуються широкого кола питань наведено нижче.

2.1. Тероризм

Тероризм	
Держфінмоніторинг https://fiu.gov.ua/pages/dijalnist/protidija-terorizmu/perelik-teroristiv	Перелік осіб, пов'язаних з провадженням терористичної діяльності або стосовно яких застосовано міжнародні санкції
Сайт «Миротворець» https://myrotvorets.center	Центр дослідження ознак злочинів проти національної безпеки України, миру, безпеки людства та міжнародного правопорядку.
Державний департамент США https://www.state.gov/country-reports-on-terrorism-2/	Перелік країн, що підтримують тероризм.
Офіс Генерального прокурора України https://gp.gov.ua/detectable	**Список підозрюваних магістральної справи «24 лютого»** «Магістральна» кримінальна справа щодо повномасштабного вторгнення росії в Україну.
Служба безпеки України https://ssu.gov.ua/	Розшук осіб, які звинувачуються у вчиненні злочинів проти основ національної безпеки.

Реєстр російських воєнних злочинців https://rwc.shtab.net/	Громадська організація «Антикорупційний штаб» разом зі «Слідство.Інфо» створили онлайн-мапу «Російські воєнні злочинці». Онлайн-реєстр містить персональні дані військових російської армії, ідентифікованих осіб полонених росіян, а також вбитих під час війни в Україні росіян.

Рух ЧЕСНО	**Реєстр зрадників**
https://www.chesno.org	База даних про українських державних зрадників: політиків, медійників, юристів та правоохоронців. Дізнайтесь імена колаборантів і повідомляйте про факти співпраці з ворогом. Рух ЧЕСНО – це громадська організація з експертизою у сферах парламенту і місцевого самоврядування, політичних фінансів та виборів.

2.2. Списки РБ ООН

	Зведений список Ради Безпеки ООН

Рада Безпеки ООН	
https://www.un.org/securitycouncil/content/un-sc-consolidated-list https://scsanctions.un.org/search/	Зведений перелік фізичних і юридичних осіб, до яких застосовуються заходи, введені Радою Безпеки ООН.

2.3. Дані щодо фізичних осіб

Дані щодо фізичних осіб

http://wanted.mvs.gov.ua/searchperson	**Міністерство внутрішніх справ України** Особи, які переховуються від органів влади. Набір даних містить інформацію щодо осіб, які переховуються від органів влади. Інформація в наборі розділена на окремі ресурси, кожен з яких відповідає вказаній щодо нього інформації.
https://corruptinfo.nazk.gov.ua	**Національне агентство з питань запобігання корупції** Єдиний державний реєстр осіб, які вчинили корупційні або пов'язані з корупцією правопорушення.
YouControl https://youcontrol.com.ua	Система YouControl дозволяє перевіряти фізичних осіб на ризики через модуль «Перевірка фізичних осіб». Система надає актуальні та історичні дані з офіційних та відкритих джерел, включаючи судові рішення, санкції, політично значущих осіб, недійсні документи, борги, люстрованих осіб, розшук та терористів. Функція моніторингу щодня сповіщає про зміни у реєстрах.

Доступна інформація про фігурантів журналістських розслідувань, бази «ДержЗрадники» та «Миротворець».

«Експрес-аналіз» для фізичних осіб – інноваційний модуль в системі YouControl для швидшої, простішої та ефективнішої перевірки. Створений на основі більше 100 відкритих джерел та більше 70 факторів обачності, «Експрес-аналіз» фізичних осіб дозволяє миттєво отримати резюмовану інформацію про особу та оцінити рівень уваги, який варто приділити її подальшій перевірці.

Опендатабот https://opendatabot.ua	Opendatabot надає доступ до державних реєстрів України, дозволяючи перевіряти штрафи, наявність арештів на автомобілі, інформацію про нерухомість, а також перевіряти осіб за ІПН та у базах розшуку.

2.4. Перевірка чинності документів

	**Перевірка чинності документів**

Державна міграційна служба України (ДМСУ) https://dmsu.gov.ua/services//nd.html	База даних недійсних, викрадених або втрачених документів, що посвідчують особу.

Міністерство внутрішніх справ України (Єдиний державний веб-портал відкритих даних) https://dmsu.gov.ua/services/nd.html	Перевірка за базою недійсних документів.

2.5. Санкції

Міністерство економіки України http://www.me.gov.ua/SpecialSanctions/List?lang=ukUA&showFrgn=True&company=linge	**Міністерство економічного розвитку та торгівлі України** Перелік осіб, до яких застосовані спеціальні санкції.

Апарат РНБО Апарат РНБО України https://drs.nsdc.gov.ua/	**Державний реєстр санкцій** Реєстр створено з метою надання безоплатного публічного доступу до актуальної та достовірної інформації про суб'єктів, щодо яких застосовано санкцій.

Міністерство фінансів США	OFAC публікує список осіб і компаній, які належать, контролюються або діють за чи від імені цільових країн. Санкції, пов'язані з Україною та росії. У списку також перераховані окремі особи, групи та організації, зокрема, терористи та торговці наркотиками, визначені в рамках програм, які не стосуються конкретної країни. У сукупності такі особи та компанії називаються «спеціально призначеними громадянами» або «SDN». Їхні активи заблоковані, і громадянам США, як правило, заборонено мати з ними справу.
https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-list-data-formats-data-schemas https://sanctionssearch.ofac.treas.gov/ https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information/ukraine-russia-related-sanctions	
Sanctions List Monitor	Sanctions List Monitor є частиною портфоліо послуг із запобігання фінансовим злочинам, спрямованих на зменшення витрат і ризиків, пов'язаних із дотриманням законодавства. Sanction List Monitor – це безплатна служба SWIFT для користувачів, яка негайно повідомляє електронною поштою про зміни в певних списках санкцій.
https://www.swift.com/our-solutions/compliance-and-shared-services/financial-crime-compliance/sanctions-solutions/sanctions-list-monitor	

OpenSanctions	OpenSanctions – це міжнародна база даних осіб і компаній, які мають політичні, кримінальні чи економічні інтереси. Проєкт об'єднує санкційні списки, бази даних політичних діячів та іншу інформацію про осіб, що становлять суспільний інтерес, в єдиний, простий у користуванні набір даних.
https://www.opensanctions.org	

Фінансові санкції введені Великою Британією	На цій сторінці перераховано всі фінансові санкції, запроваджені у Великій Британії за країнами, адміністраціями чи терористичними групами, зокрема: *щодо РФ* https://www.gov.uk/government/publications/financial-sanctions-ukraine-sovereignty-and-territorial-integrity *щодо РБ* https://www.gov.uk/government/publications/financial-sanctions-belarus
GOV.UK https://www.gov.uk/government/collections/financial-sanctions-regime-specific-consolidated-lists-and-releases	

Санкції Європейського Союзу	ЄС запровадив масштабні обмежувальні заходи (санкції) проти росії, спочатку у відповідь на незаконну анексію Криму та навмисну повномасштабну агресію проти України. ЄС вимагає від росії негайного припинення військових дій, виведення збройних сил і військової техніки, поваги до територіальної цілісності, суверенітету й незалежності України.
 https://ec.europa.eu	
https://ec.europa.eu/info/business-economy-euro/banking-and-finance/international-relations/restrictive-measures-sanctions/sanctions-adopted-following-russias-military-aggression-against-ukraine_en	

Європейський Союз суттєво розширив санкції проти росії у відповідь на її військову агресію проти України, включно з визнанням окупованих територій Донецької та Луганської областей і введенням туди російських військ.

Після 24 лютого 2022 року санкції були спрямовані на ослаблення економічної бази росії, обмеження доступу до критичних технологій та ринків, щоб суттєво знизити її здатність продовжувати війну.

Одночасно посилено санкції щодо білорусі через її підтримку російської агресії, що включає надання території для розміщення військ та матеріально-технічне забезпечення. Санкції ЄС залишаються ключовим інструментом протидії агресору.

SanctionsExplorer	SanctionsExplorer спрощує вивчення питання завдяки поєднанню даних із багатьох державних джерел. Sanctions Explorer – це проєкт, ініційований співпрацею між Archer, колишньою некомерційною організацією з Берклі, яка використовує технології для покращення прав людини та безпеки людей, і C4ADS, некомерційною організацією, яка займається проведенням досліджень глобальних конфліктів і транснаціональної безпеки на основі даних і фактів. питань. Ітерація SanctionsExplorer була повністю розроблена командою даних і технологій C4ADS і призначена для поєднання поточних і історичних даних про санкції в усіх основних органах, що накладають санкції.
https://sanctionsexplorer.org/	

2.6. Реєстри Міністерства юстиції України

МІНІСТЕРСТВО ЮСТИЦІЇ minjust.gov.ua	**Автоматизовані системи Єдиних та Державних реєстрів, що створюються відповідно до наказів Міністерства юстиції України**

Реєстри Міністерства юстиції України	Оприлюднені дані з Єдиних та Державних реєстрів, що створюються відповідно до законодавства України.
https://nais.gov.ua/registers	
https://minjust.gov.ua/uniform_and_registry	Інформація про Єдині та державні реєстри.

2.7. Інформація Національної комісії з цінних паперів та фондового ринку

НАЦІОНАЛЬНА КОМІСІЯ З ЦІННИХ ПАПЕРІВ ТА ФОНДОВОГО РИНКУ	Національна комісія з цінних паперів та фондового ринку є державним колегіальним органом який регулює ринок цінних паперів.

https://www.nssmc.gov.ua	Сайт містить розділ «реєстри», який розкриває інформацію про діяльність з цінними паперами.
https://www.nssmc.gov.ua/for-market-participants/services/open-data/#	Інформація про власників (в т.ч. пакетів голосуючих) акцій (5 відсотків і більше) акціонерних товариств.
https://www.nssmc.gov.ua/register/nahliad/kontrolna-diialnist	Реєстри правозастосування (емітенти з ознаками фіктивності, відсутність за місцезнаходженням, заборона торгівлі ЦП на біржах тощо).
Stockmarket http://stockmarket.gov.ua	Загальнодоступна інформаційна база даних Національної комісії з цінних паперів та фондового ринку про ринок цінних паперів.
Smida http://smida.gov.ua	Інформація про діяльність фондового ринку.

2.8. Судові органи

Реєстр судових рішень

Реєстр судових рішень Стан розгляду справ	Єдиний державний реєстр судових рішень. Інформація щодо стадій розгляду судових справ.
 https://reyestr.court.gov.ua/ https://court.gov.ua/fair/	

2.9. Аналітичні платформи для перевірки компаній, які зареєстровані в Україні

Аналітичні платформи, які спрямовані на забезпечення прозорості, безпеки та ефективності в бізнесі, управлінні ризиками та прийнятті рішень.

Інтернет адреси	
https://youcontrol.com.ua https://opendatabot.ua https://vkursi.pro https://finap.com.ua https://ca.ligazakon.net https://clarity-project.info	Аналітичні платформи, які створені для роботи з відкритими даними. Забезпечують користувачів інструментами для перевірки осіб, отримання даних з державних реєстрів, баз даних та інших джерел для ефективного управління бізнес-ризиками, контролю за прозорістю діяльності, аналізу судових справ тощо.

YouControl	
https://youcontrol.com.ua/	YouControl - комплексна аналітична система для бізнес-аналітики, комплаєнсу/дью-діліджденс, Osint, належних перевірок у сфері фінансового моніторингу та оподаткування, дотримання стандартів ESG. Система YouControl агрегує дані з понад 220 відкритих надійних джерел та формує повне досьє на кожну компанію України та ФОП, відстежує зміни та візуалізує зв'язки.

Функціональні можливості системи YouControl: містить дані для перевірки іноземних компаній; дозволяє отримати актуальну інформацію про фізичну особу з офіційних джерел; автоматичний моніторинг змін відповідно до даних з реєстрів; містить базу даних українських та іноземних PEPs та пов'язаних з ними осіб (LIPs); можна перевірити інформацію про приналежність особи до міжнародних санкційних списків.

Скоринговий показник «Експрес-аналіз» досліджує діяльність підприємств за майже 600 факторами, в тому числі щодо актуальної та історичної пов'язаності з росією, Білоруссю, Іраном.

В аналітичній системі YouControl представлено понад 2 тисячі фінансово-промислових груп, що дозволяє користувачам отримувати структуровану інформацію про їхню діяльність, власників, взаємозв'язки, фінансовий стан та можливі ризики.

Також користувачам YouControl доступний інтегрований AI-чат на базі ChatGPT, який заощаджує час необхідний для аналізу досьє контрагента.

Опендатабот https://opendatabot.ua/open/russian-federation-business	Опендатабот – це інструмент для фінансового моніторингу та управління ризиками. Сервіс дозволяє аналізувати зв'язки компаній, групи компаній, перевіряти судові рішення та виявляти можливі зв'язки зі країною-агресором. Для перевірки фізичних осіб доступні різні підходи: ручна перевірка, масова обробка даних та автоматична перевірка через API.

Опендатабот спрощує процеси онбордингу та KYC, забезпечуючи відстеження змін статусу PEP-клієнтів, а також суттєвих змін у юридичних особах.

2.10. Компанії, зареєстровані в Європейському Союзі

	Реєстри підприємств – пошук компанії в ЄС. Відповідно до Директиви 2012/17/ЄС сервіс пошуку інформації охоплює бізнес-реєстри всіх країн ЄС, а також Ісландії, Ліхтенштейну та Норвегії.
https://e-justice.europa.eu/content_find_a_company-489-en.do	
Реєстри бізнесу, банкрутства та землі Інформація про бізнес, земельні реєстри та реєстри банкрутства на рівні ЄС та національному рівні.	
https://e-justice.europa.eu/514/EN/registers__business_insolvency_amp_land	
Реєстри підприємств у країнах ЄС У Європі бізнес-реєстри пропонують ряд послуг, які можуть відрізнятися від однієї держави-члена до іншої.	
https://e-justice.europa.eu/106/EN/business_registers_in_eu_countries	
Земельні книги - рівень ЄС У цьому розділі коротко обговорюються дії, вжиті для покращення координації між земельними реєстрами на європейському рівні.	
https://e-justice.europa.eu/108/EN/land_registers__eu_level	
Земельні книги в країнах ЄС Земельні реєстри в державах-членах пропонують широкий спектр послуг, які можуть відрізнятися від однієї країни до іншої.	
https://e-justice.europa.eu/109/EN/land_registers_in_eu_countries	
Реєстри банкрутства та неплатоспроможності Усі країни-члени ЄС мають реєстри неплатоспроможності та банкрутства, інформацію про які можна знайти. Ці реєстри знаходяться в процесі з'єднання та пошуку з центральної точки.	
https://e-justice.europa.eu/110/EN/bankruptcy_and_insolvency_registers	

Реєстри банкрутства та неплатоспроможності - пошук неплатоспроможних боржників в ЄС Пошук неплатоспроможних організацій, фізичних або юридичних осіб, у межах ЄС.
https://e-justice.europa.eu/246/EN/bankruptcy_amp_insolvency_registers__search_for_insolvent_debtors_in_the_eu
Реєстри бенефіціарних власників – пошук інформації про бенефіціарних власників Система взаємозв'язку реєстрів бенефіціарної власності («BORIS») — це інструмент для підключення національних центральних реєстрів, що містять інформацію про бенефіціарну власність корпоративних та інших юридичних осіб, трастів та інших типів юридичних угод.
https://e-justice.europa.eu/38590/FR/beneficial_ownership_registers_interconnection_system_boris?action=maximize&clang=en&idSubpage=1

2.11. Компанії, зареєстровані в іноземних юрисдикціях

Інформаційні ресурси щодо перевірки компаній нерезидентів

OpenCorporates	OpenCorporates публікує дані юридичних осіб. Дані беруться з національних реєстрів підприємств у 140 юрисдикціях і представлені в стандартизованій формі. Зібрані дані містять назву організації, дату реєстрації, зареєстровані адреси, імена директорів та іншу корисну інформацію.
https://opencorporates.com	

Sayari	Сервіс для бізнес-розвідки, медіа-розслідувачів та аналітичних підрозділів правоохоронних органів, орієнтований на збір документів та інформації про комерційний і фінансовий світ. Сервіс охоплює корпоративні реєстри, реєстри цивільних судових процесів, митні дані та дані про імпорт/експорт, право власності на землю та нерухомість, життєві записи, офіційні газети та державні закупівлі різних країн.
https://sayari.com	

YC World	YCWorld - міжнародна платформа для перевірки нерезидентів, що дозволяє знайти актуальну інформацію з офіційних джерел, побудувати та візуалізувати зв'язки.
https://youcontrol.world	

YC World містить інформацію про понад 76 млн фізичних осіб та 85 млн компаній з майже 300 джерел даних із 74 країн світу.

Однією з найпотужніших функцій платформи є візуалізація актуальних зв'язків на графі, яка відкриває новий рівень аналізу даних. Користувач може швидко виявляти взаємозалежності й зв'язки між різними сутностями – організаціями, фізичними особами чи подіями.

В систему YC World вбудована автоматична транслітерація, яка стає особливо актуальною у 2024 році, враховуючи зростаючу інтеграцію міжнародних бізнесів і потребу в ефективній роботі з даними різними мовами.

Ця функція забезпечує зручний пошук за назвами компаній та іменами, написаними кирилицею, автоматично конвертуючи їх у латиницю або навпаки. Така транслітерація сприяє ефективності пошуку, полегшує перевірку міжнародних контрагентів та дозволяє уникнути втрат інформації через різницю у написанні.

Система YC World автоматично підсвічує ключові загрози, такі як приналежність до PEP, наявність санкцій чи зв'язків із країнами високого ризику.

	Центр з дослідження корупції та організованої злочинності
https://www.occrp.org	

Центр з дослідження корупції та організованої злочинності – це міжнародне об'єднання засобів масової інформації та окремих репортерів, які займаються журналістськими розслідуваннями.

OCCRP систематично публікує актуальні міжнародні журналістські розслідування актуальних схем з легалізації (відмивання) доходів, одержаних злочинним шляхом, які базуються на витоку документів із різних державних та приватних структур щодо прихованої діяльності корумпованих чиновників та організованих злочинних угрупувань.

 https://aleph.occrp.org/	Глобальний архів дослідницького матеріалу для розслідувань. Платформа даних Aleph об'єднує архів поточних та історичних баз даних, документів, витоків та розслідувань. Ця мережа допомагає бачити зв'язки, знаходити вкрадені кошти, виявляти політичний вплив і розкривати корупцію.

INTERNATIONAL CONSORTIUM OF INVESTIGATIVE JOURNALISTS https://offshoreleaks.icij.org	**База даних офшорних витоків** База містить інформацію щодо офшорних компаній, фондів і трастів із розслідувань PandoraPapers, ParadisePapers, BahamasLeaks, PanamaPapers та OffshoreLeaks.

DOW JONES https://riskcenter.dowjones.com	Рішення з управління ризиками та комплаєнсу. Ресурс для перевірки структури власності.

DatoCapital en.datocapital.com	Онлайн база про компанії та їх директорів.
База містить інформацію про компанії зареєстрованих в Нідерландах, Великій Британії, Гібралтарі, Іспанії, Панамі, Каймановних Островах, Люксембурзі, Британських Віргінських Островах, Мальті, Кюрасао.	

BureauvanDijkElectronicPublishing https://www.bvdinfo.com	Масштабна реєстраційна база про компанії, що зареєстровані у різних юрисдикціях по всьому світу. Незначну інформацію можна отримати безплатно (організаційно-правова форма, місце розташування, активна/неактивна), скориставшись онлайн сервісом пошуку.

Відкритий портал даних Європейського союзу	Доступ до відкритих даних, опублікованих установами та органами ЄС.
http://data.europa.eu/euodp/en/home	

Регіон (країна)	Опис	Адреса
Австрія	Реєстр та дані фінансової звітності компаній з Австрії. Містить платний контент.	https://www.firmenbuchgrundbuch.at/fbgb/easy/fb/search
Британські Віргінські острови	Дані про компанії Британських Віргінських островів.	http://www.bvifsc.vg
Велика Британія	Судовий реєстр Верховного суду Великої Британії.	https://www.supremecourt.uk/current-cases/index.html
Велика Британія	Судовий реєстр адміністративних апеляцій Високого суду.	https://www.judiciary.gov.uk/about-the-judiciary/who-are-the-judiciary/judicial-roles/tribunals/tribunal-decisions/osccs-decisions/
Велика Британія	Реєстр компаній Великобританії.	https://beta.companieshouse.gov.uk/
Велика Британія	Інформація про компанію в Сполученому Королівстві Великої Британії та Північної Ірландії, що, поміж іншим, охоплює: (адреса, дата заснування); поточні та колишні посадові особи компанії; сканкопії документів (реєстрація, зміни посадових осіб, річні звіти тощо); інформація про обтяження; попередні назви компанії.	https://www.gov.uk/government/organisations/companies-house
Велика Британія	Інформація про нерухомість, що, поміж іншим, охоплює: відомості про майно, включно з реєстрацією права власності, номером документа про реєстрацію права власності, відомості про власника, ціну купівлі, будь-які права проходу чи проїзду через територію, а також дані про те, чи «погашена», тобто виплачена, іпотека. Аналогічні реєстри нерухомості є в Північній Ірландії (https://www.nidirect.gov.uk/articles/searching-the-land-registry) та Шотландії (https://www.ros.gov.uk/).	https://www.gov.uk/search-property-information-land-registry
Велика Британія	PrivateEyeRegistry – це аналітична платформа, створена для надання доступу до даних	http://www.private-eye.co.uk/registry

Регіон (країна)	Опис	Адреса
	про компанії, їхніх директорів та акціонерів.	
Велика Британія	У Великій Британії поліція має право встановлювати право власності на транспортний засіб через Національну базу даних поліції (PoliceNationalDatabase – PND). Державне агентство Великої Британії з реєстрації транспортних засобів і видачі посвідчень водія (UK DriverandVehicleLicensingAgency – DVLA) веде облік зареєстрованих «тримачів» автомобілів, інформацію про яких надає за «достатніх підстав», навіть якщо особа, яка потребує такої інформації, не офіцер поліції.	https://www.gov.uk/request-information-from-dvla
Велика Британія	Реєстрація повітряних суден у Великій Британії передбачає ведення реєстру та застосування засобів ідентифікації для британських власних та експлуатованих комерційних і приватних повітряних суден, до того ж реєстраційні позначення починаються з ідентифікаційного префікса «G». Реєстр веде Управління цивільної авіації Великої Британії.	http://www.caa.co.uk/Aircraft-register/G-INFO/Guidance-on-using-the-G-INFO-Database/
Велика Британія та Північна Ірландія	У цій реєстраційній базі Сполученого Королівства безкоштовно можна отримати наступну інформацію: - інформацію про компанію (адреса, дата заснування); - про діючих та колишніх посадових осіб компанії; - сканкопії документів (реєстрації, зміни посадових осіб, річна звітність тощо); - відомості про обтяження; - попередні назви компанії; - відомості щодо неплатоспроможності; - відомості про бенефіціарів.	https://beta.companieshouse.gov.uk/

Регіон (країна)	Опис	Адреса
Естонія	Реєстр електронного бізнесу є офіційним порталом Естонської держави, який містить дані всіх зареєстрованих в Естонії юридичних осіб в єдиному середовищі. Реєстратором є відділ реєстрації Тартуського окружного суду. Крім того, інформація про іноземні компанії також доступна через Європейський бізнес-реєстр.	https://ariregister.rik.ee/eng
Кіпр	Реєстр компаній Республіки Кіпр	https://efiling.drcor.mcit.gov.cy http://cy-check.com https://i-cyprus.com
Чехія	Реєстр компаній Чехії	https://rejstriky.finance.cz https://rejstrik.penize.cz
Польща	Реєстр компаній Польщі	http://infoveriti.pl
Болгарія	Реєстр компаній Болгарії	https://newregister.bcci.bg/edipub

2.12. Дані щодо транспортування або торгівлі товарами

Бази даних про міжнародні поставки є важливим інструментом для збору інформації, якщо суб'єкт пошуку займається транспортуванням або торгівлею товарами. У сфері ПВК/ФТ такі бази даних допомагають ідентифікувати ризики, пов'язані з незаконними операціями, фіктивними поставками чи обходом санкцій.

Доступ до даних про маршрути перевезень, учасників угод, обсяги та кінцевих отримувачів товарів дозволяє:

виявляти «фіктивні» операції, де поставки використовуються для легалізації незаконно отриманих коштів;

аналізувати торговельні ланцюги, пов'язані із санкційними юрисдикціями, що може свідчити про обхід міжнародних обмежень;

знаходити фінансові зловживання, наприклад, штучне завищення цін або обсягу товарів для приховування нелегальних доходів;

ідентифікувати можливі канали фінансування тероризму через незаконне використання транспорту чи логістики.

Бази даних допомагають забезпечити прозорість операцій, посилити контроль за фінансовими та логістичними потоками, а також запобігти використанню міжнародної торгівлі у злочинних схемах.

Імпортно/експортні операції	Пошук глобальних записів імпорту/експорту від митниці США. ImportGenius має повні дані про торгівлю для 18 країн. ImportGenius відстежує транспортну діяльність по всьому світу, щоб показати, що саме відбувається в імпортно-експортному бізнесі.
ImportGenius https://www.importgenius.com/	

Імпортно/експортні операції	Panjiva – це платформа, яка забезпечує прозорість глобальної торгівлі завдяки глобальному охопленню, потужним технологіям машинного навчання та динамічній візуалізації даних.
Panjiva S&P Global https://panjiva.com/	

Імпортно/експортні операції	Дані про імпорт із США, а також записи про глобальний експорт та імпорт.
Import Key https://importkey.com/	

2.13. Відстеження літаків

У 2024 році відстеження літаків залишається важливою темою. Сучасні онлайн-ресурси дозволяють здійснювати відстеження польотів у реальному часі з використанням GPS-сигналів, ADS-B та інших технологій.

Спостереження за авіацією через аеродроми та їх оточення. Використання відкритих джерел інформації (OSINT) для спостереження за авіацією, включаючи аналіз аеродромів, до яких і з яких здійснюються рейси, може стати важливим інструментом у розслідуванні злочинів, відмивання коштів та фінансування тероризму.

Відстеження авіарейсів через онлайн-ресурси, дає можливість моніторити маршрути літаків, особливо тих, які можуть бути пов’язані з підозрілими

фінансовими або терористичними операціями. Аеропорти, до яких часто прилітають літаки без явних комерційних або логістичних причин, можуть вказувати на можливу причетність до незаконних фінансових схем.

Аеродроми є ключовими точками, через які проходять великі потоки капіталу, вантажів та осіб, які можуть слугувати орієнтирами для планування розслідування чи пошуку інформації.

Одним із найважливіших ідентифікаторів літака є його хвостовий номер (реєстраційний номер). Однак, літаки можуть змінювати свої хвостові номери через перепродаж або реорганізацію авіакомпанії. В таких випадках серійний номер літака (який не змінюється протягом усього його життя) стає критично важливим для ідентифікації літака та відстеження його переміщень у майбутньому.

Атрибути для пошуку	Назва ресурсу	Посилання на сайт	Опис ресурсу
База даних реєстрації літаків			
Хвостовий номер, серійний номер	Airframes.org	airframes.org	Онлайн база даних для ідентифікації та реєстрації повітряних суден.
Фотографії повітряних суден			
Модель літака, тип повітряного судна	Planespotters.net	planespotters.net	Вебсайт з фотографіями повітряних суден, що допомагає ідентифікувати літаки.
Модель літака, хвостовий номер	JetPhotos.com	jetphotos.com	База даних з фотографіями літаків та можливістю пошуку за реєстраційним номером.
Відстеження польотів			
Номер рейсу, місце знаходження	Flightradar24	flightradar24.com	Вебсайт для відстеження польотів у реальному часі по всьому світу.
Номер рейсу, місце знаходження	ADSBExchange	globe.adsbexchange.com	Глобальна мережа для обміну даними по відстеженню літаків за допомогою ADS-B.
Номер рейсу, місце знаходження	RadarBox	radarbox.com	Платформа для відстеження рейсів та аналізу даних авіаперевезень.
Номер рейсу, місце знаходження	FlightAware	flightaware.com	Платформа для відстеження рейсів з можливістю перегляду історії польотів.

2.14. Відстеження кораблів

Кораблі також можна відстежувати за допомогою онлайн ресурсів.

Відстеження руху кораблів стає особливо актуальним в межах викриття схем обходу санкційного режиму.

Деякі російські судна почали маскувати свої подорожі, маніпулюючи навігаційним програмним забезпеченням своєї системи автоматичної ідентифікації (AIS) – системою глобального відстеження вантажів, яка допомагає суднам уникати зіткнень, затримок та інших ризиків.

Відстеження суден	Опис ресурсу
IMO https://gisis.imo.org	Глобальна інтегрована інформаційна система судноплавства.
Equasis https://www.equasis.org	База даних про судно.
MarineTraffic https://www.marinetraffic.com	Глобальна розвідка про відстеження суден.
FleenMon https://www.fleetmon.com	Відстеження суден з відкритим кодом.
VesselFinder https://www.vesselfinder.com	Відстеження та інформація з відкритим кодом.

2.15. Діяльність сумнівних інвестиційних проєктів

НАЦІОНАЛЬНА КОМІСІЯ З ЦІННИХ ПАПЕРІВ ТА ФОНДОВОГО РИНКУ www.nssmc.gov.ua https://www.nssmc.gov.ua/activity/insha-diialnist/zakhyst-investoriv	З метою захисту прав споживачів фінансових послуг Національна комісія з цінних паперів та фондового ринку здійснює моніторинг діяльності сумнівних інвестиційних проєктів.

Метою таких проєктів є заволодіння коштами громадян України шляхом надання уявлення щодо інвестування в різні фінансові активи та здійснення діяльності без відповідних дозвільних документів.

Національна комісія з цінних паперів та фондового ринку публікує на офіційному сайті інформацію про інвестиційні проєкти, які відповідають ознакам сумнівності та можуть нести загрозу втрати коштів громадян України (діяльність/інша діяльність/захист інвесторів).

2.16. Набори корисних посилань

Фінансові посередники, правоохоронні та розвідувальні органи, журналісти також покладаються на ті ж інструменти, щоб дізнатися більше про злочин, підозрюваного, організацію чи особу, яка їх цікавить.

На жаль, слід також визнати, що шахраї та злочинці можуть використовувати ті ж самі інструменти та методи. Наприклад, при створенні фальшивого посвідчення особи шахрай може об'єднати дані, отримані з даркнет-ринку, з даними, отриманими з відкритих джерел.

Посилання	Опис
https://www.maltego.com	Maltego – це гнучка розвідувальна платформа з відкритим вихідним кодом, яка може скоротити і прискорити запити. Для більш точних досліджень вона надає доступ до 58 джерел даних, дозволяє додавати дані вручну і містить бази даних з 1 мільйоном об'єктів. Функції візуалізації також дозволяють вибирати різні формати, такі як блокові, ієрархічні або кругові діаграми, а також додавати ваги та анотації для ще більш детального аналізу.
https://osintframework.com	OSINT Framework – це чудовий інструмент. Це зручніше, ніж самостійно досліджувати кожну доступну програму та інструмент, оскільки він містить все – від джерел даних до корисних зв'язків та успішних інструментів.
https://gijn.org/ru/istorii/sovety-po-poisku-tajnyh-vladelcev-podstavnyh-kompanij/	Набір корисних посилань для пошуку даних про корпорації та їх власників.

2.17. Архів Інтернету

INTERNET ARCHIVE https://archive.org	Некомерційна організація створює цифрову бібліотеку, яка дозволяє отримати доступ до цифрового архіву Інтернету та всесвітньої павутини. Платформа періодично робить скріншоти вебсторінок і зберігає їх для подальшого використання.
CachedView https://cachedview.com	Інструмент для перегляду вмісту вебсторінки. Онлайн-інструмент, що підтримується Google і деякими іншими середовищами.

2.18. Інші ресурси

rupep https://rupep.org	База даних політично значущих осіб росії. Інформація в базі базується на даних, зібраних із публічних джерел: державні сайти; офіційні державні реєстри; публікації в ЗМІ; інформація з витоку баз даних (ParadisePapers, PanamaPapers, Transbordercorruptionarchive, Aleph OCCRP тощо); профілі в соціальних мережах.
List-Org https://www.list-org.com	Основні відомості про будь-яку російську юридичну особу чи підприємця.
https://egrul.nalog.ru	Податкова служба росії. Сайт містить дані про суб'єктів господарювання.

Засоби масової інформації почали більше розслідувань, які направлені на оточення керівництва росії.

ЗМІ	Опис	Адреса
Forbes	Публікує список російських товстосумів	https://www.forbes.ru
FinancialTimes	Почали стежити за найближчим оточенням керівництва росії та заможними олігархами.	https://www.ft.com
WallStreetJournal	Почали стежити за найближчим оточенням керівництва росії та заможними олігархами.	https://www.wsj.com

Для проведення пошуку інформації (OSINT) потрібно мати певні практичні та технічні знання використання інструментів та спеціалізованих платформ. Технології дозволяють збільшити якість та кількість отриманої інформації і може покращити процедури фінансового моніторингу.

Посилання на джерела даних для проведення OSINT та підходи для його постійно змінюються, що вимагає від користувача постійно оновлювати знання.

Питання захисту особи, яка здійснює OSINT (Open Source Intelligence), є актуальним та важливим, особливо в умовах сучасного цифрового середовища. З ростом доступу до інформації, швидким розвитком технологій та збільшенням кібератак, збереження особистої безпеки стає пріоритетом для будь-якої особи, яка працює з відкритими джерелами.