РИЗИКИ ТА ЗАГРОЗИ ЛЕГАЛІЗАЦІЇ (ВІДМИВАННЯ) ДОХОДІВ, ОДЕРЖАНИХ ЗЛОЧИННИМ ШЛЯХОМ, ФІНАНСУВАННЯ ТЕРОРИЗМУ В УМОВАХ ВІЙСЬКОВОЇ АГРЕСІЇ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ

2023

Державна служба
фінансового моніторингу
України

Держфінмоніторинг створений як підрозділ фінансової розвідки та реалізує державну політику у сфері запобігання і протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення.

Держфінмоніторинг належить до різновидів фінансової розвідки так званого «адміністративного типу».

Держфінмоніторинг у своїй діяльності дотримується Принципів обміну інформацією між підрозділами фінансової розвідки Егмонтської групи від 28.10.2013 (постійно оновлюються)[1].

Ключове завдання Держфінмоніторингу полягає в збиранні, обробленні та проведенні аналізу (операційного і стратегічного) інформації про фінансові операції, що підлягають фінансовому моніторингу, інші фінансові операції або інформації, що може бути пов'язана з підозрою у легалізації (відмиванні) доходів, одержаних злочинним шляхом, фінансуванні тероризму чи фінансуванні розповсюдження зброї масового знищення.

Держфінмоніторинг встановлює принципи опрацювання одержаної від суб'єктів первинного фінансового моніторингу інформації про фінансові операції, що підлягають фінансовому моніторингу, та критерії проведення аналізу таких операцій.

У разі наявності достатніх підстав вважати, що фінансова операція або сукупність пов'язаних між собою фінансових операцій можуть бути пов'язані з ВК/ФТ/ФРЗМЗ або із вчиненням кримінального правопорушення Держфінмоніторинг подає до правоохоронних та розвідувальних органів відповідні узагальнені матеріали.

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

[1] https://egmontgroup.org/wp-content/uploads/2022/07/2.-Principles-Information-Exchange-With-Glossary_April2023.pdf

ЗАТВЕРДЖЕНО
Наказ Державної служби
фінансового моніторингу України
27.12.2023 №118

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

У типологічному дослідженні вивчено питання різновидів схем легалізації (відмивання) злочинних доходів та фінансування тероризму (сепаратизму), що вчиняються в умовах військової агресії росії, розкрито індикатори підозрілості, методи та інструменти схем ВК/ФТ/ФРЗМЗ.

Визначено важливість застосування ризик-орієнтованого підходу з метою виявлення вищевказаних злочинів та розробки стратегій для їх запобігання та протидії.

Типологічне дослідження може стати підґрунтям для виявлення та протидії поширенню злочинів, що можуть бути характерними під час війни. Дослідження 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	протидія легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму
КБВ	кінцевий бенефіціарний власник
КК України	Кримінальний кодекс України
НПО	неприбуткові організації
ПФР	підрозділ фінансової розвідки іноземної держави
РБ, білорусь	республіка білорусь
РФ, 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

Завдяки винятковій стійкості Українського народу, високому професіоналізму та героїзму Сил оборони України, єдності влади та суспільства, а також міжнародній підтримці, наша країна дає гідну відсіч повномасштабній російській агресії.

Продовженню агресії росії сприяють злочини, що зазвичай поширюються в умовах війни, зокрема, це може бути корупція, підкуп та інші.

Країна-агресор всіляко намагається обійти санкційні обмеження, що накладені на неї світовою спільнотою. Росія дедалі ігнорує міжнародні норми та правила.

Росія не приховує, що активно співпрацює з Іраном. Російські гроші та товари, що надходять до скарбниці Ірану, зміцнюють економічні та військові позиції двох країн.

Все вищезазначене вимагає рішучої реакції з боку української та міжнародної спільноти. Для бізнесу важливе усвідомлення ризиків та загроз, що несе співпраця з країною агресором.

Наразі та в майбутньому погляди всього світу будуть прикуті до осіб та організацій, відповідальних за співучасть у фінансуванні злочинів росії.

Викоріненню схем легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансування тероризму та фінансування розповсюдження зброї масового знищення, під час агресивної війни росії проти України, сприятиме розроблена тема типологічного дослідження.

Ігор Черкаський

ВСТУП

Відкрита широкомасштабна російська агресія проти незалежної, мирної та демократичної України створила нові виклики перед системою фінансового моніторингу.

Актуальність дослідження тематики злочинів, пов'язаних з російською агресією, обумовлена ризиками, з якими наразі стикнулась фінансова система України та міжнародна фінансова система в цілому.

Це типологічне дослідження націлене на вивчення питання отримання та використання злочинних доходів в умовах військової агресії.

Окремий напрямок дослідження охоплює питання виявлення активів, встановлення прихованих бенефіціарних власників, підсанкційних осіб та ухилення (обходу) санкційних обмежень.

За результатами розкриття теми дослідження здійснено актуалізацію виявлених інструментів та методів легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансування тероризму та фінансування розповсюдження зброї масового знищення.

Дане типологічне дослідження відображає актуальні схеми ВК/ФТ/ФРЗМЗ в умовах військової агресії росії, визначає актуальні методи та інструменти, які використовуються в схемах.

РОЗДІЛ І. ЗАГАЛЬНІ ТЕНДЕНЦІЇ

1.1. Росія держава-спонсор тероризму

Війна розпочата росією проти України вже понад дев'ять років призводить до загибелі людей та руйнування інфраструктури України, порушення світового порядку.

Зовнішньополітичний курс України був використаний росією як формальний привід для початку повномасштабних бойових дій проти України.

Демократична Україна веде війну за незалежність проти російського неоколоніалізму, який уособлений авторитарним режимом, що відкидає право на існування самостійної української нації. Україна захищає увесь світ натомість росія прагне змінити баланс сили у світі, застосовуючи принцип права сили.

Обстріл території та знищення інфраструктури

6 червня 2023 року російські окупанти підірвали Каховську ГЕС, що стало черговим актом державного тероризму з боку росії та призвело до небаченої гуманітарної та екологічної катастрофи на півдні України.

Фактично починаючи з 2022 року, росія розпочала активно застосовувати ракетне озброєння та дрони-камікадзе для ударів по об'єктах критичної інфраструктури України.

Росія намагається знищити в зимовий сезон українську енергетичну систему та позбавити мирне населення електроенергії, водопостачання та опалення.

Порушення принципів ядерної безпеки

Росія окуповує атомні електростанції чим загрожує ядерній безпеці у світі. Під окупацією була Чорнобильська атомна електростанція та залишається окупованою військами росії найбільша в Європі Запорізька АЕС.

Російська сторона свідомо порушує принципи ядерної безпеки, розміщує озброєння в приміщеннях і на території атомних електростанцій та продовжує безвідповідальну риторику як важіль ядерного шантажу України та світу, створюючи найсерйозніші загрози для глобальної безпеки.

Ядерні погрози та шантаж, а також мілітаризація тимчасово окупованої Запорізької АЕС провокують катастрофу загальносвітового масштабу.

Приклад 1.1.1. Порушення принципів ядерної безпеки

Три атомні електростанції Рівненська, Південноукраїнська та Хмельницька були відключені від енергосистеми України внаслідок ракетної атаки, яку 23 листопада 2022 року здійснила росія по об'єктах енергетичної інфраструктури по всій країні.

Контрольована російськими окупантами Запорізька АЕС також систематично переходить в режим роботи в умовах повного блекауту.

Ризики для глобальної фінансової безпеки з боку росії

FATF була створена країнами G7 для забезпечення глобальної фінансової безпеки. FATF встановлює стандарти та сприяє ефективному впровадженню правових, регуляторних та операційних заходів для обмеження трьох основних ризиків: відмивання грошей, фінансування тероризму та фінансування розповсюдження зброї масового знищення.

Членство росії в FATF зупинено 24 лютого 2023 року. Війна росії проти України суперечить принципам FATF щодо сприяння безпеці та цілісності глобальної фінансової системи та зобов'язанням щодо міжнародного співробітництва та взаємної поваги, які члени FATF погодилися впроваджувати та підтримувати.

Україна наполягає на прийнятті FATF рішень щодо включення росії до чорного списку (списку держав (юрисдикцій), що не виконують чи неналежним чином виконують рекомендації міжнародних, міжурядових організацій, задіяних у сфері ПВК/ФТ/ФРЗМЗ).

Чорний список FATF є найефективнішим інструментом для обмеження доступу терористів до світової економіки, оскільки це змусить всі держави застосовувати посилену належну перевірку до будь-яких транзакцій, пов'язаних з фінансовою системою юрисдикції, внесеної до чорного списку.

Включення росії до чорного списку FATF сприятиме:

- запобіганню ухиленню росії від санкцій;
- проведенню фінансовими установами світу додаткових перевірок клієнтів з росії;

а також:

- перешкоджатиме торгівлі росії зі світом;
- зменшить надходженню інвестицій в росію та спричинить відтік багатьох інвесторів.

Будь-яка транзакція з російським фінансовим сектором буде переглянута і ретельно перевірена. Це значно підвищить «вартість» ведення бізнесу з росією і фактично позбавить злочинців з росії можливості фінансувати війну.

Співпраця з терористичними угрупованнями та державами, внесеними до чорних списків

Окремої уваги заслуговує факт співпраці росії з різними радикальними та терористичними угрупованнями, а також державами, внесеними до чорних списків.

Російські фізичні та юридичні особи вчиняють дії, які спрямовані на підтримку розповсюдження зброї масового знищення та балістичних програм Північної Кореї.

Іранські дрони-камікадзе використовувалися для атак на українські цивільні об'єкти та вбивають громадян України.

Регіональні органи влади росії для участі у війні проти України здійснюють вербування населення на військовий контракт серед мігрантів, банкрутів, боржників, безробітних та інших уразливих соціальних верств суспільства.

Активна робота з вербування на контракт для участі у війні здійснюється також через оголошення, банери та спокусу великими грошима.

1.2. Фінансування тероризму та колабораціонізму

Фінансування тероризму та колабораціонізму може виникати з різних причин, які можуть бути поєднанні або взаємопов'язані, і вони можуть варіюватися в залежності від конкретної ситуації та обставин.

Розуміння причин фінансування тероризму та колабораціонізму дозволяє ефективно розробити стратегію протидії.

Причини ФТ/ФРЗМЗ

Фінансування тероризму (як і фінансування розповсюдження зброї масового знищення) може виникати з численних причин, серед яких можливо визначити наступні:

- ідеологічні мотиви (терористи та колабораціоністи можуть вірити в ідеологію, що виправдовує їхні дії, і вважати, що фінансування допомагає реалізувати їхні цілі);
- політичні амбіції (керівництво терористичних організацій може використовувати ФТ та ФРЗМЗ для підтримки політичних цілей, включаючи зміну режимів або вибори у владу);
- фінансово вигідний стан (злочинці та терористи можуть отримувати фінансовий прибуток від ФТ та ФРЗМЗ, що може бути вигідним для них особисто);
- економічні фактори (залучення до ФТ або ФРЗМЗ може бути реакцією на економічні труднощі, борги чи безробіття);
- політичні конфлікти та війни (умови політичних конфліктів і війн можуть створювати можливості для злочинців та терористів використовувати ФТ та ФРЗМЗ для досягнення своїх цілей);
- соціальні та релігійні фактори (релігійні та соціокультурні фактори можуть впливати на мотивацію і підтримку осіб, що займаються ФТ та ФРЗМЗ).

Вчинення фінансування тероризму (як і фінансування розповсюдження зброї масового знищення) в умовах військової агресії росії створює серйозні загрози і ризики, включаючи:

- підтримку тероризму та дестабілізацію: фінансування терористичних груп може сприяти подальшій дестабілізації вже крихкого політичного та соціального середовища в умовах війни;
- поширення зброї масового знищення: ФРЗМЗ може призвести до небезпечного збільшення доступності цих засобів та збільшити загрозу для безпеки та стабільності;

- терористичні акти: ФТ може бути пов'язаним із підготовкою та здійсненням терористичних актів, які можуть завдати шкоди життям та майну, порушити громадський порядок та загрожувати безпеці;
- зловживання гуманітарними ресурсами: ФТ може використовувати гуманітарні ресурси для підтримки своєї діяльності, що може заважати гуманітарним операціям та допомозі;
- використання технологій і криптовалют: злочинці можуть використовувати криптовалюти та інші технології для анонімних та надійних фінансових операцій;
- експлуатацію природних ресурсів на території України: можливість отримання величезних доходів від сектора видобутку корисних копалин в зоні окупації росії або в розташованих поруч регіонах, що представляє серйозну уразливість для економіки;
- вразливість електронних та Інтернет платежів, які терористи використовують для оперативного (швидкого) переказу грошових коштів.

Діяльність окремих терористів та терористичних організацій, включаючи іноземні, становить серйозну загрозу безпеці та стабільності, серед яких:

- терористичні акти: основною загрозою є можливість здійснення терористичних актів, включаючи вибухи, напади та інші насильницькі дії, які можуть завдати шкоди життям та майну та порушити громадський порядок;
- рекрутинг і радикалізація: терористичні організації активно рекрутують і радикалізують індивідів, що може призвести до зростання чисельності бойовиків;
- вплив на міжнародні відносини: діяльність іноземних терористичних організацій може сприяти напруженню міжнародних відносин, викликати реакцію держав та призвести до геополітичних конфліктів;
- фінансування та ресурси: терористичні організації потребують фінансування для своєї діяльності, і це може призвести до використання нелегальних шляхів для збору коштів, включаючи ФТ;
- поширення ідеології тероризму: терористичні групи можуть просувати ідеології, що виправдовують насильство та тероризм, що може мати вплив на індивідів та суспільство;
- залучення іноземців: терористичні організації можуть залучати іноземців до своєї діяльності, включаючи бойових ветеранів та іноземних терористів, що може створювати міжнародну загрозу;
- кіберзлочини та кібератаки: терористичні організації можуть використовувати кібернетичні засоби для атак на критичну інфраструктуру та інші цілі.

Колаборанти можуть здійснювати фінансування тероризму, оскільки вони можуть надавати підтримку терористичним групам через різні канали.

Це може включати незаконні фінансові операції, використання фіктивних компаній для переміщення грошей, а також використання благодійних організацій як засобу для приховування фінансування тероризму.

Основні причини, що можуть призводити до колабораціонізму:

- самозбереження та безпека (індивіди, групи або організації можуть співпрацювати з окупантами з метою забезпечення власної безпеки);
- матеріальний інтерес (колабораціоністи можуть отримувати матеріальні вигоди або фінансову підтримку в обмін на співпрацю з окупаційними силами);
- ідеологічні чи політичні переконання (особи або групи можуть поділяти ідеологічні чи політичні переконання з окупантами та вважати співпрацю за необхідну для досягнення своїх цілей);
- страх перед репресіями (існує страх перед можливими наслідками або репресіями, і це може спонукати осіб чи групи до співпраці з агресором);
- етнічні або соціальні конфлікти (складні етнічні або соціальні конфлікти можуть призводити до співпраці з окупантами для захисту власних інтересів чи спільнот).

1.3. Міжнародний тероризм

Агресія росії проти незалежної України та міжнародний тероризм є одними із факторів кризи глобальної системи міжнародної безпеки.

Актуальними тенденціями розвитку міжнародного тероризму є:

- збільшення активності міжнародних терористичних організацій;
- наявність у незаконному обігу великих обсягів зброї та боєприпасів;
- наявність сепаратистських настроїв населення та збільшення радикалізації суспільства;
- використання новітніх технологій у терористичній діяльності та її фінансуванні.

Поширення інформації терористичними організаціями здійснюють через канали передачі даних, включаючи засоби медіа, краудфандінгові сайти, додатки для обміну повідомленнями та соціальні мережі.

Публікації здійснюються через такі майданчики, як Telegram, X (Twitter), Facebook, Instagram та Tik Tok, як у постах, так і в коментарях.

Іноді портал збору коштів можна ідентифікувати як такий, що перебуває на стороні терористичної діяльності та просуває ідеї терористичних організацій, а в інших випадках зовнішній вигляд порталу начебто стосується лише гуманітарної допомоги, але кошти згодом спрямовуються фізичним або юридичним особам, пов'язаним з терористичними організаціями.

Для проведення фінансових операцій терористичні організації використовують різні канали та місця для переказу коштів, включаючи банківські та електронні перекази, кредитні картки, сучасні платіжні засоби та криптовалюти (такі як BTC, ETH, USDT, USDC та TRX).

В цьому контексті важливим є не тільки виявлення криптоадрес, рахунків та цифрових платіжних засобів терористичних організацій, а їх блокування на державному рівні.

Водночас злочинці використовують альтернативні майданчики для продовження фінансування тероризму, наприклад, хавалу.

Неприбуткові організації

Використання неприбуткових організацій є одним з найпоширеніших механізмів фінансування тероризму.

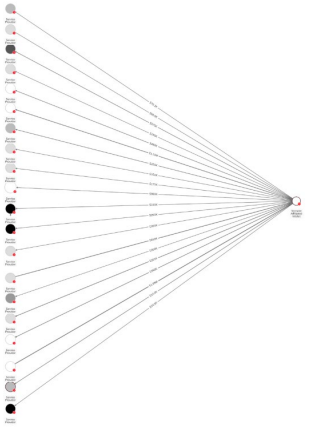
Протягом багатьох років терористичні організації неодноразово використовували цей метод для збору коштів у різних країнах. Іншим поширеним методом зловживання неприбутковими організаціями є створення «фіктивних» або підставних організацій. Ці організації удавано збирають гроші на благодійні гуманітарні цілі, тоді як насправді кошти використовуються для підтримки тероризму.

Фінансування тероризму через торгівлю (TBTF)

Терористичні організації використовують міжнародну торгівлю, щоб приховати передачу вартості з метою підтримки своєї діяльності. Ці схеми часто включають завищення або заниження вартості товарів, спотворення інформації про продукти та фіктивне постачання.

Відомо, що терористичні організації використовують продаж товарів, у тому числі основних харчових продуктів, для фінансування свого військового крила та повсякденних операцій.

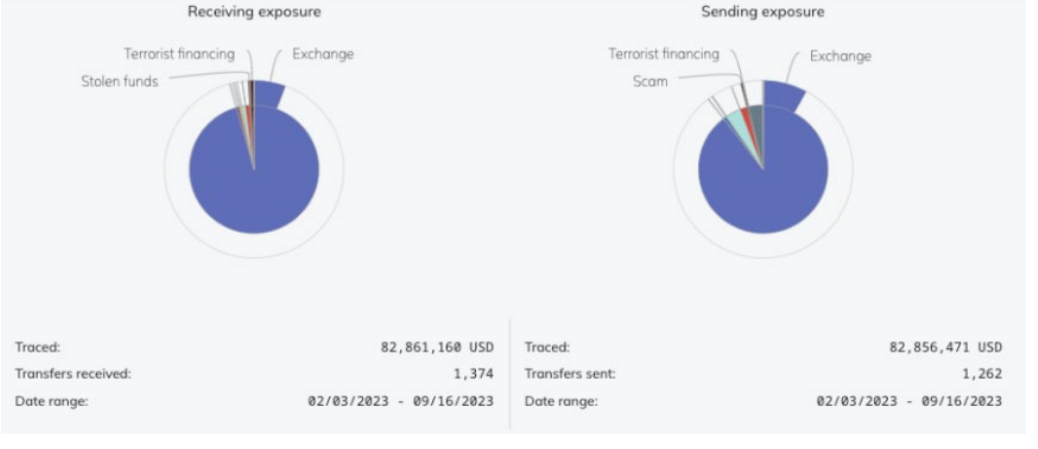
Аналіз потоків терористів у блокчейні



Приклад використання інструменту **Chainalysis Reactor** для аналізу контрагентів гаманця, який пов'язаний з фінансуванням тероризму.

Щонайменше знайдено 20 підозрюваних постачальників послуг. Кожен із підозрюваних постачальників послуг отримав від усіх своїх контрагентів від 8,4 до 1,1 мільярда доларів у криптовалюті.

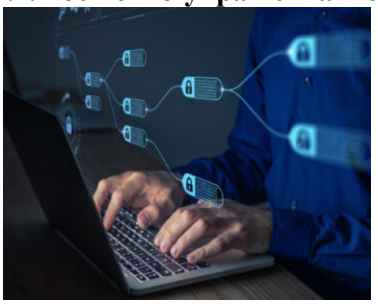
З приблизно 82 мільйонів доларів у криптовалюті, отриманих на цю адресу, близько 450 000 доларів було переведено з відомого гаманця, пов'язаного з тероризмом.



Враховуючи активність цієї адреси, особа або група людей, які її контролюють, імовірно, не та сама особа, яка контролює пов'язаний з тероризмом гаманець, а скоріше постачальник послуг, який свідомо чи несвідомо сприяв фінансуванню тероризму.

У наведеному вище прикладі для фінансування тероризму було зібрано криптовалюту на суму 82 мільйони доларів. Але набагато ймовірніше, що невелика частина цих коштів була призначена для терористичної діяльності, а більшість коштів, оброблених через підозрюваного постачальника послуг, не були пов'язані.

1.4. Російсько-українська кібервійна



За даними Служби безпеки України, упродовж 2022-2023 років заблоковано діяльність 76 ботоферм, загальною потужністю понад 3 млн акаунтів, які діяли на території нашої держави та відпрацьовували проросійські наративи.

Ворог регулярно намагається розхитати ситуацію в інформаційному просторі України.

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA систематично фіксуються кібератаки з боку структур, пов'язаних з країною агресором на державні органи України, установи та організації різних форм власності.

Кібератаки можуть мати серйозний негативний вплив на економіку України через великі фінансові втрати, порушення довіри та збитки для бізнесу та державних установ. Такі атаки можуть стати додатковим фінансовим тягарем.

Можливі наслідки від кібератак:

- **втрати для бізнесу.** Кібератаки можуть призвести до великих фінансових втрат для українських компаній. Наприклад, атаки на фінансові установи можуть призвести до крадіжок грошей, атаки на підприємства можуть спричинити втрату конфіденційної інформації або призупинення виробництва;
- **втрати для державних установ.** Кібератаки на державні установи можуть призвести до витоку конфіденційної інформації, порушення нормального функціонування державних систем, а також до втрати даних;
- **порушення довіри до цифрових систем.** Кібератаки можуть призвести до порушення довіри до цифрових систем та послуг. Це може призвести до зменшення активності в інтернет-торгівлі, електронному банкінгу та інших сферах електронної комерції;
- **збільшення витрат на кібербезпеку**. Компанії та державні установи можуть зазнавати значних витрат, які пов'язані із захистом від кіберзагроз та відновленням після атак.

Приклад 1.4.1. Кібератаки на мережу зв'язку «Київстар»

12 грудня 2023 року мережа зв'язку «Київстар» стала мішенню потужної хакерської атаки, що стала причиною технічного збою, у результаті якого тимчасово недоступні послуги зв'язку та доступу в інтернет, повідомила пізніше компанія в релізі. Це став найбільший збій не лише для «Київстар», а й для всіх українських операторів за останні роки.

Відповідальність за атаку вже взяло на себе одне з російських псевдохакерських угруповань. Воно є хакерським підрозділом головного

управління генштабу збройних сил росії (більш відомого як гру), яке таким чином публічно легалізує результати своєї злочинної діяльності.

Цифровій інфраструктурі «Київстару» було завдано критичних уражень, тому відновлення всіх послуг із дотриманням необхідних протоколів безпеки вимагало часу та відповідно було завдано економічних збитків на рівні країни.

Представники банків внаслідок втручання у діяльність мережі «Київстар» змушені були оперативно реагувати на непередбачувані події. Переважно проблеми виникали з роботою частини POS-терміналів торговельної мережі, що працюють з використанням мобільного зв'язку «Київстар».

Крім того, це мало негативний вплив на розрахунки з підприємствами та фізичними особами-підприємцями, які використовують для розрахунків платіжні картки. Також це призвело до недоотримання доходів, що має наслідком скорочення надходжень до бюджету.

Для досягнення успіхів росії у війні проти України, підконтрольні російській владі угрупування здійснюють кібератаки на країни (організації), які надають допомогу Україні або підтримують її.

Детально значення кіберзагроз досліджено у звіті «Туман війни: як конфлікт в Україні змінив ландшафт кіберзагроз» на основі аналізу загроз Google (TAG), Mandiant і Trust&Safety.

Звіт охоплює нові висновки та ретроспективні висновки щодо підтримуваних державою зловмисників, інформаційних операцій (IO) та учасників загроз екосистеми кіберзлочинців.

Він також включає детальні аналізи загроз, зосереджених на конкретних кампаніях з 2022 року[2].

Група аналізу загроз Google (TAG) продовжує виявляти групи, які підтримуються російським урядом, та діяльність яких направлена на війну в Україні[3].

У I кварталі 2023 року підтримувані урядом росії фішингові кампанії були націлені найбільше на користувачів в Україні.

FROZENBARENTS (така ж Sandworm), група, яку приписують підрозділу 74455 Головного управління Генерального штабу (ГРУ) збройних сил росії,

[2]https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf
[3]https://blog.google/threat-analysis-group/ukraine-remains-russias-biggest-cyber-focus-in-2023/

продовжує зосереджуватися на війні в Україні, проводячи кампанії, що охоплюють збір розвідданих та витік зламаних даних через Telegram.

FROZENBARENTS залишається найбільш універсальним кіберактором ГРУ з наступальними можливостями, включаючи фішинг облікових даних, мобільну активність, зловмисне програмне забезпечення, зовнішнє використання служб тощо. Ціль для збору інформації: урядові органи, оборонні дані, енергетика, транспорт/логістика, освіта та діяльність гуманітарних організацій.

Приклади діяльності frozenbarents

Каспійський трубопровідний консорціум

Каспійський трубопровідний консорціум (КТК) контролює один із найбільших у світі нафтопроводів, який транспортує нафту з Казахстану до Чорного моря.

FROZENBARENTS докладає постійних зусиль, спрямованих на атаку компаній, які пов'язані з енергетичним сектором в Європі. Для таких цілей використовувались фішингові посилання, які надсилалися через SMS.

Енергетичний сектор в Східній Європі

Протягом І кварталу 2023 року FROZENBARENTS проводив численні атаки проти організацій енергетичного сектору в Східній Європі, надаючи посилання на підроблені пакети оновлень Windows.

У разі виконання фальшивого оновлення відбудеться активація варіанта викрадача Rhadamanthys для вилучення збережених облікових даних, зокрема, файлів cookie браузера.

Українська оборонна промисловість

FROZENBARENTS запустив кілька фішингових кампаній, націлених на українську оборонну промисловість, військових і користувачів вебпошти Ukr.net.

Ці фішингові електронні листи фальсифікували сповіщення безпеки та інші типи сповіщень системного адміністратора, а в деяких випадках надсилалися через сторонні служби керування електронними кампаніями.

Поширення фейкових новин

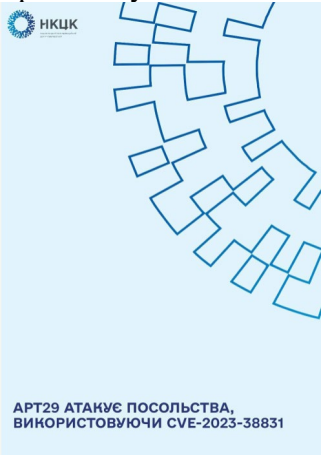
FROZENBARENTS створює аккаунти для поширення проросійських новин та витоку вкрадених даних. Фактично йде формування та поширення новин проти України, НАТО та країн ЄС.

Наприклад, «Cyber Army of Russia» або «Cyber Army of Russia_Reborn» (контролюється FROZENBARENTS) представлені в Telegram, Instagram і YouTube.

На початку вересня 2023 року угрупування APT29, пов'язане з російською службою зовнішньої розвідки (далі – сзр), здійснило кібератаку проти дипломатичних представництв, міжнародних організацій та, навіть, інтернет-провайдерів.

Основна увага була зосереджена на дипломатичних акаунтах, причому Міністерства закордонних справ Азербайджану та Італії взяли на себе основний удар.

Крім того, серед численних мішеней також були посольства в Греції та Румунії, та поштові скриньки відомого грецького інтернет – провайдера Otenet. Список жертв розширився до найбільших міжнародних організацій, що підкреслює зухвалість і масштаби цієї кампанії.



Серед кількох можливих мотивів, однією з найбільш очевидних цілей сзр може бути збір розвідувальної інформації про стратегічну діяльність Азербайджану. Варто зазначити, що країни-мішені – це Греція, Румунія та Італія (підтримують значні політичні та економічні зв'язки з Азербайджаном).

Методологія атаки передбачала використання фішингових електронних листів, які містили приманки із зображенням продажу автомобілів BMW. Це тактика, яку раніше використовувала APT29 під час атак на посольства в Києві.

Список міжнародних організацій, атакованих в рамках кампанії APT29

Домен	Організація
@gccsg.org	Генеральний секретаріат Ради співробітництва Перської затоки
@ec.europa.eu	Європейська комісія
@unhcr.org	Верховний комісар ООН у справах біженців
@unicef.org	Міжнародний дитячий надзвичайний фонд ООН
@auf.org	Університетське агентство франкофонії
@francophonie.org	Міжнародна організація франкофонії
@iom.int	Міжнародна організація з міграції
@worldbank.org	Світовий банк
@selec.org	Центр правоохоронних органів Південно-Східної Європи
@coe.int	Рада Європи
@euro.who.int	Європейський регіон Всесвітньої організації охорони здоров'я

1.5. Використання новітніх технологій для вчинення злочинів

Нові технології, продукти та пов'язані послуги мають потенціал до стимулювання фінансових інновацій та ефективності й покращення фінансових послуг, але вони також створюють нові можливості для злочинців та терористів у відмиванні їх доходів або фінансуванні їх незаконної діяльності.

Віртуальні активи використовують інноваційні технології для швидкої передачі вартості по всьому світу та мають багато потенційних переваг, включаючи швидше та дешевше здійснення платежів. Певна анонімність, пов'язана з віртуальними активами, також приваблює злочинців, які використовують такі активи для відмивання доходів від низки злочинів, таких як торгівля наркотиками, незаконна контрабанда зброї, шахрайство, ухилення від сплати податків, кібератаки, ухилення від санкцій, експлуатація дітей та торгівля людьми.

Використання криптовалюти в злочинних цілях

З розвитком ринку криптоактивів та залучення широких мас населення, зростає й кількість злочинів, які пов'язані з такими активами. Криптовалюта як і фіатні гроші можуть використовуватись для розрахунку у злочинній діяльності.

Криптовалюту використовують також корупціонери для того, щоб брати хабарі без надання будь-якої персональної інформації, і щоб скоріше вивести незаконні статки на захищений безіменний рахунок.

Блокчейн

Розслідування злочинів вчинених з використанням віртуальних активів потребує використання технологій та доступу до блокчейну.

Блокчейн містить розподільну децентралізовану інформаційну систему, що використовує криптографічний метод підтвердження здійснення кожної транзакції та надає можливість для запису та відстеження руху всіх транзакцій.

Інформація про час і послідовність здійснення кожної транзакції записується у блоки, які потім реєструються у ланцюжку блоків за заданими в системі правилами.

Кожен блок містить хеш (унікальний ідентифікатор) останніх транзакцій з відмітками часу, а також хеш попереднього блоку.

Криптовалютні біржі

Сервіс обміну криптовалют (криптовалютна біржа) – це онлайн-сервіс, який дозволяє клієнтам обмінювати криптовалюти на інші активи, наприклад, звичайні фіатні гроші або інші цифрові валюти. Ідентифікація адреси сервісу обміну криптовалют є важливим кроком для боротьби зі злочинами.

Для ідентифікації адреси сервісу обміну криптовалют можна використовувати такі методи:

1. Аналіз блокчейну. Шляхом аналізу блокчейну можна виявити адреси сервісів обміну криптовалют, які пов'язані з нелегальними операціями. Наприклад: контрольована правоохоронним органом транзакція, дозволяє встановити адресу сервісу обміну криптовалют.

2. Співпраця з сервісами обміну криптовалют: державні та правоохоронні органи можуть співпрацювати для виявлення та блокування адрес, які використовуються для нелегальних операцій.

3. Використання спеціалізованих програм: існують програми, які дозволяють виявляти та аналізувати адреси криптовалютних гаманців, що може допомогти в ідентифікації сервісів обміну криптовалют.

Ідентифікація адрес сервісів обміну криптовалют є складним завданням, але це важливий крок для розслідування.

Приклад співпраці

Криптовалютні біржі можуть допомогти ідентифікувати власників криптогаманців. Зокрема, біржі можуть надавати наступну інформацію:

- документ, що посвідчує особу;
- електронну адресу;
- IP-адресу;
- назву та IMEI пристрою, з якого здійснюється вхід до облікового запису криптовалютної біржі;
- інформацією про проведені операції;
- наявність додаткових гаманців;
- наявність банківських рахунків, через які здійснюється поповнення баланс на біржі;
- номери рахунків, на які виводяться кошти.

Виявлення активів, які належать фігурантам кримінальних проваджень, на біржах дозволить вживати заходи щодо зупинення чи накладення арешту на криптовалюти.

До того ж в цій сфері дуже важливим чинником є взаємодія компетентних органів різних країн, оскільки віртуальні активи характерні своєю транснаціональною природою.

Ризики використання віртуальних валют

Засновані на віртуальних валютах платіжні продукти та послуги створюють ризики відмивання коштів і фінансування тероризму в значних обсягах.

Ця технологія дозволяє здійснювати анонімні перекази коштів в міжнародному масштабі.

Оскільки криптовалюти значною мірою анонімні, зручні та глобальні за своєю природою, деякі найбільші злочинні угрупування у світі зацікавлені у їх використовуванні як способу відмивання коштів.

Певна анонімність, пов'язана з віртуальними активами, також приваблює злочинців, які використовують такі активи для відмивання доходів від низки злочинів, таких як торгівля наркотиками, незаконна контрабанда зброї, шахрайство, ухилення від сплати податків, кібератаки, ухилення від санкцій, експлуатація дітей та торгівля людьми.

Незаконні операції за участю криптобіржі Binance

Міністерство фінансів США через Мережу боротьби з фінансовими злочинами (FinCEN), Управління контролю за іноземними активами (OFAC) і Службу кримінальних розслідувань (IRS) вжило безпрецедентних дій щодо Binance Holdings Ltd та її філій (Binance).

Binance є відповідальною за порушення законів США про боротьбу з відмиванням грошей і санкцій, які захищають національну безпеку США та цілісність міжнародної фінансової системи.

1.6. Використання дітей для вчинення злочину

Правоохоронні органи фіксують зростання злочинності за участю дітей, які є вразливі для вербування спецслужбами росії.

З початку 2023 року отримано 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 все частіше залучають дітей.

Перед відправленням повідомлень про фейкові мінування «анонімні терористи» отримують від своїх російських кураторів перелік «пріоритетних» об'єктів в Україні.

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 1.6.1. Використання учнів місцевої школи для повідомлення про мінування

Службою безпеки України викрито двох учнів старших класів місцевої школи, які повідомили про «мінування» обласної військової адміністрації та міського торговельного центру.

За даними слідства, юнаки діяли за вказівкою представників спецслужб росії, які завербували школярів через підконтрольні Телеграм-канали.

Наразі за цим та іншими фактами тривають розслідування за ст. 259 КК України (свідоме неправдиве повідомлення про загрозу безпеці громадян, знищення чи пошкодження об'єктів власності).

Приклад 1.6.2. Використання підлітка для збору інформації про пересування захисників України

Правоохоронні органи викрили 17-річного жителя Харківської області, якого завербував працівник спецслужб росії. За його завданнями підліток збирав та передавав інформацію про пересування сил та засобів Збройних сил України.

Світ ігор насправді є платформою, яка може впливати на громадську думку, охоплювати аудиторію, особливо молодь. Російська пропаганда вже почала поширюватись на світові відеоігри.

Приклад 1.6.3. Використання популярних ігор для втягування підлітків у війну

У Minecraft, захоплюючій грі, що належить Microsoft, російські гравці відтворили битву за Соледар, місто в Україні, яке російські війська окупували у січні 2023 року, опублікувавши відео гри в найпопулярнішій соціальній мережі своєї країни ВКонтакте.

Приклад 1.6.4. Використання популярних ігор для популяризації пропаганди росії серед населення

Канал російської версії World of Tanks, бойової гри для кількох гравців, відзначив 78-му річницю поразки нацистської Німеччини в травні відтворенням параду танків Радянського Союзу в Москві в 1945 році.

Ці ігри та суміжні дискусійні сайти, такі як Discord і Steam, стають онлайн-платформами для російської агітації, поширюючи серед нової, переважно молодшої аудиторії, потоки пропаганди, якими кремль намагався виправдати війну в Україні.

РОЗДІЛ ІІ. САНКЦІЇ

Повномасштабне вторгнення росії на територію України у 2022 році спровокували запровадження масштабних та безпрецедентних санкцій проти країни-агресора.

Санкції мають практичний вплив на росію та призвели до послаблення економіки агресора та збільшення логістичного шляху проходження товарів.

На сьогодні росія є найбільш підсанкційною країною світу та наразі проти російських фізичних та юридичних осіб діє велика кількість санкцій (це значно більше, ніж після подій 2014 року). До вторгнення росії в Україну найбільш санкційною державою в історії був Іран.

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

Обмеження руху визначених активів

Росії заборонено купувати західні мікросхеми, зброю та інші технологічні товари. Водночас санкційні товари через довгий ланцюг компаній у світі потрапляють на територію росії. Наприклад, мікрочипи, дрони та інші високотехнологічні інструменти.

Дослідження конкретних іноземних компонентів, виявлених в російському обладнанні на території України, дозволяє створити базу даних про російську міжнародну торгівлю для розслідування схем обходу та/або порушення санкцій.

Роль імпортованих компонентів

Майже вся сучасна військова техніка росії залежить від складної електроніки, імпортованої з розвинутих країн світу. Наприклад: США, Великобританія, Німеччина, Нідерланди, Японія, Ізраїль та Китай.

Деякі компоненти є цивільними товарами подвійного призначення, що ускладнює процес експортного контролю. Для продовження експортних операцій в умовах санкцій, росія здійснює маскування постачання імпортних компонентів через залучення третіх країн як посередників.

Приклад 2.1. Постачання автомобілів класу люкс до росії в обхід санкцій

Вантажне транспортне підприємство LTG Cargo звернулось до Генеральної прокуратури Литви щодо можливого порушення міжнародних санкцій при експорті автомобілів класу люкс до третіх країн.

Експерти LTG Cargo, які відповідальні за санкційний нагляд, мають підозри щодо використання компанії для можливих схем обходу санкцій на постачання до росії люксових автомобілів.

LTG Cargo проінформувала клієнтів, що через неприйнятний ризик, який представляють компанії, які прагнуть обійти санкції, LTG Cargo припиняє перевезення всіх автомобілів класу люкс залізницею через територію Литви.

Є підозри, що автомобілі класу люкс, призначені для третіх країн – Білорусі, Казахстану, Киргизії, Узбекистану, Таджикистану, Грузії, Туркменістану – насправді везуть до росії, відносно якої застосовані санкції.

LTG Cargo проаналізувала інформацію про 447 легкових автомобілів Mercedes, Porsche Cayenne, Cadillac та інших автомобілів класу люкс, з'ясувалося, що 75 з них зареєстровані в росії, 55 потрапили до неї через інші країни, а ще по 279 автомобілям немає жодних даних за місцем реєстрації.

Встановлено, що у можливій схемі обходу санкцій було залучено 4 компанії та з метою мінімізації ризиків, компанія не схвалюватиме заявки на перевезення до третіх країн автомобілів класу люкс, випущених за останні п'ять років вартістю понад 50 тисяч євро.

Виявлення схем обходу санкцій можливе лише при здійсненні постійного моніторингу.

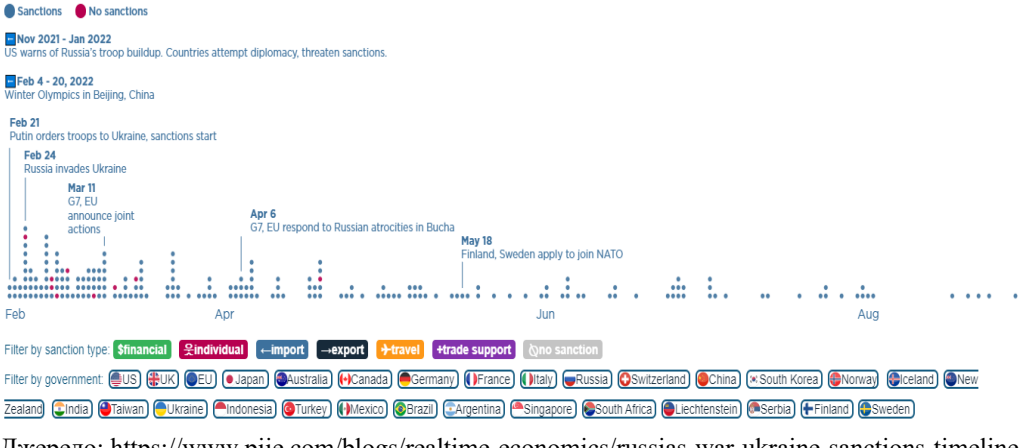
За даними ForbesUA, найбільші торгові потоки у 2022 році з росією наростили Туреччина, Казахстан, Вірменія, Узбекистан і Киргизстан. Казахстан є привабливим для торгових операцій з росією, оскільки має один з найпротяжніших сухопутних кордонів з нею.

Паралельно з цим відбулося значне зростання торгових операцій до цих країн із західних держав.

Також найбільшим торговим партнером росії залишається Китай та інші місця посідають Туреччина, Вірменія та країни Середньої Азії.

PIIE

Інститут міжнародної економіки Петерсона систематично проводить дослідження санкційної політики щодо росії та створив інтерактивний моніторинговий модуль візуалізації застосування санкцій.



Джерело: https://www.piie.com/blogs/realtime-economics/russias-war-ukraine-sanctions-timeline

Дані, що лежать в основі дослідження постійно оновлюються та доступні на сайті Інституту міжнародної економіки Петерсона в режимі завантаження (формат Microsoft Excel).

Алгоритм роботи модуля. Інтерактивний моніторинговий модуль відстежує економічні санкції, введені Сполученими Штатами, Європейським Союзом, Сполученим Королівством та іншими великими економіками, надаючи важливі відомості про їх виконання. Серед них санкції проти росії, а також проти білорусі за сприяння та підтримку дій росії у війні.

Санкції США

За 2023 рік Сполучені Штати Америки застосували наступні санкції проти росії за повномасштабне вторгнення на територію України та інших країн за сприяння та підтримку дій росії у війні, зокрема, запроваджено санкції щодо:

права людини

- осіб за причетність до серйозних порушень прав людини (в тому числі порушення прав правозахисника, відомого лідера російської опозиції);

категорії осіб

- представників російської еліти, в тому числі фінансової еліти та значущих компаній, які підтримують чи постачають технології для продовження війни;
- Федеральної служби безпеки росії (ФСБ) та Розвідувальної організації Корпусу вартових Ісламської революції Ірану (IRGC-IO) за неправомірне затримання громадян США;
- членів пов'язаної з російською розвідкою злочинної групи впливу за їх роль у кампаніях російського уряду з дестабілізації та продовження зловмисного впливу в Молдові;
- осіб, які причетні до іранського виробника безпілотних літальних апаратів (БПЛА) та програмам балістичних ракет Ірану (в тому числі щодо доступу до компонентів іноземного виробництва іранським компаніям, які постачають безпілотники до росії);
- компаній за підтримку військової та оборонно-промислової бази росії (у тому числі з Китаю та з росії). Здійснювалось також постачання запчастин для безпілотників;
- юридичних та фізичних осіб причетних до закупівлі товарів для програми Ірану щодо безпілотних літальних апаратів (БПЛА). Такі особи базуються в Ірані, Китаї, Гонконгу, Туреччині та Об'єднаних Арабських Еміратах);
- компаній, які підтримують військову та оборонну промисловість росії, в тому числі через постачання напівпровідників. Такі компанії з Китаю, а також з інших країн (тобто Естонії, Фінляндії, Німеччини, Індії, Туреччини, Об'єднаних Арабських Еміратів і Сполученого Королівства);

- осіб та активів, що базуються в Ірані, Гонконгу, Китаї та Венесуелі, які підтримують іранські програми балістичних ракет і безпілотних літальних апаратів (БПЛА);
- компаній Китаю, Туреччини та Об'єднаних Арабських Еміратів за надсилання в росію товарів подвійного призначення високого пріоритету, а також проти російських банків та інших фізичних та юридичних осіб;
- осіб перехідного уряду Малі та військових за сприяння розгортанню та розширенню діяльності в Малі групи Вагнера;

економіка

- обмеження цін на російські нафтопродукти, підвищення мит на російський імпорт (включаючи сталь і алюміній) та санкції проти російського металургійного та гірничодобувного секторів, військових постачальників;
- осіб, пов'язаних з групою Вагнер. Групу визначено транснаціональною злочинною організацією;
- організацій, які працюють в оборонному секторі російської економіки, а також інших організацій, пов'язаних з російською Державною корпорацією з атомної енергії (Росатом);
- обмеження доступу росії до товарів, які підтримують її військові та військові зусилля;
- майбутньої енергетичної можливості;
- доступу до міжнародної фінансової системи;
- позбавлення росії доступу до технологій, вироблених G7 та необхідних для її технологічного, аерокосмічного та оборонного секторів;
- судновласників за порушення цінового ліміту, встановленого коаліцією Price Cap (країни G7, Європейський Союз та Австралія), транспортуючи нафту, придбану за понад 60 доларів за барель;

ухилення від санкцій

- фізичних та юридичних осіб країнах (в різних юрисдикціях), пов'язаних із мережею ухилення від санкцій та підтримують військово-промисловий комплекс росії;
- осіб, які причетні до ухилення від санкцій (зокрема, причетних до підтримання енергетичної можливості росії, спробу сприяти угоді про постачання зброї між Північною Кореєю та росією);
- осіб та організацій, за намагання обійти або уникнути санкцій та інших економічних заходів проти росії, каналів, які росія використовує для придбання критично важливих технологій, своїх майбутніх можливостей видобутку енергії та свого сектора фінансових послуг. Сполучені Штати Америки визначають осіб, які причетні до розширення майбутнього виробництва та експорту енергії в росії;

білорусь

- організацій та осіб у білорусі, пов'язаних з режимом Лукашенка, який є співучасником війни росії проти України;

зупинення привілеїв

- призупинення експортних привілеї для осіб і компаній за постачання заборонених товарів російській армії;
- призупинення експортних привілеїв для ряду компаній і російських громадян, які проживають у США, за перенаправлення частин цивільних літаків до росії;
- відмови в припиненні експортних привілеїв для групи Aratos (конгломерат з оборони та технологій, пов'язаних з НАТО) та її президента за ймовірну підтримку російських спецслужб;

торгівля людьми

- фізичних та юридичних осіб, пов'язаних із примусовим переміщенням та депортацією українських дітей.

Санкції Європейського Союзу

За 2023 рік Європейський Союз застосував санкції проти росії за повномасштабне вторгнення на територію України та інших країн за сприяння та підтримку дій росії у війні, зокрема, запроваджено санкції:

- щодо окремих секторів російської економіки (в тому числі обмеження цін на російські нафтопродукти). Введено обмеження експорту та імпорту, заморожування активів та заборону на в'їзд певних осіб;
- на осіб і організації, відповідальних за поширення пропаганди та підтримку війни (Recent Reliable News, RIA FAN);
- на приватну військову компанію Вагнер (ПВК «Вагнер»);
- на осіб і організації в білорусі через триваючі порушення прав людини та причетність країни до вторгнення росії в Україну, а також накладає обмеження на експорт певних технологій, у тому числі тих, що використовуються в авіаційній та космічній промисловості;
- проти Ірану за військову підтримку росії (зокрема щодо іранських виробників безпілотників), введено заборону ЄС експортувати до Ірану компоненти, які використовуються для розробки та виробництва безпілотних літальних апаратів (БПЛА);
- у вигляді заборони на поїздки та заморожування активів осіб, залучених до іранської програми БПЛА.

РОЗДІЛ ІІІ. РОЗШУК (ВИЯВЛЕННЯ) АКТИВІВ

Головним завданням Держфінмоніторингу є збирання, оброблення та проведення аналізу інформації про фінансові операції (будь-які дії щодо активів клієнта), що підлягають фінансовому моніторингу, інші фінансові операції або інформації, що може бути пов'язана з підозрою у легалізації (відмиванні) доходів, одержаних злочинним шляхом, фінансуванні тероризму чи фінансуванні розповсюдження зброї масового знищення.

Ключовою актуальною проблемою пошуку активів для застосування обмежувальних заходів у аспекті розпорядження такими активами полягає у тому, що переважна кількість бенефіціарів, які мають зв'язки із росією та з фізичними і юридичними особами, зазначеними у санкційних списках РНБО, володіють такими активами як бенефіціари з непрямим впливом, тобто через третіх осіб.

Крім цього, обмеженість доступу до іноземних реєстрів та/або обмеженість наявної інформації в таких реєстрах не завжди дає можливість швидко та ефективно ідентифікувати реального КБВ.

Головним завданням застосування обмежувальних заходів та розпорядження такими активами є виявлення зв'язку між підсанкційною особою та третьою особою, через яку підсанкційна особа здійснює керування активами, доведення зв'язку між ними та факту непрямого керування такими активами підсанкційної особи.

Іншим актуальним питанням є пошук активів осіб, які причетні до ВК/ФТ або вчинення інших кримінальних правопорушень.

Можливо навести наступні аспекти (методи) та індикатори, які дозволяють встановити управління активами:

- фактичне управління активами третіми особами;
- можливість прямо чи опосередковано вчиняти щодо активів дії з боку третіх осіб, тотожні за змістом здійсненню права розпорядження;
- наявність між власником та особою родинних, дружніх або інших зв`язків, відносин підпорядкування тощо;
- придбання, набуття права власності на актив за дорученням та/або в інтересах особи, яка не зазначена його власником;
- здійснення особою та/або власником, за його дорученням, витрат, пов`язаних з утриманням активу;
- здійснення особою та/або власником, за його дорученням, правочинів, пов`язаних з ефективним використанням активу;
- поліпшення властивостей активу або підлаштування умов його використання під власні потреби;
- можливість особою визначати користування активом іншими особами (наприклад, членами своєї сім'ї);

- можливість особою впливати на долю активу, в тому числі шляхом надання відповідного доручення власнику;
- наявність права особи та/або членів його сім'ї на отримання доходу від використання такого майна тощо.

Перший крок для пошуку активів визначити, чи має суб'єкт пошуку тісні зв'язки з конкретною країною.

При пошуку активів необхідно визначати профіль особи для пошуку, що його більш цікавить. Деякі з цих активів за своєю суттю є більш помітними та відстежуваними, ніж інші. Наприклад, породисті коні, які самі по собі можуть також виступати активом.

Утримання багаторівневих міжнародних офшорних структур може бути дорогим задоволенням, і для управління ними олігархи наймають спеціалізованих юристів і довірених професіоналів. Швидше за все, ці структури створено для захисту активів. Як правило країни з низьким рівнем прозорості є привабливими для приховування активів.

Активом може бути наприклад: нерухомість, трасти, судна або транспортні засоби (супер яхта, приватний літак або автомобіль), цінні папери чи облігації, предмети розкоші, витвори мистецтва, ювелірні вироби, готівка, кошти на банківських рахунках, криптоактиви та інші.

Як приклад, російські олігархи віддають перевагу країнам, які здатні забезпечити розкішне життя та верховенство права.

Наприклад, Нью-Йорк, Лондон і Париж є привабливими напрямками для купівлі нерухомості. Такі місця, як Монако, Об'єднані Арабські Емірати та Чорногорія, також дуже притягують своїм теплим кліматом.

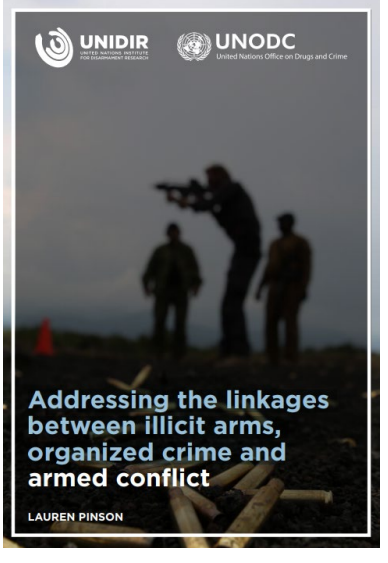
Активи олігархів, що фізично розташовані в таких місцях, як Європа, часто належать юридичним особам, зареєстрованим у юрисдикціях з режимом фінансової секретності, таких як Британські Віргінські острови, Ліхтенштейн та Панама.

РОЗДІЛ IV. ОГЛЯД АКТУАЛЬНИХ ДОСЛІДЖЕНЬ

Держфінмоніторинг продовжує діяльність з надання методологічної підтримки суб'єктам фінансового моніторингу, у тому числі шляхом вивчення, узагальнення та оприлюднення найкращих практик проведення фінансового моніторингу.

Держфінмоніторинг продовжує публікувати на вебсайті корисні дослідження та тематичні новини.

4.1. Дослідження щодо конфліктів та війни



Розгляд зв'язків між незаконною зброєю, організованою злочинністю та збройним конфліктом

Незаконна зброя та боєприпаси пов'язують конфлікт зі злочинністю, а також злочин із конфліктом.

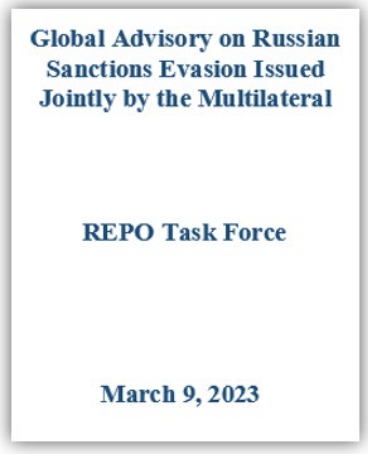
У цьому звіті досліджуються численні зв'язки між незаконною зброєю, організованою злочинністю та збройним конфліктом у зв'язку з (1) джерелом незаконної постачання зброї, (2) процес незаконного придбання зброї та (3) зміни в динаміці збройних конфліктів та організованої злочинності.

Конфлікт в Україні та його вплив на організовану злочинність і безпеку

У цьому звіті оцінюється вплив конфлікту в Україні та його наслідки для організованої злочинності та проблем, пов'язаних з безпекою для сусідніх країн, з акцентом на Молдову.

До них належать:

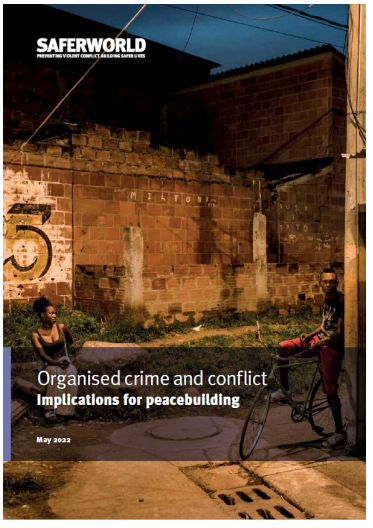
- організована злочинність і незаконна торгівля (включаючи торгівлю людьми, наркотиками, зброєю, незаконним тютюном та іншими товарами);
- кіберзлочини та шахрайство;
- дезінформація та пропаганда;
- хімічні, біологічні, радіологічні та ядерні загрози.



Глобальне консультування щодо ухилення від санкцій росією

Члени робочої групи REPO виявили різні випадки, коли російські еліти передавали бенефіціарну власність юридичних осіб та організацій, а також інше майно своїм дітям, намагаючись забезпечити постійний контроль, а також доступ до багатства після введення санкцій.

В іншому випадку учасники REPO встановили, що вказані олігархи напряму перераховували кошти членам родини, намагаючись приховати активи.

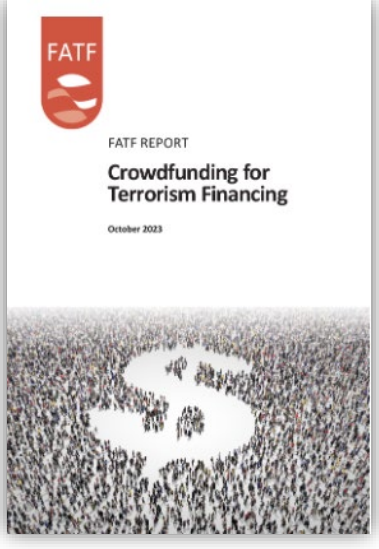


Організована злочинність і конфлікт: наслідки для розбудови миру

Цей звіт має на меті відійти від грубих інструментів закону та порядку (спрямованих на розрив мереж організованої злочинності) та боротьби з тероризмом (спрямованих на приниження збройних груп).

У ньому визнається потенціал мирних угод і зусиль з розбудови миру як важливих засобів для закладення основ для стійкого миру.

4.2. Дослідження щодо фінансування тероризму



Краудфандинг для фінансування тероризму (гуртове фінансування тероризму)

Гуртове фінансування (фінансування гуртом) – це співпраця людей, які добровільно об'єднують свої гроші чи інші ресурси разом, як правило через інтернет, аби підтримати зусилля інших людей або організацій.

Громадське фінансування може виконувати різні завдання – допомога постраждалим від стихійних лих, підтримка з боку вболівальників чи фанатів, підтримка політичних кампаній, фінансування стартап-компаній та малого бізнесу, створення вільного програмного забезпечення тощо.

Краудфандинг – це дуже корисний спосіб охопити велику аудиторію, щоб зібрати гроші на благодійну справу, фінансувати стартап або фінансувати творчий проєкт. Переважна більшість краудфандингової діяльності є законною, але події в усьому світі показали, що її також можна використовувати в незаконних цілях.

Це стосується терористів і терористичних груп, які можуть використовувати платформи збору коштів і краудфандингові дії в соціальних мережах, щоб отримати фінансування для своєї терористичної справи від глобальної аудиторії.

Ландшафт краудфандингу, ймовірно, розвиватиметься далі завдяки впровадженню нових платіжних технологій і поширенню онлайн-платформ, що підтримують різні типи краудфандингу. Однак у всьому світі існує недостатнє розуміння ризиків, пов'язаних із цим сектором, і через це регулювання різниться від країни до країни.

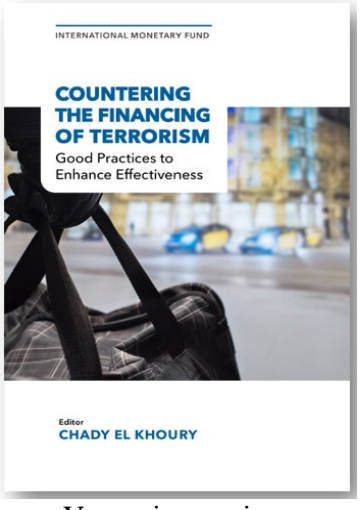
У цьому звіті FATF аналізується, як терористи зловживають платформами краудфандингу. У звіті, який базується на досвіді Глобальної мережі FATF, галузевих експертів, наукових кіл та громадянського суспільства, розглядаються проблеми, з якими стикаються під час виявлення та запобігання фінансуванню тероризму через екосферу краудфандингу. Проблеми включають складність краудфандингових операцій, використання методів анонімізації та відсутність підготовки та досвіду фінансування тероризму в індустрії краудфандингу для виявлення підозрілої діяльності.

У звіті висвітлюються передові практики, починаючи з включення краудфандингу в національну оцінку ризиків фінансування тероризму, охоплення сектору краудфандингу та ефективних внутрішніх і міжнародних механізмів обміну інформацією.

Перелік індикаторів ризику має на меті допомогти суб'єктам державного та приватного секторів, а також широкій громадськості визначити потенційні спроби фінансування тероризму за допомогою краудфандингу.

Боротьба з неправомірним використанням НПО для цілей фінансування тероризму

Терористи та терористичні організації можуть намагатися використовувати неприбуткові організації для збору та переміщення коштів, надання матеріально-технічної підтримки, заохочення вербування терористів, створення видимості легітимності або надання іншої підтримки терористичним організаціям.



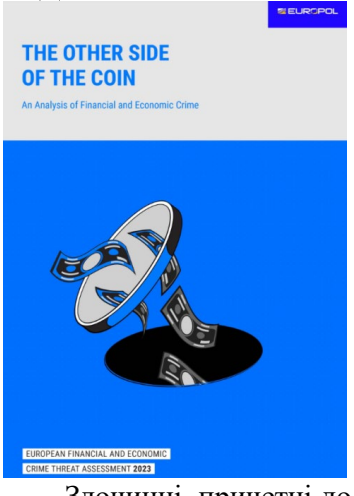
Боротьба з фінансуванням тероризму

Країни-члени МВФ стикаються зі значними проблемами, коли йдеться про підвищення ефективності боротьби з фінансуванням тероризму.

Це дослідження призначено для того, щоб допомогти розробникам політики та практикам у боротьбі з відмиванням грошей і фінансуванням тероризму (ПВК/ФТ) у визначенні ключових проблем і передових практик для підвищення ефективності механізмів боротьби з фінансуванням тероризму.

У дослідженні представлені доповіді експертів МВФ, ООН, Егмонтської групи підрозділів фінансової розвідки, Інтерполу та Європолу.

4.3. Дослідження щодо злочинності

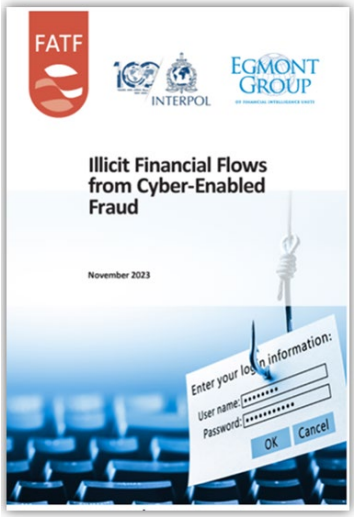


Оцінка загрози європейської фінансової та економічної злочинності до 2023 року

Європолом підготовлено всебічну та поглиблену оцінку загроз від фінансових та економічних злочинів на рівні Європейського Союзу.

Організована злочинність продовжує загрожувати внутрішній безпеці Європейського Союзу. Кримінальний ландшафт постійно змінюється, оскільки злочинці шукають нові можливості та використовують кризи у власних інтересах.

Злочинці, причетні до економічних і фінансових злочинів, дуже вправно використовують переваги економіки Європейського Союзу у своїх цілях і обирають своєю мішенню все більшу кількість жертв. Фактично, організована злочинність побудувала паралельну глобальну кримінальну економічну та фінансову систему навколо відмивання грошей, незаконних фінансових переказів та корупції.



Незаконні фінансові потоки від кібершахрайства

Кібершахрайство є великою транснаціональною організованою злочинністю, яка за останні роки експоненціально зросла як за кількістю повідомлених шахрайств, так і за їх глобальним поширенням.

Такі злочини можуть мати руйнівний вплив на окремих осіб, організації та економіку в усьому світі, спричиняючи значні фінансові втрати та підриваючи довіру до цифрових систем.

Транснаціональний характер цього злочину, коли доходи від кібершахрайства часто швидко переміщуються до різних юрисдикцій, викликає глобальне занепокоєння.

Оскільки цифрові інновації продовжують розвиватися, зростатимуть витонченість і масштаби кібершахрайства, якщо його не зупинити.

FATF у партнерстві з Групою Егмонт та Інтерполом проаналізували, як розвивався кібернетичний ландшафт шахрайства, його зв'язки з іншими злочинами та те, як злочинці можуть використовувати слабкі місця в нових технологіях. У звіті наводяться приклади національних оперативних заходів і стратегій, які довели свою ефективність у боротьбі з кібершахрайством, а також охоплює необхідність зруйнувати схеми, прискорити та розширити співпрацю в різних секторах як на внутрішньому, так і на міжнародному рівнях.

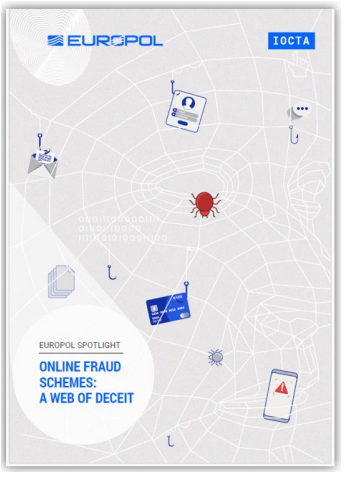
Важливо, щоб країни працювали разом і вживали заходів, щоб зупинити ескалацію загрози кібершахрайства.

У звіті визначено три пріоритетні сфери, в яких юрисдикції повинні діяти для більш ефективної боротьби з цим злочином і пов'язаним з ним відмиванням коштів:

- покращення внутрішньої координації між державним і приватним секторами;
- підтримка багатостороннього міжнародного співробітництва та посилення виявлення та запобігання шляхом підвищення обізнаності та пильності;
- полегшення повідомлення про такі злочини.

У звіті також визначено індикатори ризику, рекомендації та засоби боротьби з шахрайством, які можуть допомогти суб'єктам державного та приватного секторів виявити та запобігти кібершахрайству та пов'язаному з ним відмиванню грошей.

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



Схеми шахрайства в Інтернеті: мережа обману

Дослідження розглядає схеми шахрайства в Інтернеті, які включають широкий спектр злочинних дій, що здійснюються виключно або в основному в Інтернеті або за допомогою комп'ютерів.

Щороку шахраї отримують численні мільярди незаконних прибутків на шкоду окремим особам, компаніям і державним установам.

4.4. Огляд актуальних досліджень щодо віртуальних активів

Огляд законодавства щодо регулювання віртуальних активів

Держфінмоніторингом оприлюднено огляд, який корисний як суб'єктам державного фінансового моніторингу, так і установам, які займаються наданням послуг у сфері обороту віртуальних активів.

Банкам та окремим небанківським фінансовим установам також варто звернути на нього увагу з огляду на те, що вони є потенційними фінансовими посередниками, які будуть поєднувати постачальників послуг з обороту віртуальних активів із їхніми клієнтами.

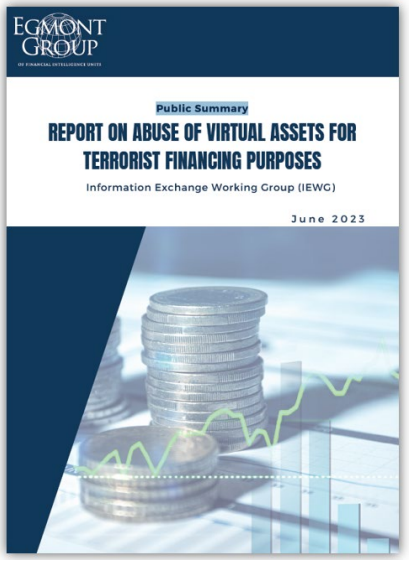
Ризики відмивання коштів та фінансування тероризму у світі віртуальних активів

Цей звіт представляє комплексний огляд ризиків відмивання коштів і фінансування тероризму у світі віртуальних активів та їхніх постачальників послуг у країнах-членах MONEYVAL.

Цільове оновлення в контексті імплементації стандартів FATF щодо віртуальних активів та VASP

Цей звіт є четвертим звітом FATF про глобальне впровадження Стандартів FATF щодо ВА та VASP, зокрема Travel Rule.

Звіт містить огляд глобальної імплементації Рекомендації 15; окреслює виклики імплементації Стандартів FATF; ділиться запропонованими рішеннями або прогресом, досягнутим державним і приватним секторами; а також надає огляд нових ризиків, пов'язаних з віртуальними активами.



Звіт про зловживання віртуальними активами з метою фінансування тероризму

Егмонтська група усвідомлює, що віртуальні активи можуть бути використані для фінансування тероризму.

Розуміння тенденцій у нових технологіях допоможе виявити потенційну вразливість, пов'язану з новими технологіями, зокрема віртуальними активами.

4.5. Дослідження щодо використання відкритих даних

Використання відкритих джерел для оперативного та стратегічного аналізу підрозділів фінансової розвідки (ПФР)

Робоча група з обміну інформацією (IEWG) Егмонтської групи (EG) ініціювала проєкт «Використання відкритих джерел для оперативного та стратегічного аналізу підрозділів фінансової розвідки (ПФР)», щоб оцінити ступінь впливу розвідки з відкритих джерел (OSINT) на оперативний і стратегічний аналіз.

Проєкт також мав на меті виявити найкращі практики, за допомогою яких ПФР визначають надійні джерела даних, і розробити список джерел інформації, які найчастіше використовуються.

РОЗДІЛ V. СПЕЦІАЛЬНА ЧАСТИНА ТИПОЛОГІЇ

Внаслідок широкомасштабної збройної агресії росії проти України значно зріс рівень усіх ризиків, які впливають на економічну стабільність та підривають національну безпеку України.

Росія провокує військові конфлікти в світі, зокрема, через скрите чи відкрите фінансування військових дій. Надалі росія використовує такі конфлікти для зменшення уваги в світі на агресію проти України та пропонує себе як рівноправного партнера на переговорах щодо врегулювання.

Найбільш розповсюджені схеми легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансування тероризму в умовах військової агресії російської федерації наведено нижче у відповідних розділах.

РОЗДІЛ 5.1. ФІНАНСУВАННЯ ТЕРОРИЗМУ ТА ВІДМИВАННЯ КОШТІВ ЯК ЧАСТИНА ФІНАНСУВАННЯ ВІЙНИ

Події, які останнім часом відбуваються в Україні (повномасштабна військова агресія росії, діяльність незаконних терористичних угрупувань, прояви сепаратизму та колабораційна діяльність на тимчасово окупованих територіях) засвідчують, що для їх здійснення необхідно неабияке фінансування, а отже, питання фінансування тероризму є надзвичайно актуальним для нашої держави.

Небезпека від фінансування тероризму полягає в тому, що такі дії створюють умови для існування та ефективної діяльності агресорам та їх пособникам, полегшують ведення агресивної військової та терористичної діяльності, та є суттєвою складовою у фінансуванні війни на території України.

З точки зору загрози для національної безпеки країни фінансування тероризму слід визначити як мультизагрозу. Тобто практика фінансування тероризму одночасно може мати багаторівневі характеристики, які негативно впливають на різні елементи.

Необхідність фінансових ресурсів для терористичної організації полягає в тому, що є потреба, власне, як у фінансуванні конкретних військових та терористичних актів, так і покритті витрат на поточну діяльність (від оплати праці найманців та навчання до розвідувальної діяльності).

Матеріальне сприяння терористичному угрупуванню полягає у передачі певного майна такому угрупуванню, або сприяння у заволодінні таким майном як відкрито, так і завуальовано. Майно може передаватись як безпосередньо (надання матеріальних цінностей або коштів від продажу незаконно привласненого майна, перерахування коштів на рахунки учасників терористичного об’єднання тощо), так і опосередковано (використання посередників, кур’єрів, проміжних банківських рахунків тощо).

Ідентифікація джерел фінансування тероризму є вкрай важливою складовою системи запобігання та протидії. Сьогодні джерела змінюють свою форму, проте в окремих випадках залишаються все ті ж, що діяли десятки років

тому, але зі зміною їх частки в загальному бюджеті терористичної організації – це і зовнішня фінансова підтримка на рівні окремих держав, релігійних організацій, фінансових установ і корпорацій, приватних осіб, а також кошти, які отримані внаслідок відмивання незаконних доходів, здобутих внаслідок вчинення інших злочинів.

Проте слід враховувати той факт, що на сучасному етапі наявна достатньо велика кількість способів фінансування тероризму, яке під впливом розвитку інформаційно-комп'ютерних технологій постійно розширюється та удосконалюється.

Поряд із традиційними способами з'являються нові, що базуються на доступності інтернету, стрімкому поширенні соціальних мереж, які на сьогодні виступають основним каналом фінансування тероризму приватними особами.

Крім того, навіть дієві, професійні механізми боротьби з фінансуванням тероризму необхідно модифікувати у зв'язку з появою нових загроз, впровадженням сучасних цифрових технологій.

Кіберпростір дозволяє значно полегшити доступ більшої кількості людей до пропаганди терористичних організацій та незаконної діяльності.

За таких умов особливу небезпеку з точки зору фінансування тероризму несе технологія DarkNet.

З однієї сторони DarkNet, спрямований на забезпечення недоторканності особистого життя та захисту від політичних репресій, а з іншої – приховує в собі низку небезпечних цілей. Зокрема, з його використанням відбуваються злочини у сфері інформаційних технологій, незаконне розповсюдження файлів, захищених авторськими правами, та фінансується тероризм.

DarkNet є дуже популярним місцем для різного роду незаконної діяльності, зокрема для продажу нелегальної зброї й вибухових речовин.

Для терористичних цілей DarkNet використовується не тільки для вербування найманців та пропаганди, але й для використання віртуальних валют. Криптовалюта часто використовується для платежів, пов'язаних з незаконною торгівлею, відмиванням грошей злочинними угрупуваннями та фінансуванням терористичної діяльності.

Розуміння джерел фінансування військових конфліктів та використання червоних прапорців є важливим для ПВК/ФТ/ФРЗМЗ.

Протягом останніх років терористичні організації диверсифікують свої джерела фінансування військових дій.

Один з напрямів такої диверсифікації є збір коштів в Інтернеті, як за допомогою традиційних платформ для внесків в Інтернеті та соціальних мережах, так і за допомогою криптовалют.

Узагальнені типові приклади, пов'язані з фінансуванням війни, у т.ч. через фінансування тероризму та відмивання коштів, наведено нижче.

Приклад 5.1.1. Схема прихованої діяльності фізичної особи, спрямованої на фінансування колабораційної діяльності

Держфінмоніторингом, з урахуванням інформації, наданої правоохоронним органом, виявлено схему прихованої діяльності фізичної особи, спрямованої на маскування походження коштів, які можуть бути спрямовані на фінансування колабораційної діяльності.

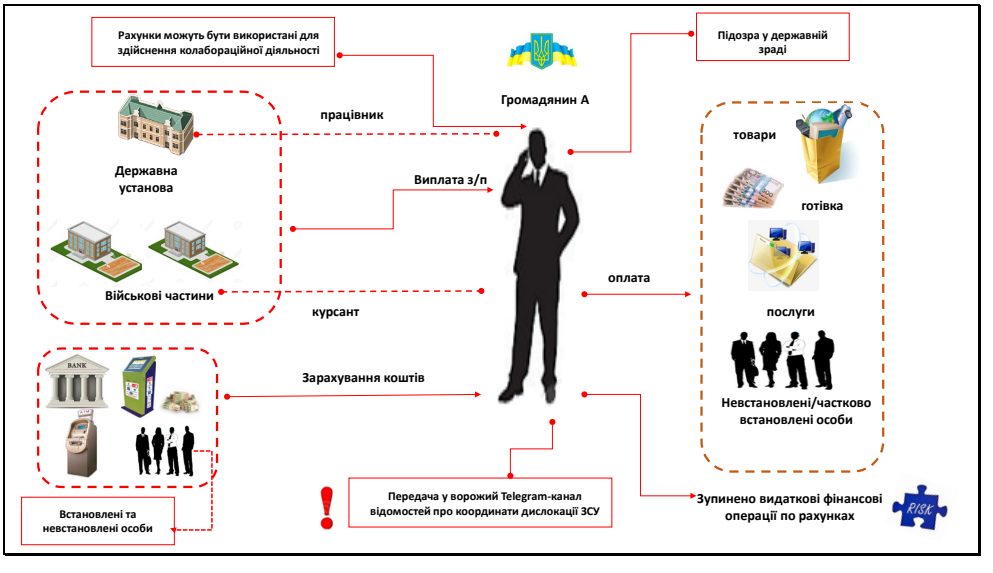
Військовослужбовцю **Громадянину А**, який передавав відомості про координати дислокації особового складу ЗСУ через ворожі Telegram-канали, правоохоронним органом повідомлено про підозру у державній зраді.

Відомо, що **Громадянин А** на момент повномасштабної збройної агресії російської федерації проти України був працівником державної установи та курсантом військових частин на території України.

Встановлено, що у **Громадянина А** наявна велика кількість рахунків, за якими крім зарахування заробітної плати, виявлено також значні зарахування коштів у готівковій/безготівковій формі від великої кількості (понад 200) ідентифікованих та невстановлених осіб і перерахування коштів на користь великої кількості (понад 50) ідентифікованих та невстановлених осіб. Більшість операцій по рахунках здійснена після початку повномасштабної збройної агресії російської федерації. Таким чином, отримані кошти буди винагородою за надані послуги та використані на фінансування колабораційної діяльності на території України.

Держфінмоніторингом прийнято рішення про зупинення видаткових фінансових операцій по рахунках **Громадянина А**.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.1.2. Залучення фізичних осіб-підприємців до протиправної фінансової схеми з метою обготівковування в банкоматах грошових коштів для фінансування протиправної діяльності на тимчасово окупованих територіях України

Держфінмоніторингом, з урахуванням інформації правоохоронного органу, виявлено схему незаконного отримання готівки для фінансування протиправної діяльності на тимчасово окупованих територіях із залученням фізичних осіб-підприємців.

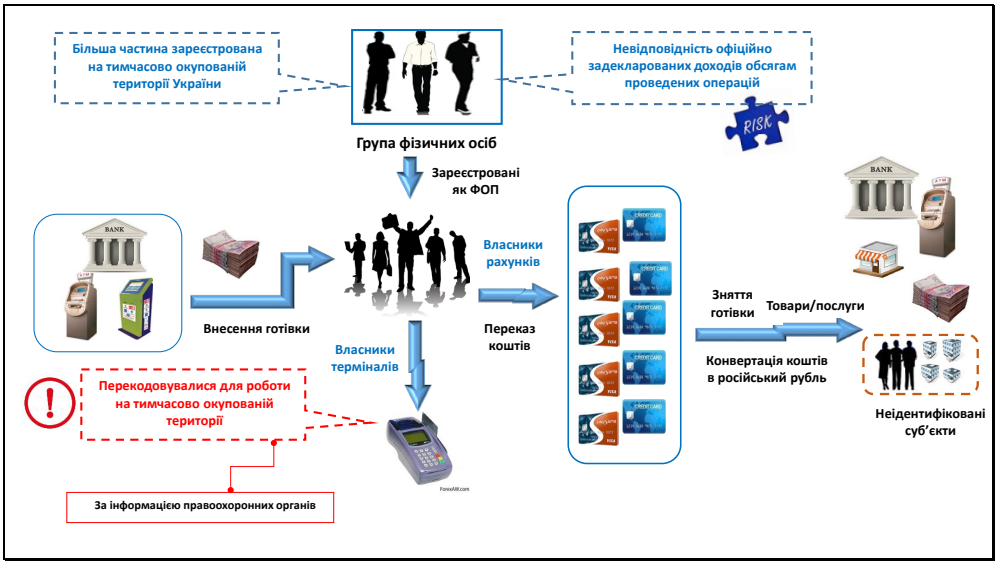
Встановлено, що громадяни України, у тому числі зареєстровані на тимчасово окупованих територіях, реєструвались як фізичні особи-підприємці та отримували від банківських установ в оренду банківські термінали, які надалі перекодовувались, встановлювались на тимчасово окупованих територіях та використовувались у незаконних операціях з отримання готівки.

Виявлено схему акумулювання значних безготівкових коштів з використанням еквайрингових розрахунків на карткових рахунках **Групи фізичних осіб-підприємців**. Після початку збройної агресії росії на ці рахунки вносились/зараховувались готівкові та безготівкові кошти як оплата різноманітних товарів, значна частина яких надалі знімалась готівкою або перераховувалась на рахунки неідентифікованих осіб.

При цьому, зазначеними **фізичними особами-підприємцями** або не задекларовано доходи взагалі, або задекларовано доходи, сукупна сума яких не відповідає обсягу проведених операцій, що може мати ознаки приховування джерел походження коштів.

Таким чином, виявлено схему надання незаконних послуг з приймання оплати від держателів платіжних карток за товари та видача їм готівки та ймовірного подальшого обміну безготівкової гривні на російські рублі, який окупаційна влада примусово намагається ввести в обіг.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.1.3. Схема використання банківських карток для здійснення валютно-обмінних операцій на тимчасово окупованих територіях

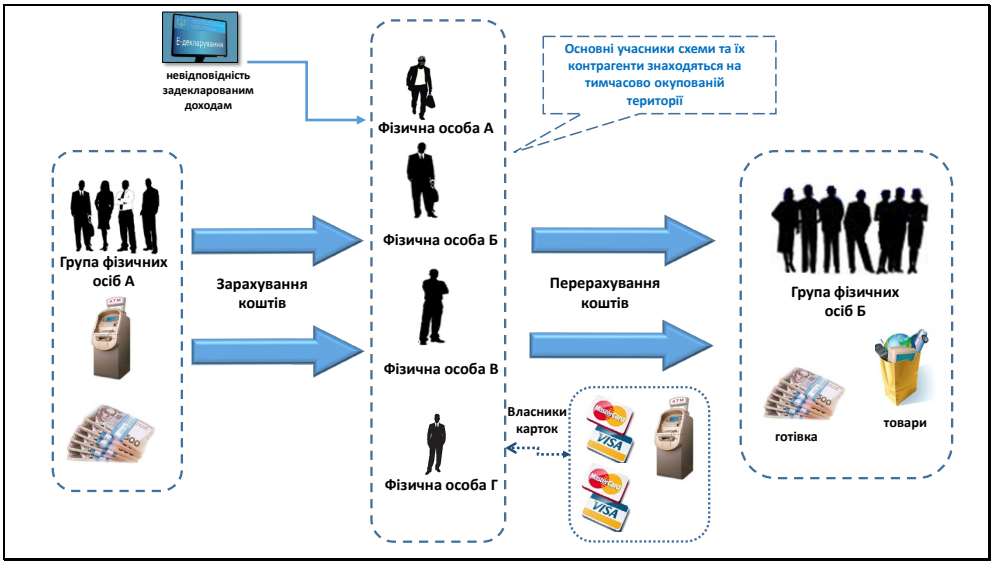
Держфінмоніторингом, з урахуванням інформації правоохоронного органу, виявлено фінансові операції, проведені фізичними особами, які не відповідають отриманим доходам та мають транзитний характер, що може свідчити про здійснення прихованої та колабораційної діяльності.

Відомо, що на тимчасово окупованих територіях окупаційною владою запроваджено безготівкові розрахунки виключно у російських рублях. З метою переведення гривні у рублі організовано незаконні валютообмінні пункти, які використовують банківські картки фізичних осіб, випущені українськими банками.

Встановлено, що на рахунки чотирьох **Фізичних осіб**, які підозрюються у пособництві державі-агресору, за короткий проміжок часу під час військової агресії російської федерації проти України зараховувались значні суми коштів у безготівковій формі від великої кількості осіб, які надалі перераховувалися на картки значної кількості інших фізичних осіб, здійснювались розрахунки за товари або зняття готівки. При цьому, джерела походження коштів та мета переказів невідомі та не очевидні.

Привертає увагу, що діяльність **Фізичних осіб** та їх контрагентів здійснюється на тимчасово окупованій території.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.1.4. Схема фінансових операцій фізичних осіб, спрямована на фінансування тероризму та колабораційної діяльності

Держфінмоніторингом, з урахуванням інформації правоохоронного органу, виявлено схему фінансових операцій фізичних осіб, спрямовану на фінансування тероризму та колабораційної діяльності на території України.

Відомо, що **Громадянин А**, використовуючи власний обліковий запис в «Telegram», під вказівками **Представника ФСБ** (росія) здійснював збір та передачу інформації про розташування військових об'єктів та об'єктів критичної інфраструктури на користь останнього.

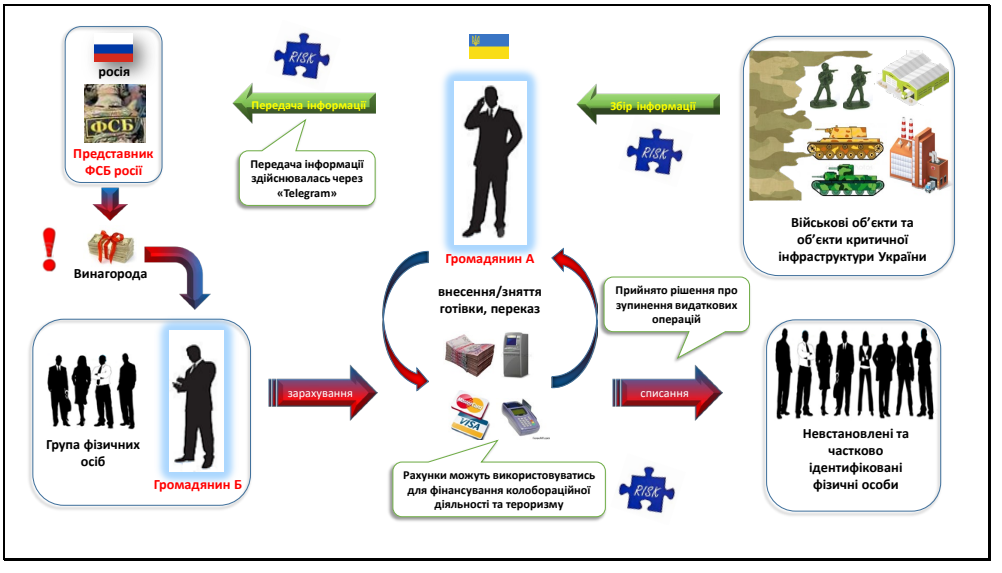
Встановлено, що на рахунок **Громадянина А** зарахувались кошти від групи фізичних осіб без зазначення мети переказів у готівковій/безготівковій формі. Надалі отримані кошти спрямовувались більш ніж на 100 карток невстановлених осіб як розрахунки за товари та послуги.

За передану інформацію, від **Представника ФСБ** через посередника **Громадянина Б** отримував винагороду, яка зараховувалась на його рахунок через банкомат та з власного карткового рахунку **Громадянина Б** із використанням відповідного додатку.

Також відомо, що **Громадянин Б** має майже 100 рахунків, відкритих в різних банківських установах, які використовуються в якості транзитних.

Таким чином, існують ризики, що здійснені фінансові операції можуть бути пов'язаними із фінансування тероризму та колабораційної діяльності на території України.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.1.5. Організація схеми зняття коштів з рахунків колаборантів, що знаходяться на тимчасово окупованій території

Держфінмоніторингом виявлено схему обготівковування коштів з використання рахунків фізичних осіб, які можуть бути використані для пособництва окупаційній владі та фінансування незаконної діяльності.

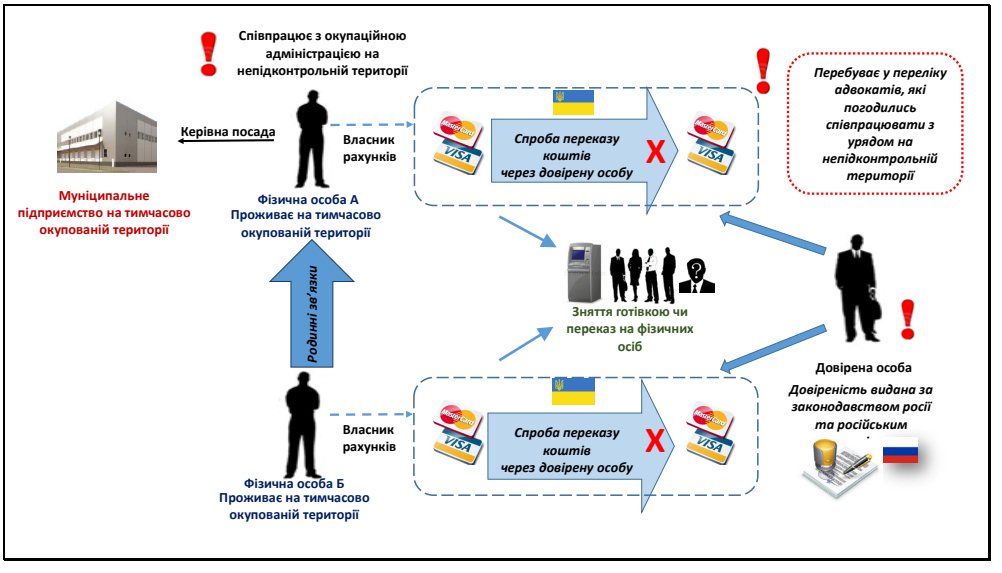
Встановлено спроби виведення коштів **Фізичною особою А**, що співпрацює з окупаційною адміністрацією на тимчасово окупованій території, займаючи керівну посаду в муніципальному підприємстві та його сином – **Фізичною особою Б**, які проживають на тимчасово непідконтрольній території.

Спроби переказів коштів здійснені **Довіреною особою** – адвокатом, що перебуває в переліку адвокатів, які погодились співпрацювати з урядом на тимчасово окупованій території.

Довіреності на користування рахунками **Фізичної особи А** та **Фізичної особи Б** видана **Довіреній особі** за законодавством країни-агресора – росії та завірені російським нотаріусом.

Також привертає увагу, що більша частина коштів, що зараховується на рахунки **Фізичної особи А** та **Фізичної особи Б** надалі переводилась у готівку, ймовірно, з метою їх конвертування в російські рублі та використання на тимчасово окупованій території.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.1.6. Схема прихованої діяльності юридичних та фізичних осіб, у тому числі нерезидентів із залученням віртуальних активів для фінансування терористичних угрупувань

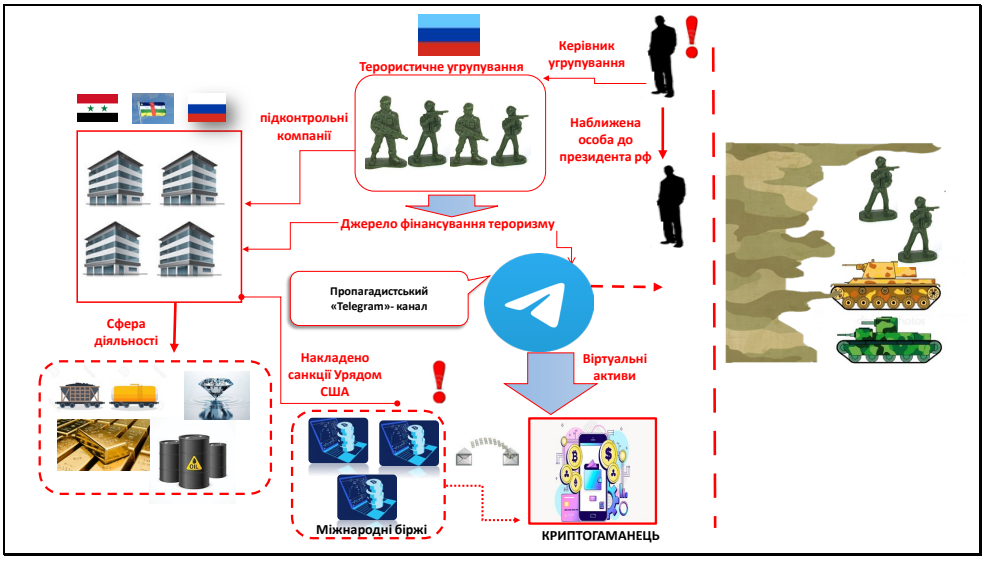
Держфінмоніторингом, з урахуванням інформації ПФР іноземної країни, виявлено схему прихованої діяльності юридичних осіб, у тому числі нерезидентів, спрямованої на маскування походження коштів, які можуть бути спрямованими на фінансування терористичних угрупувань росії.

Керівником терористичного угрупування створено схему із залученням значної кількості юридичних та фізичних осіб, у тому числі нерезидентів для фінансування своєї діяльності на території України, при цьому використовуючи нафтові та газові родовища на території країн, де воює дане угрупування.

Крім того, до підконтрольних компаній-нерезидентів **Терористичного угрупування** та фізичних осіб, які безпосередньо є учасниками угрупування, застосовані вітчизняні та міжнародні санкції.

Водночас встановлено додаткові джерела фінансування **Терористичного угрупування**, а саме за допомогою одного з пропагандистських Telegram-каналів могли отримувати віртуальні активи через поповнення криптогаманця з використанням міжнародних бірж. Отримані кошти надалі могли використовуватись на фінансування терористичної діяльності на території України.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.1.7. Схема використання рахунків фізичної особи для здійснення фінансування терористичної діяльності

Держфінмоніторингом виявлено схему фінансових операцій фізичної особи, яка може бути спрямована на фінансування терористичної діяльності на тимчасово окупованій території України

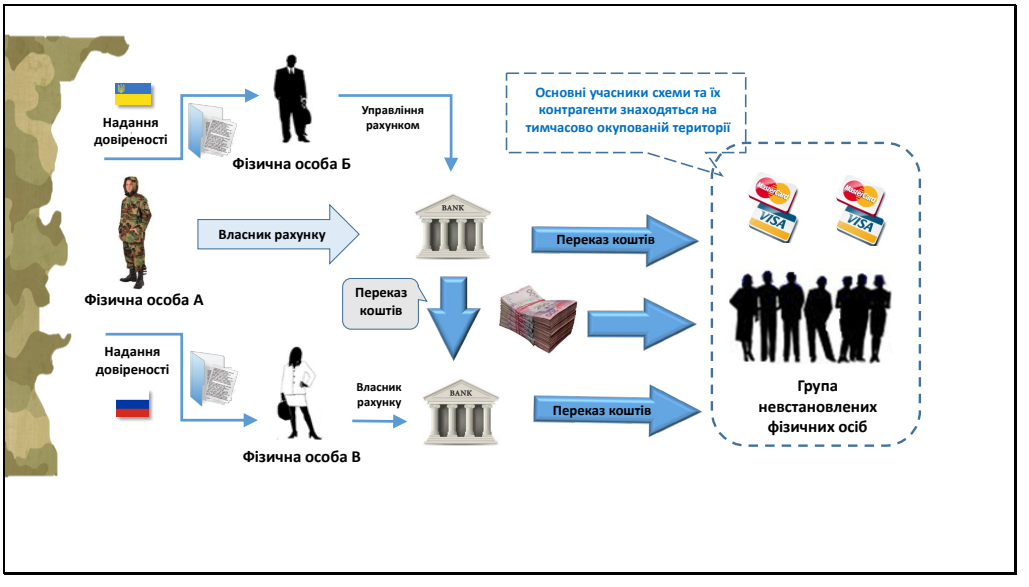
Встановлено, що рахунок **Фізичної особи А**, яка зареєстрована на тимчасово окупованій території, управляється іншою особою – **Фізичною особою Б** на підставі довіреності, виданої на території України. Фінансові операції по рахунку пов'язані зі списанням коштів через мобільний додаток на користь іншої довіреної особи – **Фізичної особи В**. Додатково встановлено, що **Фізична особа А** бере участь в незаконних збройних формуваннях на тимчасово окупованій території України.

Привертає увагу, що **Фізична особа А** надала **Фізичній особі В** довіреність на здійснення операцій за законодавством росії, завірену російським нотаріусом. При цьому почерк та підписи на довіреностях, виданих на території України та росії, візуально відрізняються між собою. До початку масштабної агресії **Фізична особа А** здійснювала операції по власному рахунку без участі довірених осіб.

Надалі кошти з рахунків **Фізичної особи А** та **Фізичної особи В** перераховано на картки спільних невстановлених осіб, що може свідчити про функціонування організованої групи для пособництва країні-агресору шляхом конвертації пенсійних виплат у російські рублі та використання на тимчасово окупованій території.

Держфінмоніторингом було прийнято рішення про зупинення видаткових операцій по рахунках **Фізичної особи А**.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.1.8. Схема ймовірного фінансування збройних формувань росії на тимчасово непідконтрольних територіях

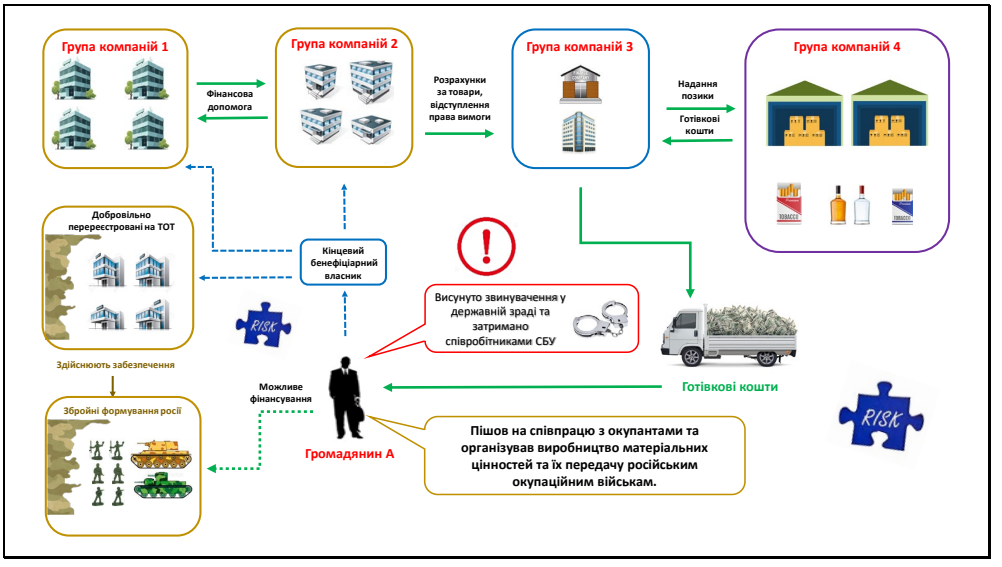
Держфінмоніторингом з урахуванням інформації правоохоронного органу виявлено схему щодо ймовірного фінансування збройних формувань росії на тимчасово непідконтрольних територіях.

Встановлено, що **Громадянин А –** кінцевий бенефіціарний власник ряду підприємств (**Група компаній 1**, **Група компаній 2**), добровільно пішов на співпрацю з окупантами та перереєстрував деякі підконтрольні йому підприємства за російським законодавством, відкрив рахунки у банківських установах росії, а також організував виробництво матеріальних цінностей та їх передачу російським окупаційним військам.

Також, встановлено, що між **Групою компаній 1** та **Групою компаній 2** здійснювалось циклічне перерахування коштів в якості надання/повернення матеріальної допомоги у значних сумах, частину з яких було перераховано на користь **Групи компаній 3** як розрахунок за промислові товари та відступлення права вимоги. Надалі, отримані **Групою компаній 3** кошти були перераховані як надання позик на користь **Групи компаній 4**, які здійснюють оптово-роздрібну торгівлю тютюновими виробами, алкогольними напоями та можуть мати необліковану готівку, з метою подальшого переведення безготівкових коштів у готівку.

Таким чином, здійснені фінансові операції можуть бути пов’язаними з переведенням безготівкових коштів у готівку з метою фінансування збройних формувань росії на тимчасово непідконтрольних територіях.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.1.9. Схема проведення фінансових операцій, які можуть бути пов'язаними із здійсненням колабораційної діяльності

Держфінмоніторингом виявлено схему проведення фінансових операцій **Громадянином А**, стосовно якого існують підозри у колабораційної діяльності, через банківську установу України.

Встановлено, що на рахунки **Громадянина А** надходила заробітна плата, у тому числі від підконтрольної державної установи, готівкові та безготівкові перекази від невстановлених та частково ідентифікованих осіб, у тому числі працівників державної установи. Відомо, що державна установа після початку повномасштабної агресії росії була перереєстрована за законодавством країни агресора. Також були перереєстровані інші підприємства, підконтрольні **Громадянину А** та його родині.

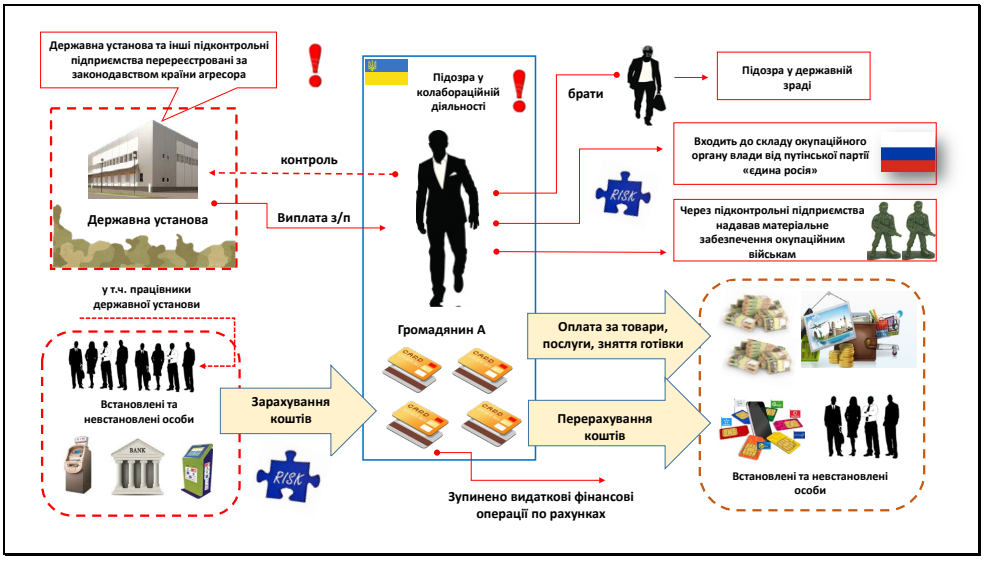
Отримані кошти надалі спрямовувались для оплати товарів і послуг, отримання готівки на тимчасово непідконтрольній території та перераховувались на користь невстановлених та частково ідентифікованих осіб. Також, на початку вторгнення **Громадянин А** здійснював валюто-обмінні операції та готівкові перекази в значних обсягах без відкриття рахунків.

Встановлено, що **Громадянин А** після окупації території України сприяв збройній агресії росії проти України та увійшов до окупаційного органу влади від путінської партії «єдина росія». Також встановлено, що **Громадянин А** через підконтрольні підприємства надавав матеріальне забезпечення окупаційним військам, зокрема пальним та продовольством. Крім того, за наявною інформацією **Громадянин А** причетний до незаконного вивезення українського зерна з тимчасово окупованої території.

Також відомо, що брату **Громадянина А** – колишньому народному депутату України, який входив до органів управління окупаційної адміністрації, оголошено підозру у державній зраді.

Держфінмоніторингом прийнято рішення про зупинення видаткових фінансових операцій по рахунках **Громадянина А**.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.1.10. Схема еквайрингових розрахунків на тимчасово окупованій території з метою отримання готівки

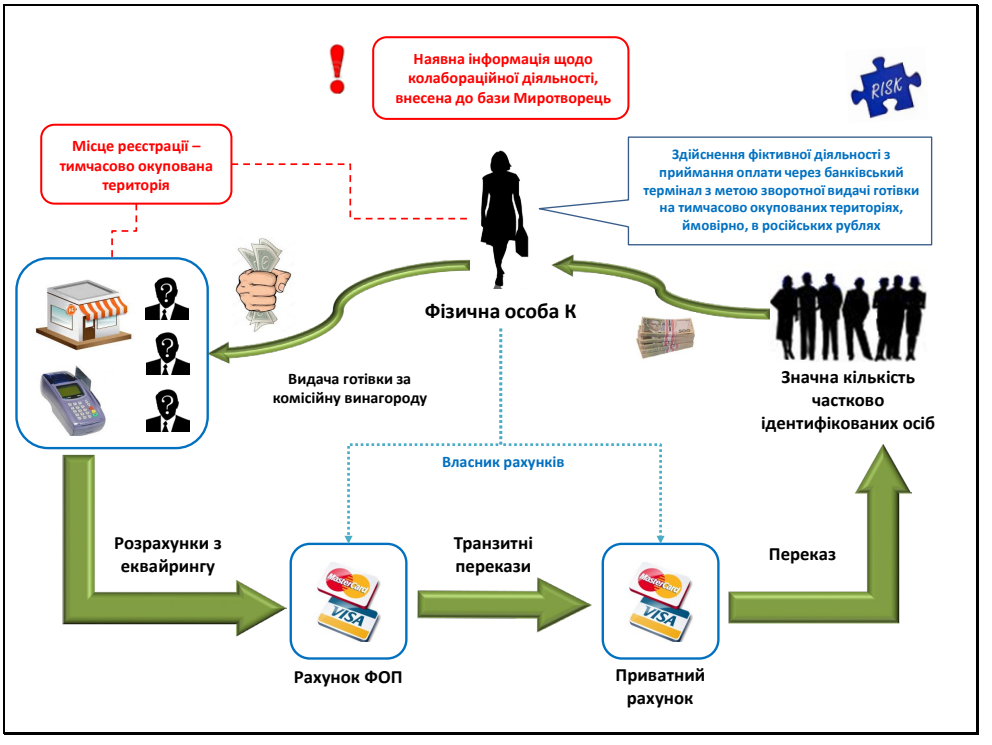
Держфінмоніторингом, з врахуванням інформації отриманої від суб'єкта первинного фінансового моніторингу, виявлено схему акумулювання значних обсягів безготівкових коштів з використанням еквайрингових розрахунків на рахунку **Фізичної особи – підприємця К**, з подальшим транзитним переказом на власний приватний рахунок, а згодом на рахунки значної кількості частково ідентифікованих осіб.

Фізична особа – підприємець К зареєстрована на тимчасово окупованій території. Зважаючи на обсяги, характер та місце проведення операцій, ймовірно, зазначеною особою надаються незаконні послуги з приймання фіктивної оплати (через банківський термінал) за товари чи послуги, з метою зворотної видачі готівкових коштів на тимчасово окупованих територіях, за певну комісійну винагороду.

В такий спосіб також може здійснюватися подальший обмін безготівкової гривні на готівковий російський рубль, який окупаційна влада примусово намагається ввести в обіг.

Привертає увагу, що **Фізична особа К** здійснює колаборайну діяльність та внесена до бази Миротворець.

Правоохоронним органом здійснюється досудове розслідування.



FinCEN ALERT

FIN-2023-Alert006 October 20, 2023

FinCEN Alert to Financial Institutions to Counter Financing to Hamas and its Terrorist Activities

Suspicious Activity Report (SAR) Filing Request:

FinCEN requests that financial institutions reference this alert in SAR field 2 (Filing Institution Note to FinCEN) and the narrative by including the key term "**FIN-2023-TFHAMAS**" and select SAR field 33(a) (Terrorist Financing-Known or suspected terrorist/terrorist organization).

The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) is issuing this alert to assist financial institutions in identifying funding streams supporting the terrorist organization Hamas.[1] FinCEN is urging financial institutions to be vigilant in identifying suspicious activity relating to financing Hamas and reporting such activity to FinCEN.

Hamas's horrific terrorist attack on the people of Israel on October 7, 2023, which left more than 1,000 innocent civilians, including citizens of the United States and dozens of other countries, wounded, killed, or taken hostage,[2] was funded by Hamas's terrorist finance network and practices.

Мережа боротьби з фінансовими злочинами Міністерства фінансів США (FinCEN) опублікувала попередження, щоб допомогти фінансовим установам у виявленні потоків фінансування, які підтримують терористичну організацію ХАМАС.

В повідомленні FinCEN наголошено, що ХАМАС збирає кошти для підтримки своїх операцій і членів наступними способами:

- підтримка з боку Ірану;
- приватні пожертви;
- глобальний портфель інвестицій;
- надання допомоги та підтримки від законних благодійних організацій;
- контроль прикордонних переходів і торгових операцій;

- вимагання, яке зазвичай має форму організованої злочинності із застосуванням погроз, жорстокого насильства;
- здирництво серед місцевого населення;
- збір коштів із використанням віртуальної валюти та фіктивних благодійних організацій, які збирають як фіатну, так і віртуальну валюту.

ХАМАС переміщує кошти через контрабанду фізичної валюти, а також через регіональну мережу причетних фінансових посередників, пунктів обміну валют і афілійованих з Хізбаллою фінансових установ.

FinCEN визначив ознаки червоного прапорця, щоб допомогти виявити, запобігти та повідомити про потенційну підозрілу діяльність, пов'язану з діяльністю ХАМАС у фінансуванні тероризму[4].

Ознаки червоних прапорців для виявлення підозрілої діяльності, пов'язаної з діяльністю ХАМАС

- клієнт або контрагент клієнта здійснює транзакції з юридичними та фізичними особами, визначеними OFAC, або транзакції, які містять зв'язок з ідентифікаторами, указаними для юридичних та фізичних осіб, визначених OFAC, включаючи адреси електронної пошти, фізичні адреси, номери телефонів або номери паспортів або віртуальні валютні адреси;
- інформація, включена в транзакцію між клієнтами, свідчить про підтримку терористичних кампаній;
- клієнт проводить транзакції з Money Services Business (MSB) або іншою фінансовою установою, включно з такою, яка пропонує послуги у віртуальній валюті, яка працює в юрисдикціях з підвищеним ризиком, пов'язаних з діяльністю ХАМАС, і обґрунтовано вважається або підозрює, що вона не проявляє належної обачності щодо клієнта. Діяльність фінансового посередника не відповідає найкращим практикам боротьби з відмиванням грошей/боротьбою з фінансуванням тероризму (ПВК/ФТ);
- клієнт здійснює транзакції, які походять від, спрямовані до або іншим чином залучають організації, які є підставними корпораціями, загальними «торговими компаніями» або іншими компаніями, які мають зв'язок з Іраном або іншими підтримуваними Іраном терористичними групами, такими як «Хезболла» та «Палестинський ісламський джихад»;
- клієнт, який є благодійною організацією або неприбутковою організацією збирає пожертви, але, здається, не надає жодних благодійних

[4]https://www.fincen.gov/sites/default/files/2023-10/FinCEN_Alert_Terrorist_Financing_FINAL508.pdf

послуг або відкрито підтримує терористичну діяльність або операції ХАМАС. У деяких випадках ці організації можуть розміщувати публікації на платформах соціальних мереж або в зашифрованих програмах для обміну повідомленнями, щоб отримати пожертви, зокрема у віртуальній валюті;

- клієнт, який є благодійною організацією або НПО, отримує великі пожертви з невідомого джерела протягом короткого періоду часу, а потім надсилає значні перекази або чеки іншим благодійним організаціям або НПО;
- клієнт здійснює транзакції з відомими або ймовірними адресами віртуальної валюти, пов'язаними з тероризмом або кампаніями, які через пожертви фінансують тероризм.

Жоден червоний прапорець не є визначальним для незаконної чи підозрілої діяльності, фінансові установи можуть враховувати сукупність наявних фактів і обставин, таких як фінансова діяльність клієнта в минулому, чи відповідають транзакції діловій практиці тощо.

Приклад 5.1.11. Продаж продуктів харчування для фінансування військових дій

У 2021 році ізраїльська влада вилучила 23 тони харчових продуктів, які призначалися для продажу в секторі Газа ХАМАС. Кошти від продажу призначалися для фінансування військових дій.

Приклад 5.1.12. Використання криптоактивів та криптобірж для фінансування радикальних угрупувань

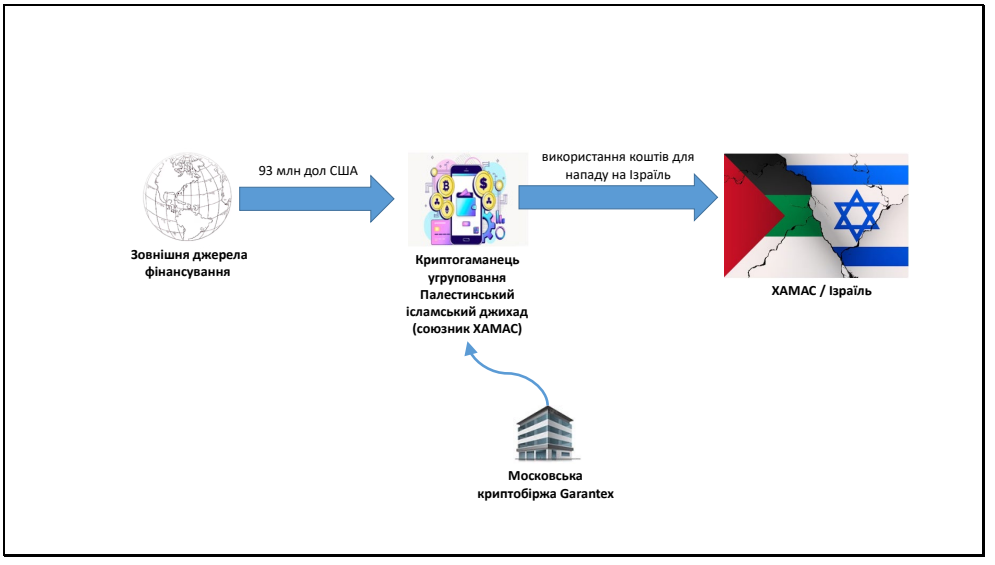
За даними ЗМІ, у 2023 році фінансування угруповання ХАМАС від зовнішніх джерел частково йшло через московську криптобіржу Garantex.

Незадовго до нападу на Ізраїль на цифрові гаманці, що належать угрупованню «Палестинський ісламський джихад», союзному до ХАМАС, було перераховано **93 млн дол США**. Частина цих коштів надійшла через російську біржу Garantex.

Garantex стала основним каналом проведення операцій з криптовалютами в російській юрисдикції.

Відносно криптобіржі Garantex відомо наступне:

- зареєстрована в Естонії, її ІТ-інфраструктура знаходиться в росії;
- криптобіржа має партнерські відносини з компаніями, зареєстрованими в ОАЕ та Таїланді;
- криптобіржу використовують заможні особи для виведення коштів з росії;
- криптобіржа використовується для відмивання доходів російськими кіберзлочинцями;
- відносно криптобіржі застосовані санкції з боку США через її роль в обході західних фінансових санкцій.



Приклад 5.1.13. Використання обміну віртуальної валюти за участю санкційної компанії

Введена під санкції компанія BuyCash, розташована в Газі, яка надає послуги з переказу грошей і обміну віртуальної валюти.

Цей постачальник послуг обробляє обсяги коштів, більші, ніж звичайна особа, і менші, ніж звичайний обмін. Деякі з них можуть бути більше схожими на позабіржових брокерів, тоді, як інші можуть бути більш схожими на вуличний грошовий бізнес, як хавала.

РОЗДІЛ 5.2. ОБХІД ФІНАНСОВИХ ОБМЕЖЕНЬ ТА САНКЦІЙ

Уведення окремими державами та міжнародними організаціями режиму санкцій проти російської федерації стало одним із ключових інструментів впливу на поведінку агресора на міжнародній арені. Обхід фінансових обмежень та санкцій на користь російської федерації залишається суттєвою проблемою.

Варто зазначити, що проблема ефективності торговельних санкцій полягає в тому, що технічно їх можливо обійти, використовуючи «сірий» імпорт та нейтральні країни. Попри зусилля держав, які вводять санкції, російська економіка продовжує функціонувати, використовуючи альтернативні ринки та партнерів, з якими поки що може успішно співпрацювати.

Для економічної стійкості та можливості забезпечувати фінансування війни проти України країна-агресор використовує нейтралітет КНР та держав Глобального Півдня, їхню неготовність приєднуватися до санкцій, накладених розвиненими країнами. Саме ці ринки стали основними споживачами

російських енергоресурсів та відіграють важливу роль у заміщенні західних товарів на російському ринку. Хоча ці держави на політичному рівні не підтримують війну росії проти України, однак їхнє небажання приєднуватися до західних санкцій фактично залишає поле для маневрів у торговельних відносинах.

Одним із важливих союзників росії у підтримці агресії проти України є Іран, який співпрацює одразу в кількох важливих аспектах: надає допомогу в пошуку способів та механізмів обходу росією санкцій чи обмеження їхнього негативного впливу на її економіку, тому що понад сорокарічний досвід існування й розвитку Ірану в умовах міжнародних санкцій є вкрай важливим для росії; сприяє в налагодженні роботи логістичних маршрутів, які допоможуть в обході санкцій; надає/продає росії різні типи зброї, оскільки інші країни не передають росії ані власну зброю, ані технології для її вироблення.

Іран за останні роки розробив окремі схеми обходу санкцій, які починає використовувати росія. Наприклад, використання тіньового флоту танкерів, що здійснює перевантаження нафти між танкерами посеред ночі з вимкненими приладами визначення місця розташування (транспондерами). Або використання підставних компаній для реалізації схеми зміни країни походження товару.

Розроблення логістичних маршрутів – важлива складова частина підтримки Іраном дій росії щодо обходу санкцій. Каспійське море є одним з основних шляхів постачання до росії ударних безпілотників іранського виробництва та іншої підтримки, яку Іран надає росії у зв'язку з війною проти України та західними санкціями.

З огляду на те, що запроваджені проти росії санкції поки що не забезпечують її повної міжнародної ізоляції, країна переорієнтовує свою економіку, у т.ч. торговельні операції, на країни Азії, Південного Кавказу та Близького Сходу. Привертає увагу значний економічний підйом у країнах – партнерах росії в цих регіонах, який, до того ж відбувається на тлі повномасштабної війни росії проти України та уповільнення світової економки внаслідок високої інфляції, складної ситуації на фінансових ринках та проблем із борговими зобов'язаннями у світі.

Різке суттєве зростання зовнішньої торгівлі товарами росії зафіксовано з Вірменією, Туреччиною, Туркменістаном, Грузією і Киргизстаном, що свідчить про високий ступінь зацікавленості росії в розвитку двосторонніх торговельних відносин. Водночас спостерігається різке зростання експорту з ЄС до Киргизстану та Казахстану технологій подвійного призначення, які використовуються в російському озброєнні.

Підсанкційні товари можуть також увозитися на територію росії без сплати мит та будь-якого контролю як транзитні товари, що призначені для постачання до країн Центральної Азії та Південного Кавказу, і залишатись у росії для використання, зокрема підприємствами військово-промислового

комплексу росії. Таким шляхом західні компоненти, зокрема, мікросхеми найбільших американських і європейських виробників, без проблем потрапляють на військові заводи агресора та використовуються при виготовленні зброї.

Агресор відчуває величезні економічні збитки від введених фінансових обмежень та санкцій, але кожного дня розробляє схеми, як їх обійти. Тому своєчасне виявлення таких схем надає змогу запобігти їх використання у майбутньому.

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

Приклад 5.2.1. Схема незаконного постачання на територію України продукції російського походження в обхід запроваджених санкцій

Держфінмоніторингом, з урахуванням інформації правоохоронного органу, виявлено схему незаконного постачання російської продукції на територію України в обхід вітчизняних санкцій та національних заборон щодо розрахунків з російською федерацією.

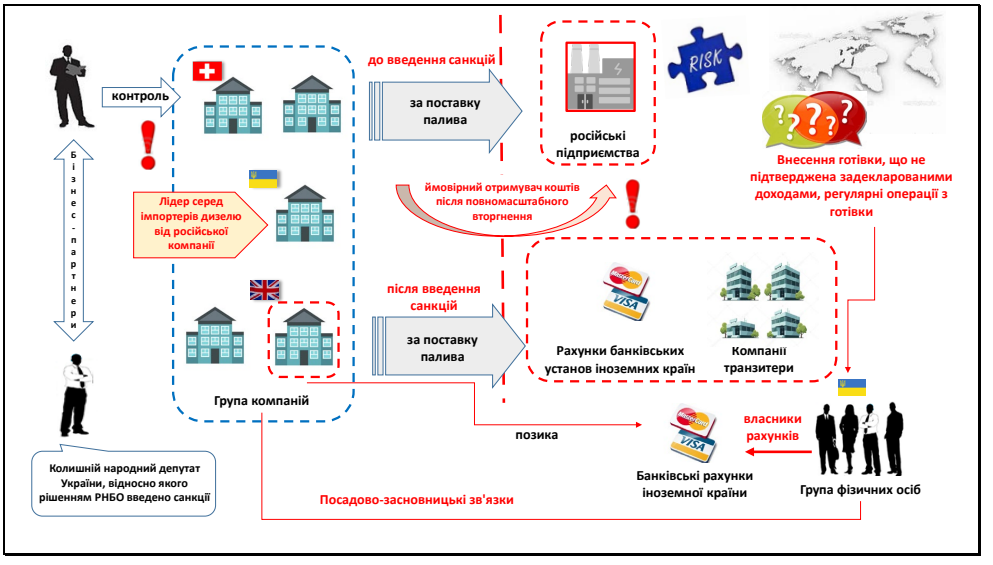
Встановлено, що **Група компаній**, до складу якої входять українські підприємства та компанії-нерезиденти, до початку повномасштабного вторгнення була найбільшим імпортером палива від російських підприємств на територію України та перераховувала основну частину коштів на користь російських постачальників, серед яких є компанія, що знаходиться під санкціями Сполучених Штатів Америки.

Також відомо, що діяльність **Групи компаній** контролюється бізнес-партнером колишнього народного депутата України, відносно якого рішенням РНБО України застосовано персональні спеціальні економічні та обмежувальні заходи (санкції).

Після початку масштабних військових дій на території України посадовими особами **Групи компаній** налагоджено механізм придбання нафтопродуктів російського походження із залученням підконтрольних компаній-нерезидентів шляхом внесення неправдивих даних щодо країн походження продукції до митних документів та проведення розрахунків через рахунки, відкриті в банківських установах країн Євросоюзу.

Крім того, за додатковою інформацією отриманої від ПФР іноземної країни відомо, що на закордонні рахунки **Групи фізичних осіб**, які мають посадово-засновницькі зв'язки з **Групою підприємств,** було зараховано значну суму коштів у вигляді позики, що, не виключено, могли бути винагородою за сприяння в прикритті незаконної діяльності.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.2.2. Схема незаконного виведення коштів по імпортним операціям на користь підприємств країни-агресора

Держфінмоніторингом, з урахуванням інформації правоохоронного органу та підрозділу фінансової розвідки іноземної країни, виявлено схему можливого незаконного придбання товарів від російських підприємств через транзитні європейські компанії.

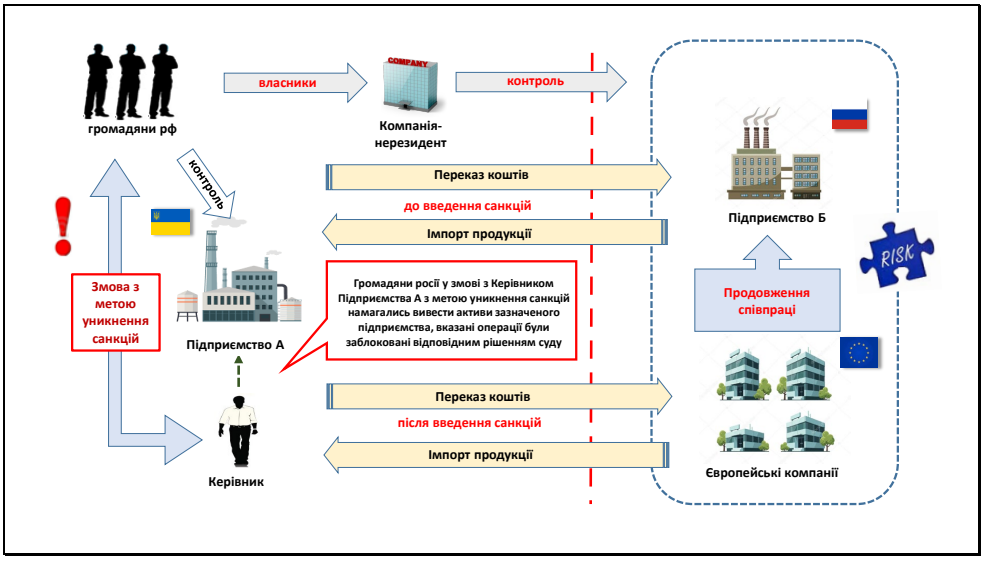
Встановлено, що до початку повномасштабного вторгнення українське **Підприємство А** здійснювало імпорт товарів від російського **Підприємства Б** та перераховувало на його користь кошти в значних обсягах.

Відомо, що на діяльність **Підприємства А** мають непрямий вирішальний вплив два **Громадяни росії**, відносно яких у 2023 році рішенням РНБО України застосовано персональні спеціальні економічні та обмежувальні заходи (санкції). Крім того, відомо, що вони також є власниками низки російських підприємств, які тісно співпрацюють з російськими державними органами.

Після початку масштабних військових дій на території України **Підприємство А** почало отримувати аналогічні товари від декількох **Європейських компаній**, які, за інформацією підрозділу фінансової розвідки іноземної країни, продовжують співпрацю з **Підприємством Б**.

Крім того, встановлено що **Громадяни росії** у змові з громадянином України **Керівником Підприємства А** з метою уникнення санкцій намагались вивести активи зазначеного підприємства, вказані операції були заблоковані відповідним рішенням суду.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.2.3. Виявлення активів осіб, афілійованих з підсанкційною особою

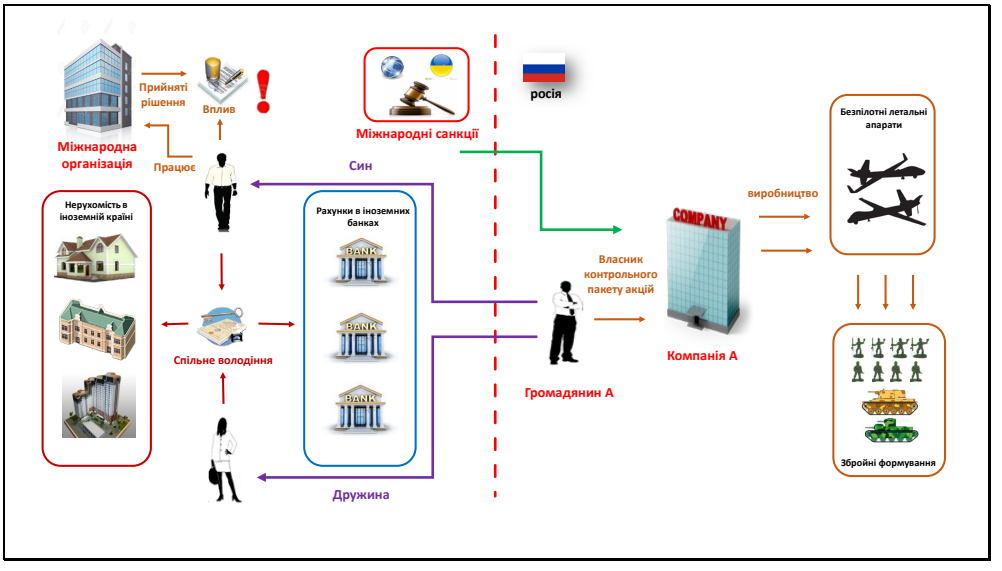
Держфінмоніторингом у співпраці з підрозділом фінансової розвідки іноземної країни, встановлено наявність активів осіб, афілійованих з підсанкційною особою.

Відомо, що Україною та рядом іноземних країн **введено** санкції проти російського підприємства оборонної сфери **Компанія А**, яка займається виробництвом безпілотних летальних апаратів. Крім того, до засновника **Компанії А** – **Громадянина А** згідно з рішенням РНБО України застосовано персональні спеціальні економічні та обмежувальні заходи (санкції).

Встановлено, що дружина та син **Громадянина А** мешкають за межами росії, мають відкриті рахунки в іноземних банківських установах та спільно володіють нерухомістю в одній з країн, яка ввела санкції проти **Компанії А**.

Крім того, син **Громадянина А** працює в міжнародній організації, пов'язаній з проблемами роззброєння, та, відповідно, може впливати на прийняті рішення і сприяти витоку службової інформації на користь країни-агресора.

Правоохоронними органами здійснюється досудове розслідування.



Приклад 5.2.4. Схема легалізації доходів, отриманих від компанії підконтрольної російському олігарху

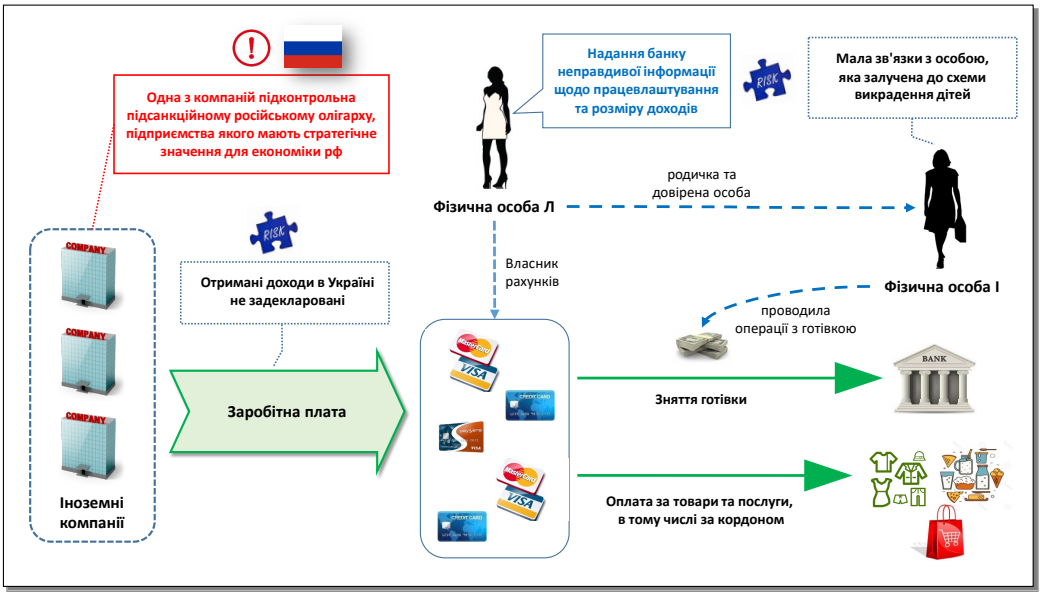
Держфінмоніторингом, з врахуванням інформації отриманої від іноземного ПФР, виявлено підозрілі фінансові операції, які проведені по рахунках **Фізичної особи Л**.

Так, на рахунки **Фізичної особи Л** зараховувались кошти від ряду іноземних компаній як виплата заробітної плати. За інформацією іноземного ПФР, власником однієї з іноземних компаній є підсанкційний російський олігарх, підприємства якого мають стратегічне значення для економіки росії.

Надалі кошти з рахунків використовувались для придбання товарів та послуг, в тому числі за кордоном, та частково знімались готівкою. Операції з готівкою проводила **Фізична особа І** – родичка та довірена особа **Фізичної особи Л**. Привертає увагу, що **Фізична особа І** мала зв'язки з особою, яка залучена до схеми викрадення дітей.

Також слід зазначити, що **Фізичною особою Л** надано до банку свідомо неправдиву інформацію щодо працевлаштування та розміру доходів. Крім того, доходи отримані **Фізичною особою Л** від іноземних компаній як заробітна плата в Україні не задекларовані.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.2.5. Схема незаконних операцій резидентів росії з оплати товарів подвійного призначення в обхід санкцій

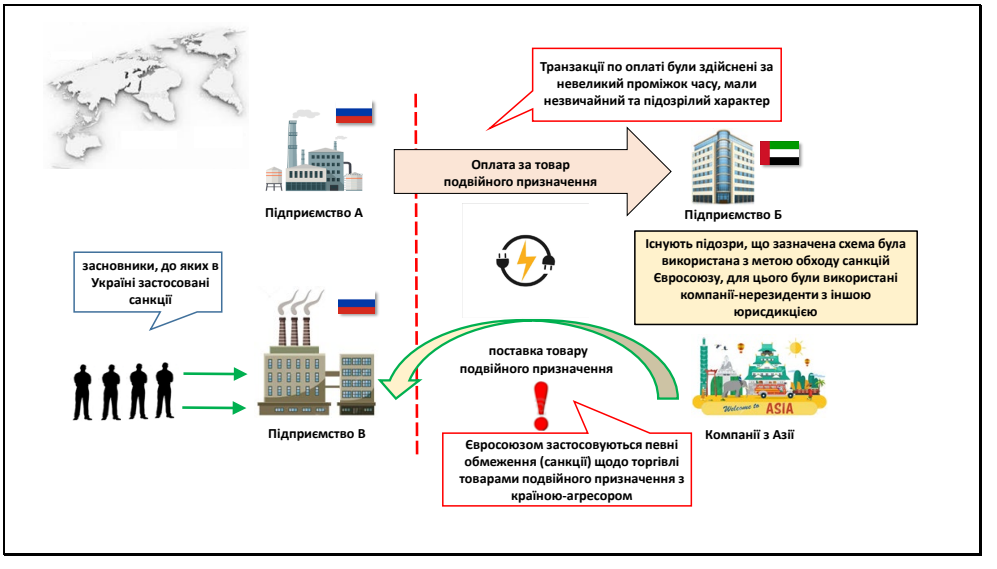
Держфінмоніторингом, з урахуванням інформації підрозділу фінансової розвідки іноземної країни, виявлено схему можливого незаконного придбання товарів подвійного призначення російськими підприємствами через транзитні компанії.

Встановлено, що російське **Підприємство А** після початку масштабних військових дій на території України здійснило перерахування значної суми коштів на користь **Компанії-нерезидента**, зареєстрованої в одній з країн на Близькому Сході, за товар подвійного призначення, до якого застосовуються певні обмеження Євросоюзу.

Привертає увагу, що перерахування здійснено протягом невеликого проміжку часу, при цьому транзакції мали незвичайний та складний характер.

Поставка зазначеного товару відбулась від інших **Компаній-нерезидентів** з країн Азії на користь іншого російського **Підприємства Б,** до засновників якого рішенням РНБО України застосовано персональні спеціальні економічні та обмежувальні заходи (санкції).

Правоохоронним органом здійснюється досудове розслідування.



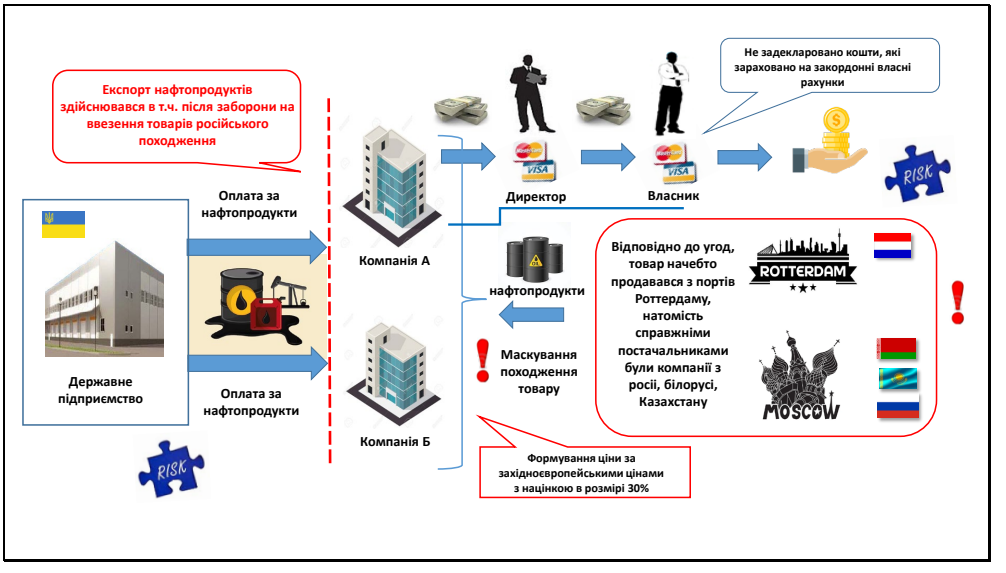
Приклад 5.2.6. Схема постачання продукції російського походження на територію України в обхід вітчизняних санкцій та національних обмежень

Держфінмоніторингом, з урахуванням інформації підрозділу фінансової розвідки іноземної країни, виявлено схему постачання продукції російського походження на територію України в обхід вітчизняних санкцій та національних обмежень щодо розрахунків з російською федерацією.

Встановлено, що дві іноземні **Компанії** здійснювали **Державному підприємству** поставку нафтопродуктів, де країнами походження товару були росія, білорусь та Казахстан, при цьому такі поставки продовжувались і після повномасштабного вторгнення рф та встановлення заборони на ввезення товарів з території країни-агресора. Привертає увагу, що відповідно до угод, нафтопродукти начебто продавались з портів Роттердаму, що давало можливість встановити західноєвропейські ціни, роблячи націнку в розмірі близько 30%.

В оплату поставленого товару **Державним підприємством** було здійснено перерахування коштів на користь цих **Компаній**. Надалі, директором **Компанії А** частину отриманих коштів по складному ланцюгу з використанням власних рахунків та рахунків підконтрольних компаній, відкритих в банківських установах різних країн, було перераховано на рахунки **Власника Компанії А**. При цьому ним не здійснено декларування коштів за ознаками доходу, отриманого за кордоном, що ймовірно є кінцевим етапом відмивання незаконних доходів **Державного підприємства**, отриманих внаслідок протиправного постачання продукції російського походження.

Правоохоронним органом здійснюється досудове розслідування.



РОЗДІЛ 5.3. РОЗКРАДАННЯ, ПРИВЛАСНЕННЯ, НЕЦІЛЬОВЕ ВИКОРИСТАННЯ ДЕРЖАВНИХ КОШТІВ, КОШТІВ СУБ'ЄКТІВ ГОСПОДАРЮВАННЯ ДЕРЖАВНОГО СЕКТОРУ ЕКОНОМІКИ ТА ЇХ ЛЕГАЛІЗАЦІЯ

Бюджетна сфера є життєво необхідною сферою економічних відносин, оскільки безпосередньо пов'язана з процесом формування, розподілу та контролю за використанням бюджетних коштів. Від законності цих відносин залежить ефективність реалізації державних оборонних, соціальних та інших програм, спрямованих на задоволення основних потреб України в умовах війни.

Разом з цим, бюджетна система України залишається досить привабливою для незаконних посягань. Злочини в цій сфері займають суттєву частку в структурі економічної злочинності.

В нинішніх умовах левова частка бюджету виділяється на оборону та безпеку у зв'язку з військовою агресією росії. Значне збільшення видатків на цю сферу створює певні ризики для можливої корупції, розкрадання бюджетних коштів.

Непоодинокими випадками стали закупівлі товарів оборонного призначення у компаній-нерезидентів з сумнівною репутацією, що призводить до неналежного виконання умов постачання товарів, які є необхідними на сьогодні. Залучення посередників з негативною бізнес-репутацією призводить до завищення вартості на придбання товарів за кошти підприємств державної власності та бюджетних установ.

Узагальнені типові приклади відмивання злочинних доходів, отриманих від розкрадання, привласнення, нецільового використання державних коштів та коштів суб'єктів господарювання державного сектору економіки, наведено нижче.

Приклад 5.3.1. Привласнення коштів державної установи з використанням іноземної компанії

Держфінмоніторингом виявлено схему незаконного заволодіння бюджетними коштами шляхом шахрайських дій за участю **Іноземної компанії**.

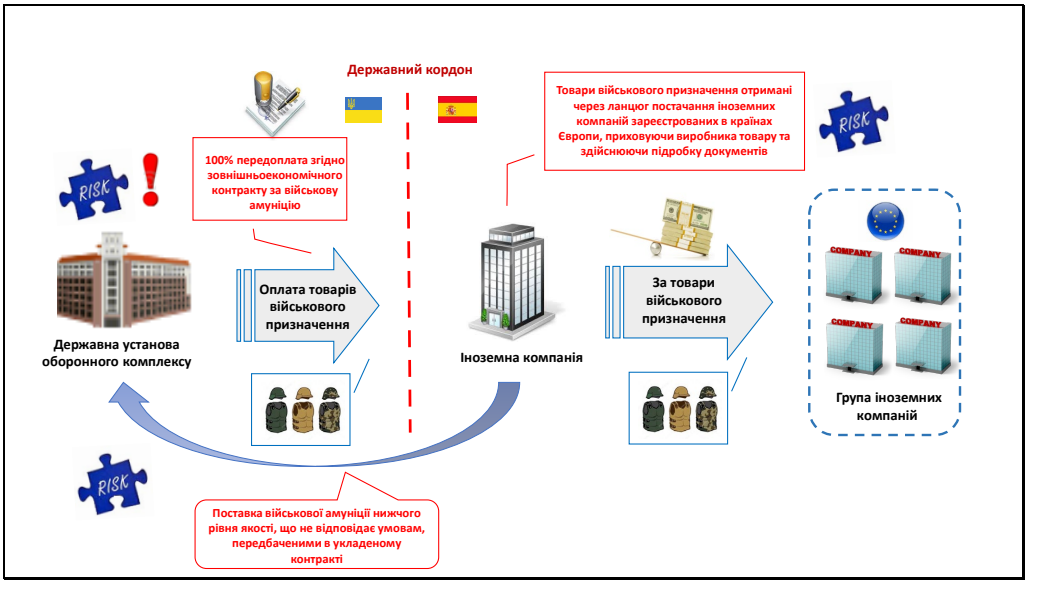
Встановлено, що **Державною установою оборонного комплексу** перераховано кошти на користь **Іноземної компанії** як оплата товарів військового призначення. При цьому, привертає увагу, що було здійснено 100% передоплату по контракту, що є достатньо ризиковим в умовах воєнного стану.

Надалі, отримані кошти **Іноземною компанією** було спрямовано на купівлю товарів військового призначення через ланцюг посередників **Групи іноземних компаній**, які зареєстровані в різних країнах Європи (приховуючи виробника товару та здійснюючи підробку документів щодо якості товарів).

В результаті на користь **Державної установи** було поставлено військову амуніцію нижчої категорії якості, ніж та, яка була зазначена у контракті.

Таким чином, постачання **Іноземною компанією** з використанням ланцюга посередників більш дешевого товару, який не відповідає замовленому рівню якості, призвело до привласнення частини бюджетних коштів, виділених на їх придбання.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.3.2. Розкрадання бюджетних коштів та їх подальша легалізація за кордоном

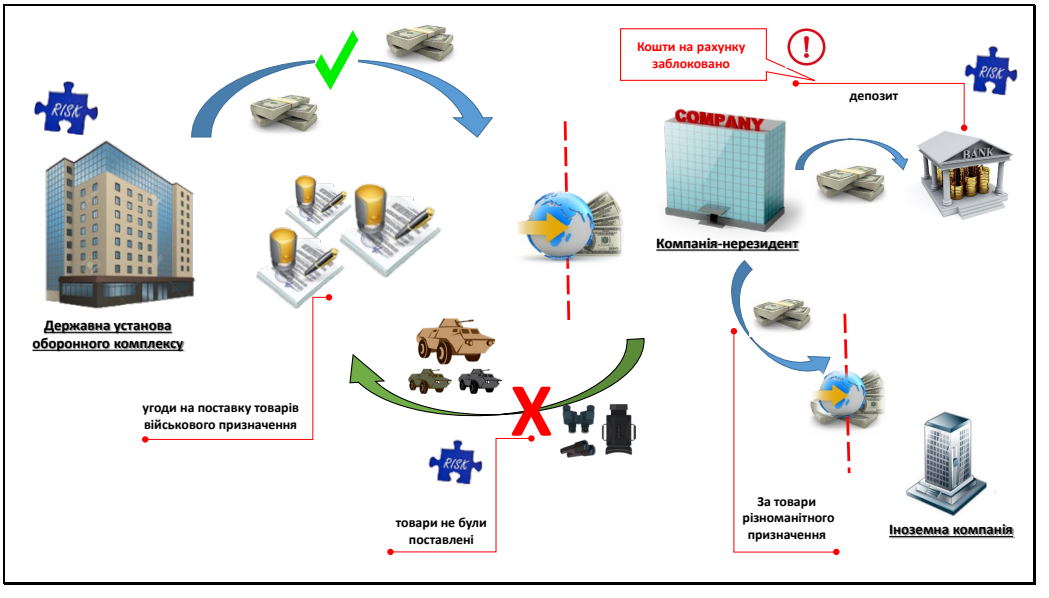
Держфінмоніторингом, з урахуванням інформації правоохоронного органу, виявлено наступну схему.

Державною установою оборонного комплексу та **Компанією - Нерезидентом** укладено низку угод, предметом яких є постачання товарів військового призначення. Натомість **Компанією - Нерезидентом** зазначені товари в обумовленому обсязі не поставлено, та бюджетні кошти не повернуто. Виявлено, що частина товару, яку **Компанія – Нерезидент** повинна була закупити в іншій країні для подальшого постачання в Україну, за рішенням уряду цієї країни була поставлена в Україну безкоштовно як допомога. Інша частина товару була поставлена у значно меншому обсязі, ніж це було передбачено угодою.

Разом з цим, надалі частина бюджетних коштів була акумульована на депозитному рахунку **Компанії – Нерезидента**, а інша частина перерахована на користь Іноземної компанії, за товари що не мають відношення до угод, укладених між **Державною установою** оборонного комплексу та **Компанією – Нерезидентом**.

Підрозділом фінансової розвідки іноземної країни заблоковано кошти, які розміщено на депозитному рахунку **Компанії – Нерезидента**.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.3.3. Привласнення бюджетних коштів з використанням афільованих нерезидентів з сумнівною репутацією

Держфінмоніторингом виявлено схему незаконного заволодіння бюджетними коштами шляхом проведення зовнішньоекономічних операцій з імпорту товарів оборонного призначення.

Встановлено, що **Державною установою** оборонної сфери було укладено контракт з **Підприємством А** на постачання військової продукції та здійснено передплату (яка не є обов'язковою) у розмірі 97% від загальної суми контракту. Своєю чергою, **Підприємством А** було укладено відповідний контракт з **Іноземною компанією**.

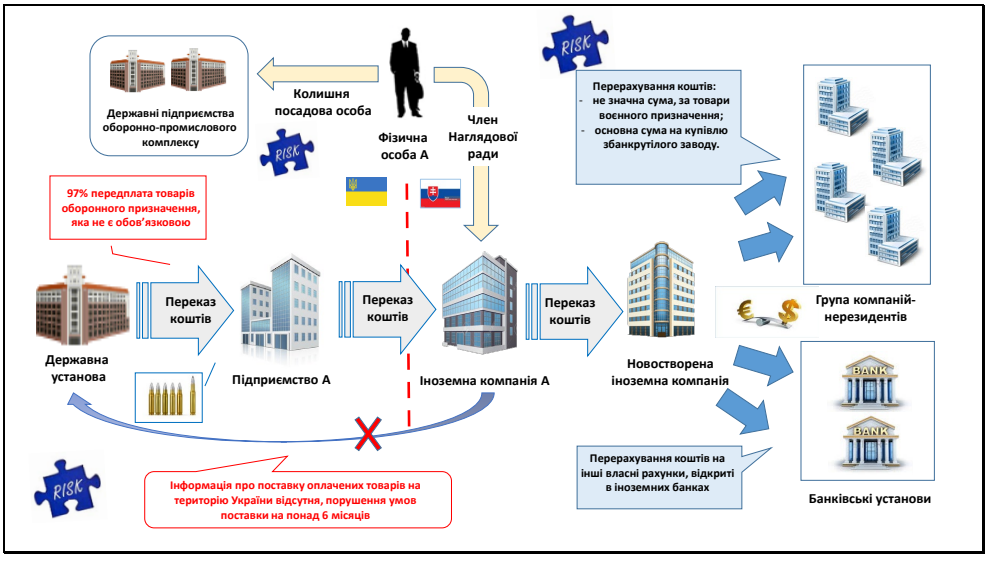
Відомо, що членом Наглядової ради **Іноземної компанії** є **Фізична особа А**, яка в минулому обіймала керівні посади у державних підприємствах оборонно-промислового комплексу України.

Надалі, 90% коштів було перераховано за товари оборонного призначення на користь **Новоствореної іноземної компанії**, яка була створена напередодні отримання коштів від **Державної установи.** Потім, незначну частину коштів було перераховано на користь **Групи компаній-нерезидентів** для купівлі товарів оборонного призначення.

Основну частинку коштів направлено як оплату за збанкрутілий завод та на власні рахунки, відкриті в іноземних банках. Товари оборонного призначення так і не були поставлені на територію України.

Таким чином, організовано схему заволодіння бюджетними коштами шляхом укладання зовнішньоекономічних договорів та залучення іноземних компаній з сумнівною репутацією.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.3.4. Легалізація (відмивання) доходів, отриманих від привласнення бюджетних коштів з використанням ланцюга транзитних підприємств

Держфінмоніторингом виявлено схему незаконного заволодіння бюджетними коштами шляхом їх нецільового використання через ланцюг підприємств, що здійснюють «транзитну» діяльність.

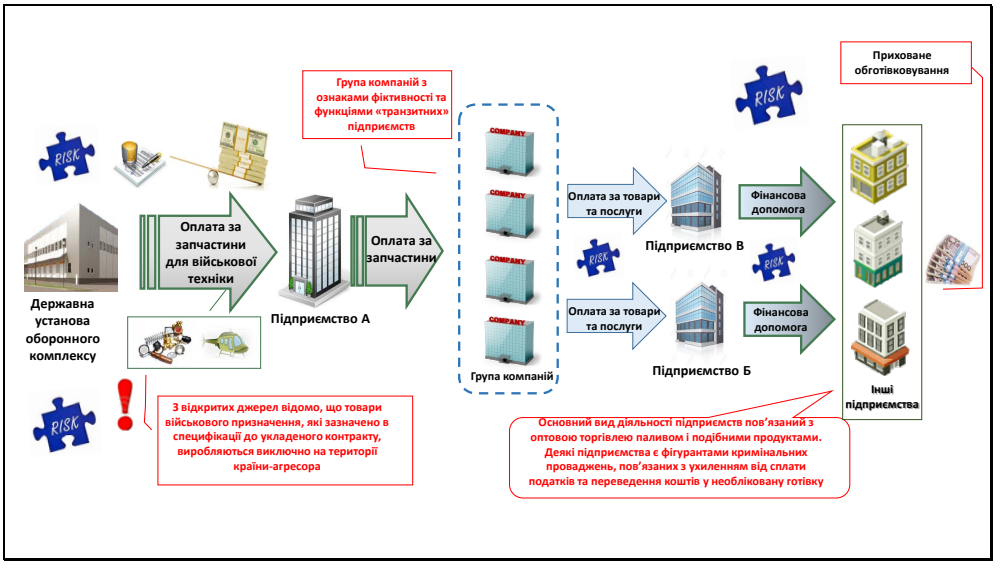
Встановлено, що **Державною установою** оборонного комплексу перераховано кошти на користь **Підприємства А**, як оплата за запчастини для військової техніки. При цьому з відкритих джерел відомо, що товари військового призначення, які зазначено в специфікації до укладеного контракту, виробляються виключно на території країни-агресора.

Надалі, отримані кошти **Підприємство А** спрямувало на оплату запчастин через ланцюг **Групи компаній**, які мають ознаки «транзитних» та фіктивних підприємств, які у свою чергу перерахували кошти на оплату товарів та послуг **Підприємству Б** та **Підприємству В**.

Отримані кошти **Підприємство Б** та **Підприємство В** перерахували у якості надання фінансової допомоги на **Інші підприємства**, діяльність яких спрямована на оптову торгівлю твердим, рідким, газоподібним паливом і подібними продуктами, з подальшим ймовірним (прихованим) обготівковуванням. Відомо, що деякі з цих підприємств є фігурантами кримінальних проваджень, пов'язаних з ухиленням від сплати податків та переведення коштів у необліковану готівку.

Таким чином, організовано схему привласнення бюджетних коштів, шляхом їх нецільового використання та залученням компаній з сумнівною репутацією.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.3.5. Легалізація (відмивання) доходів, отриманих від привласнення бюджетних коштів шляхом їх нецільового використання

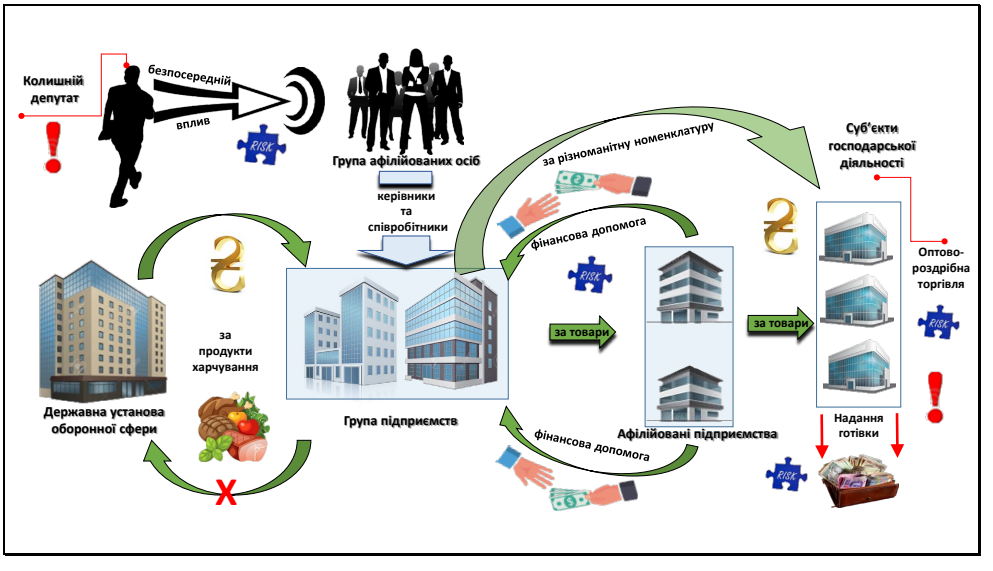
Держфінмоніторингом, з врахуванням інформації правоохоронного органу, виявлено схему незаконного заволодіння бюджетними коштами шляхом їх нецільового використання та залученням підконтрольних осіб в ланцюг придбання продовольчих товарів.

Встановлено, що **Державною установою оборонної сфери** перераховано кошти як оплату за харчові продукти для військовослужбовців на користь **Групи підприємств**. Надалі, зазначені кошти спрямовані на користь **Афілійованих підприємств** як оплата товарів та одразу повернуто у вигляді фінансової допомоги, після чого для придбання іншої номенклатури перераховувано на користь **Суб'єктів господарської діяльності,** що здійснюють оптово-роздрібну торгівлю продовольчими товарами.

Варто зазначити, що контроль над **Групою підприємств** здійснює **Колишній народний депутат України**.

Зважаючи на те, що **Суб'єкти господарської діяльності** проводять реалізацію товарів з використанням готівки, а також можуть надавати послуги з конвертації безготівкових коштів у готівку поза межами фінансової системи, ймовірно, перерахування коштів на їх рахунки здійснювалось з метою привласнення бюджетних коштів, їх подальшим обготівковуванням та формуванням податкового кредиту без фактичного постачання товару.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.3.6. Привласнення бюджетних коштів у будівельній сфері та їх легалізація з використанням осіб з ознаками фіктивності

Держфінмоніторингом, з урахуванням інформації правоохоронного органу, виявлено схему незаконного заволодіння бюджетними коштами шляхом їх нецільового використання з метою подальшої легалізації.

Встановлено, що **Бюджетною установою** було здійснено оплату на користь **Підприємства 1** та **Підприємства 2** за проведення будівельних робіт.

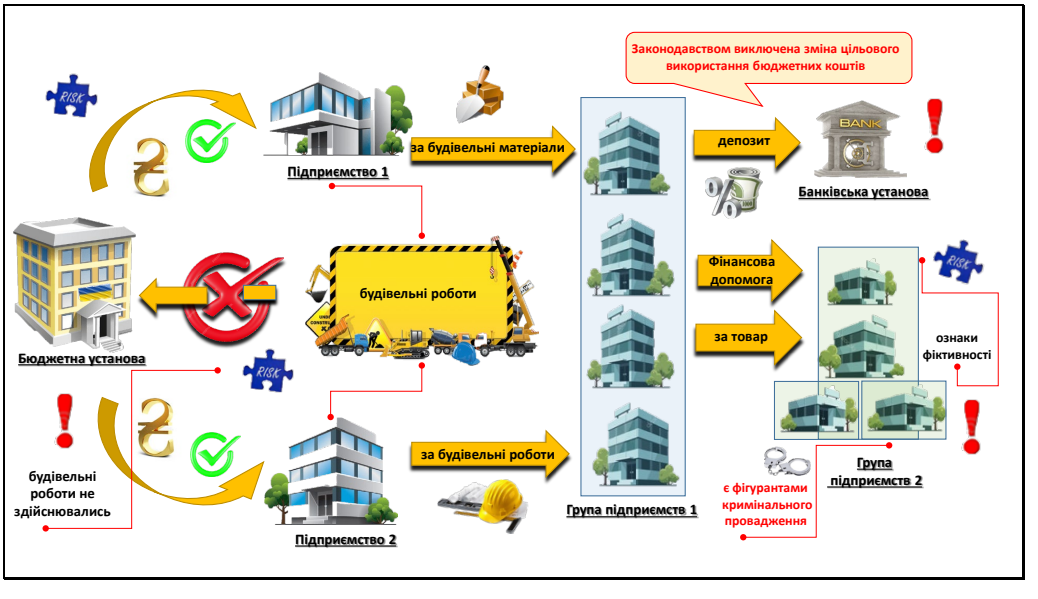
Надалі, отримані кошти було перераховано в якості оплати за будівельні матеріали та будівельні роботи на користь **Групи підприємств 1**. Далі частину коштів було перераховано на користь **Групи підприємств 2** в якості надання фінансової допомоги, оплати за товари, іншу частину коштів – на депозитні вклади в **Банківській установі.**

Варто зазначити**,** що **Група підприємств 2** мала чисельні ознаки фіктивності, зокрема, нікчемні розміри статутного капіталу, відсутність за місцем реєстрації та непрофільні напрямки діяльності. Крім того, деякі учасники **Групи підприємств 2** є фігурантами кримінальних проваджень за ознаками правопорушень, пов'язаних із легалізацією незаконних доходів.

За інформацією правоохоронного органу будівельні роботи, за які **Бюджетною установою** було сплачено кошти, виконані не були.

Таким чином, групою осіб організовано схему, спрямовану на привласнення бюджетних коштів з використанням ризикових фінансових інструментів «фінансова допомога», із залученням афілійованих суб'єктів господарювання з ознаками фіктивності.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.3.7. Легалізація (відмивання) доходів, отриманих від привласнення бюджетних коштів з використання фізичних осіб-підприємців

Держфінмоніторингом виявлено схему незаконного заволодіння бюджетними коштами шляхом штучного завищення вартості товарів та залучення афілійованих осіб до виконання контрактів.

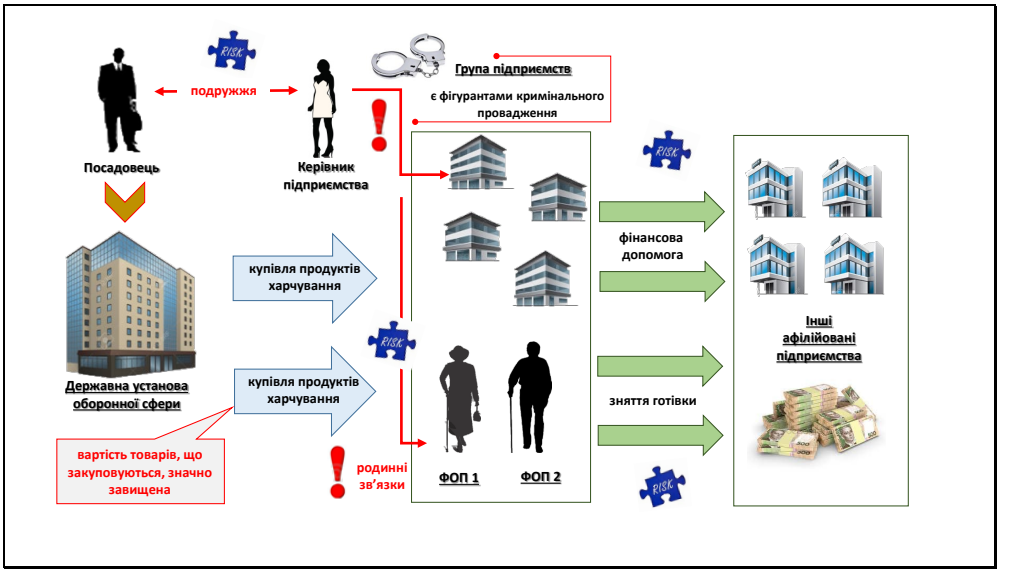
Встановлено, що **Державною установою** здійснено закупівлю товарів харчування, призначених для військовослужбовців, у **Групи підприємств** та **ФОП 1**, **ФОП 2**. При цьому, **Керівником** одного з підприємств є дружина **Посадовця,** який займає профільну посаду в **Державній установі**. Крім того, вона має родинні зв'язки з фізичними особами – підприємцями, які також є учасниками ланцюга придбання продовольчих товарів.

Серед **Групи підприємств**, залучених до виконання замовлень **Державної установи**, є юридичні особи, які наразі перебувають під слідством правоохоронних органів за сприяння в ухиленні сплати податків та відмивання коштів.

Надалі, кошти, отримані **Групою підприємств**, **ФОП 1 і ФОП 2** від **Державної установи**, частково перераховано як фінансова допомога **Іншим афілійованим підприємствам** та частково – переведено у готівку.

Результатом реалізації схеми є збільшення вартості товарів, придбаних **Державною установою**, що має на меті часткове їх привласнення з використанням корупційної складової.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.3.8. Заволодіння коштами державного підприємства шляхом примусового списання коштів

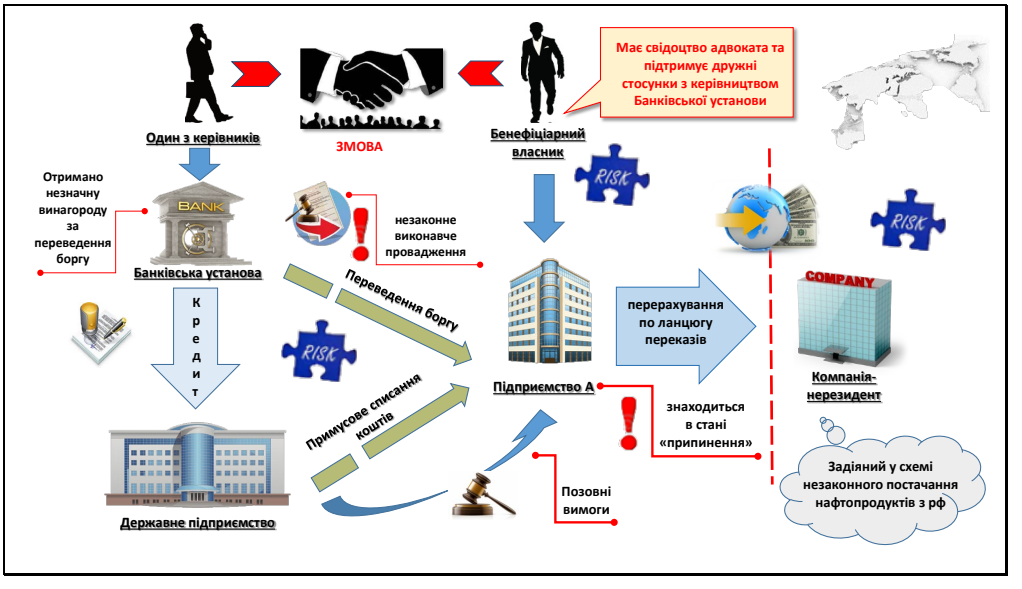
Держфінмоніторингом, з урахуванням інформації правоохоронного органу, виявлено схему заволодіння коштами державного підприємства шляхом незаконного оформлення правочину.

Встановлено, що **Підприємством А** оформлено набуття вимоги до **Державного підприємства** по його кредитним боргам перед **Банківською установою**. При цьому за таке переведення боргу **Підприємством А** було сплачено незначну винагороду на користь **Банківської установи**, джерелом походження якої стали особисті власника **Підприємства А**.

Надалі, всупереч чинному мораторію, було відкрито виконавче провадження та примусово списані кошти з рахунку **Державного підприємства** на користь **Підприємства А**. Отримані кошти по ланцюгу переказів було перераховано за межі України на користь **Компанії-нерезидента**, яка є учасником схеми незаконного постачання паливо-мастильних матеріалів з території росії.

Слід зазначити, що бенефіціарний власник **Підприємства А** має свідоцтво адвоката та підтримає дружні зв'язки з керівництвом **Банківської установи**.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.3.9. Розкрадання бюджетних коштів шляхом штучного завищення вартості продукції

Держфінмоніторингом, з урахуванням інформації правоохоронного органу, виявлено схему розкрадання бюджетних коштів шляхом зловживання службовим становищем та штучного завищення вартості продукції.

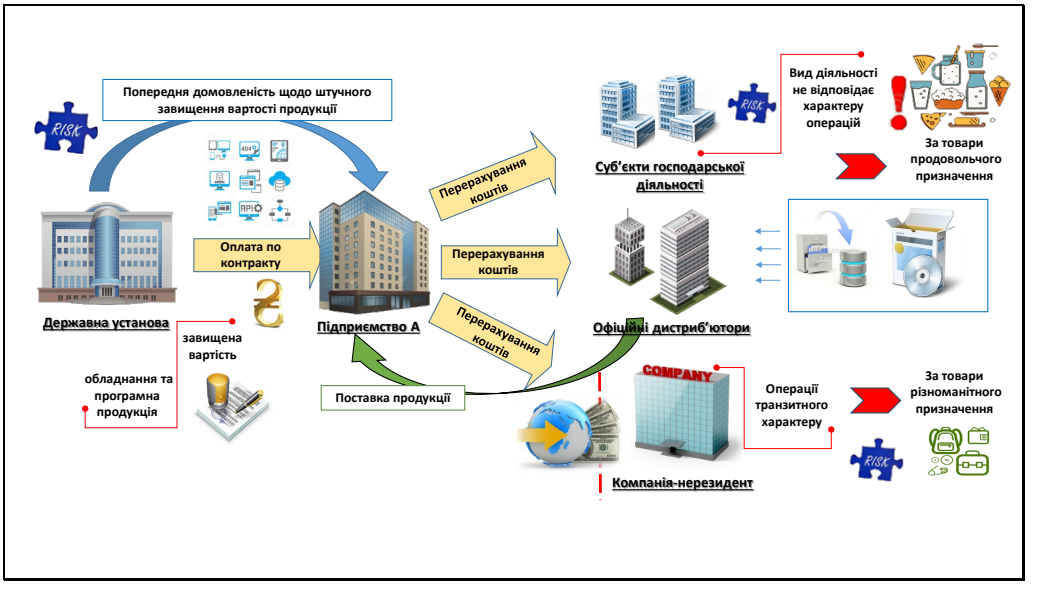
Встановлено, що між **Державною установою** та **Підприємством** було укладено угоди, предметом яких є поставка обладнання та програмного забезпечення. Враховуючи, що укладанню угод передувала домовленість посадових осіб **Державної установи** та **Підприємства**, вартість предмета угод була штучно завищена.

Отримані кошти **Підприємством** частково було перераховано на користь підприємств, які є офіційними дистриб'юторами продукції, замовленої **Державною установою**. Іншу частину коштів перераховано на користь **Суб'єктів господарювання** та **Компанії-Нерезиденту**.

Слід зазначити, що вид діяльності **Суб'єктів господарювання** не відповідає характеру замовлень, передбачених угодами на закупівлю обладнання та програмного забезпечення, та надалі кошти спрямовані на придбання продовольчих товарів.

Крім того, встановлено, що кошти, отримані **Компанією-Нерезидентом**, надалі перераховано на користь ряду інших компаній, переважно азійських, за різноманітну номенклатуру товарів, не пов'язану з предметом вищезазначених укладених угод.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.3.10. Заволодіння бюджетними коштами шляхом придбання товару за завищеними цінами

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

Держфінмоніторингом, з врахуванням інформації правоохоронного органу, виявлено схему заволодіння бюджетними коштами шляхом завищення цін при укладанні договорів постачання продовольчих товарів з обласними військовими адміністраціями.

Встановлено, що **Державним підприємством** згідно з укладеними договорами кошти перераховано як оплату за продовольчі товари на користь **Юридичної особи А**, які надалі було перераховано на користь **Компанії-нерезидента Б.**

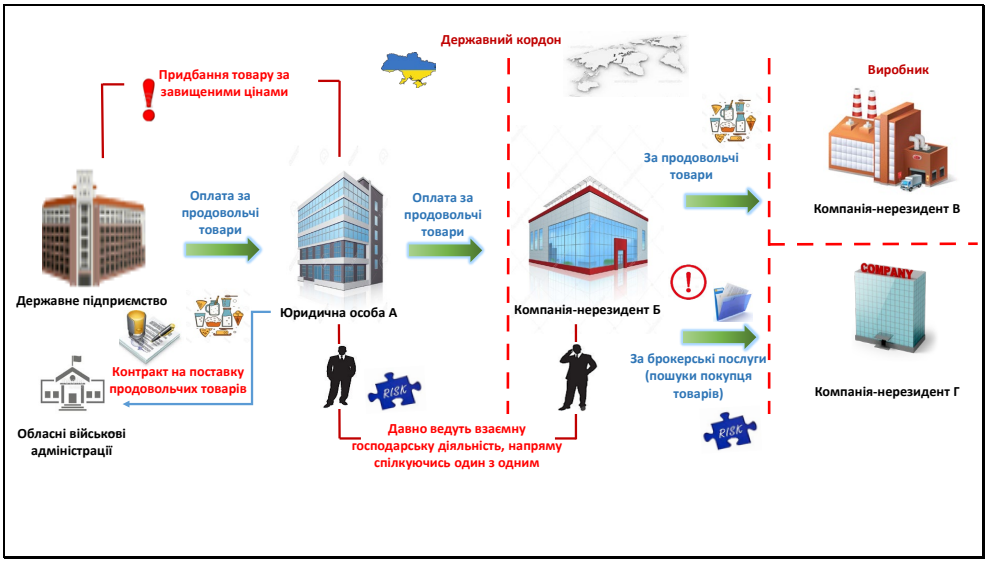
Своєю чергою, **Компанія-нерезидент Б** спрямувала лише частину даних коштів на рахунки виробника товарів – **Компанії-нерезидента В**.

Ще частину коштів було перераховано на користь **Компанії-нерезидента Г** як оплату брокерських послуг з пошуку для **Компанії-нерезидента Б** покупця продовольчих товарів, тобто **Юридичної особи А**.

При цьому, за інформацією правоохоронного органу, фактичні власники цих підприємств ведуть взаємну господарську діяльність, напряму спілкуючись один з одним.

Таким чином, виявлено схему заволодіння бюджетними коштами шляхом завищення цін при укладанні договорів постачання продовольчих товарів з подальшою легалізацією частини отриманих коштів, шляхом їх перерахування на користь **Компанії-нерезидента Г**.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.3.11. Привласнення бюджетних коштів з використанням іноземних компаній, які контролюються експосадовцями

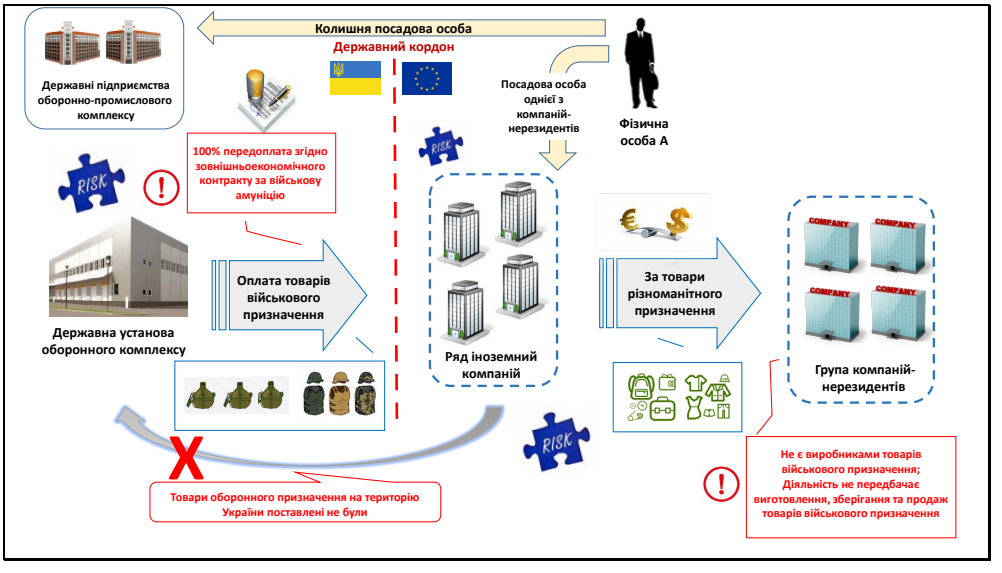
Держфінмоніторингом з урахуванням інформації правоохоронного органу виявлено схему незаконного заволодіння бюджетними коштами шляхом шахрайських дій з імпорту товарів за участю компаній-нерезидентів.

Встановлено, що **Державною установою оборонного комплексу** було укладено контракти з **Рядом іноземних компаній** на постачання військової продукції та здійснено передплату (яка не є обов'язковою) у розмірі 100% від загальної суми контракту.

Посадовою особою однієї з компаній-нерезидентів є **Фізична особа А**, яка в минулому обіймала керівні посади у державних підприємствах оборонно-промислового комплексу України.

Надалі, **Рядом іноземних компаній** отримані кошти як оплату за різноманітні товари було розпорошено на значну кількість **Компаній-нерезидентів**, які не є виробниками товарів військового призначення та діяльність яких не передбачає виготовлення, зберігання та продаж товарів військового призначення.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.3.12. Привласнення коштів державної установи із використанням гуманітарної допомоги

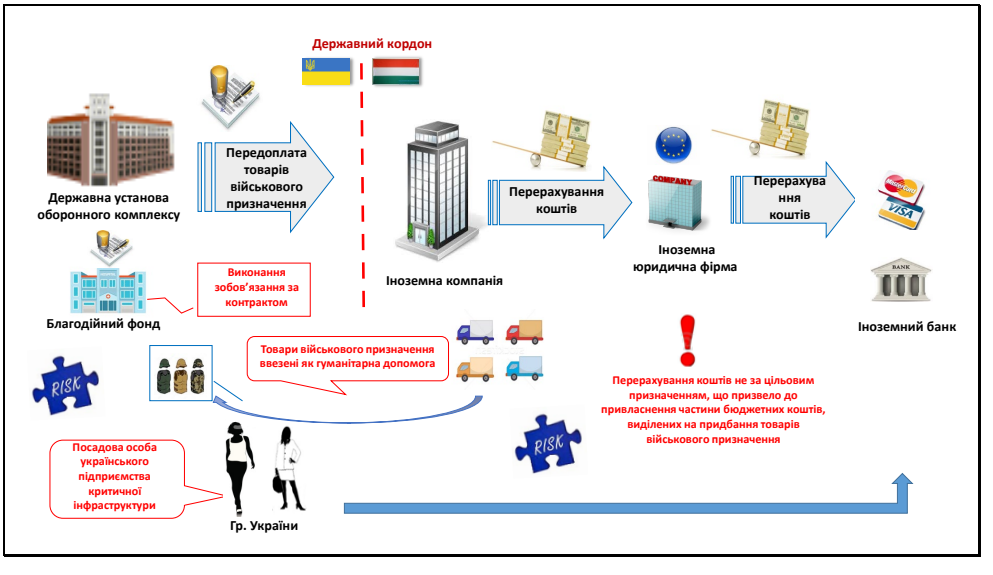
Держфінмоніторингом, з урахуванням інформації підрозділу фінансової розвідки іноземної країни, виявлено схему незаконного заволодіння бюджетними коштами шляхом шахрайських дій за участю **Компанії-нерезидента**.

Встановлено, що **Державною установою оборонного комплексу** було укладено декілька контрактів з **Компанією-нерезидентом** на постачання товарів військового призначення та на підставі них перераховано кошти як попередня оплата. В той же час, між **Державною установою оборонного комплексу** та **Благодійним фондом** укладено три контракти, предметом постачання яких є аналогічні товари військового призначення.

Привертає увагу, що зобов'язання за трьома контрактами були виконані на замовлення **Благодійного фонду**, а товари ввезені як гуманітарна допомога.

Частину отриманих коштів **Компанією-нерезидентом** було перераховано на рахунок **Іноземної юридичної фірми**, яка в свою чергу перерахувала їх на відкриті в іноземному банку рахунки **громадян України**, одна з яких є посадовою особою українського підприємства критичної інфраструктури.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.3.13. Розкрадання бюджетних коштів шляхом виведення їх за кордон з метою подальшої легалізації

Держфінмоніторингом, з урахуванням інформації правоохоронного органу, виявлено схему розкрадання бюджетних коштів шляхом виведення коштів за кордон з метою подальшої легалізації.

Встановлено, що **Підприємством А** для виконання державних контрактів з **Державною установою** оборонного комплексу було укладено низку контрактів з компаніями-нерезидентами предметом яких є постачання товарів спеціального призначення.

Привертає увагу, що ціна одиниці товару в контрактах значно завищена, порівняно з роздрібною вартістю в Україні.

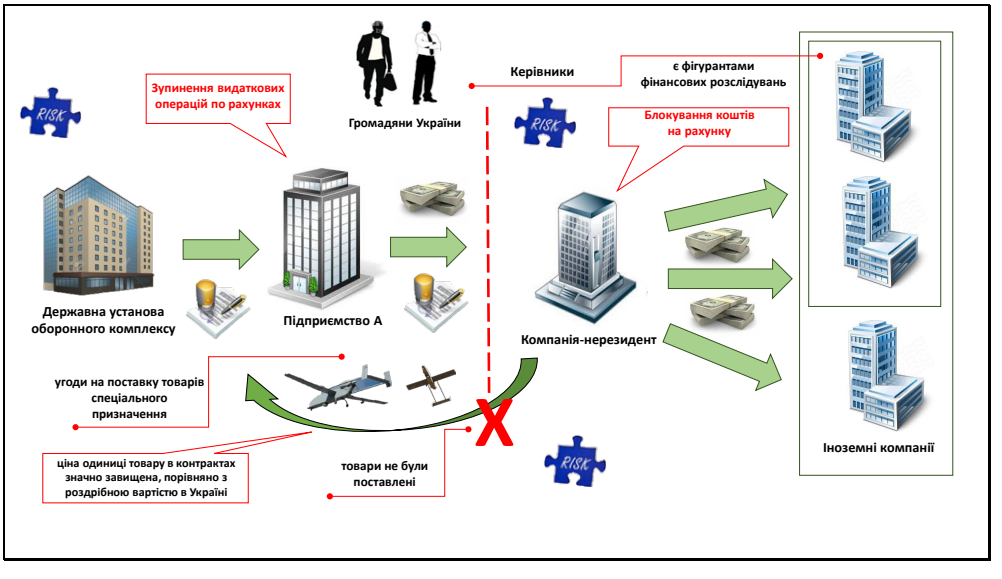
На підставі укладених контрактів **Підприємством А** на користь **Компанії-нерезидента** було перераховано кошти, які надалі перераховано на користь ряду іноземних компаній. Керівниками двох з цих **Іноземних компаній** є громадяни України, які фігурували у фінансових розслідуваннях щодо діяльності професійної мережі відмивання коштів.

Варто зазначити, що **Компанією-нерезидентом** зазначені товари в обумовленому обсязі не було поставлено та бюджетні кошти не було повернуто.

Таким чином, організовано схему розкрадання державних коштів шляхом виведення бюджетних коштів за кордон з метою подальшої легалізації.

Підрозділом фінансової розвідки іноземної країни заблоковано кошти, отримані від **Підприємства А** та які розміщено на рахунку **Компанії-нерезидента**. Крім того, Держфінмоніторингом було заблоковано здійснення видаткових операцій по рахунках **Підприємства А**.

Правоохоронним органом здійснюється досудове розслідування.



РОЗДІЛ 5.4. ВІДМИВАННЯ КОРУПЦІЙНИХ ДОХОДІВ

Корупція як соціальне явище є серйозною проблемою будь-якого суспільства та завжди перебуває в центрі уваги громадськості, а особливо в умовах війни.

Попри те, що актуальними залишаються корупційні злочини: розкрадання бюджетних коштів, зловживання владою та службовим становищем, хабарництво. Війна створила додаткові можливості для незаконного збагачення.

Російська агресія не завадила окремим чиновникам та посадовим особам скерувати свої зусилля не на порятунок держави, а на власне збагачення, наживати чималі статки та вести стиль життя, який не відповідає рівню їхніх офіційних доходів.

Як наслідок, корупційні злочини набули особливої актуальності та важливим викликом стає виявлення і руйнування схем відмивання незаконних доходів.

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

Приклад 5.4.1. Приховування джерел походження коштів, отриманих внаслідок корупційних діянь

Держфінмоніторингом, з урахуванням інформації правоохоронного органу, виявлено схему приховування джерел походження коштів, отриманих внаслідок корупційних діянь.

Встановлено, що **Посадова особа** державної установи в період дії воєнного стану через своїх родичів здійснила низку правочинів з купівлі коштовного рухомого та нерухомого майна, у тому числі на території іноземних країн.

Посадова особа державної установи при виконанні своїх службових обов'язків отримувала хабарі від великої кількості фізичних осіб та організувала схему легалізації незаконних доходів через своїх **Родичів**, які оформлені як фізичні особи-підприємці.

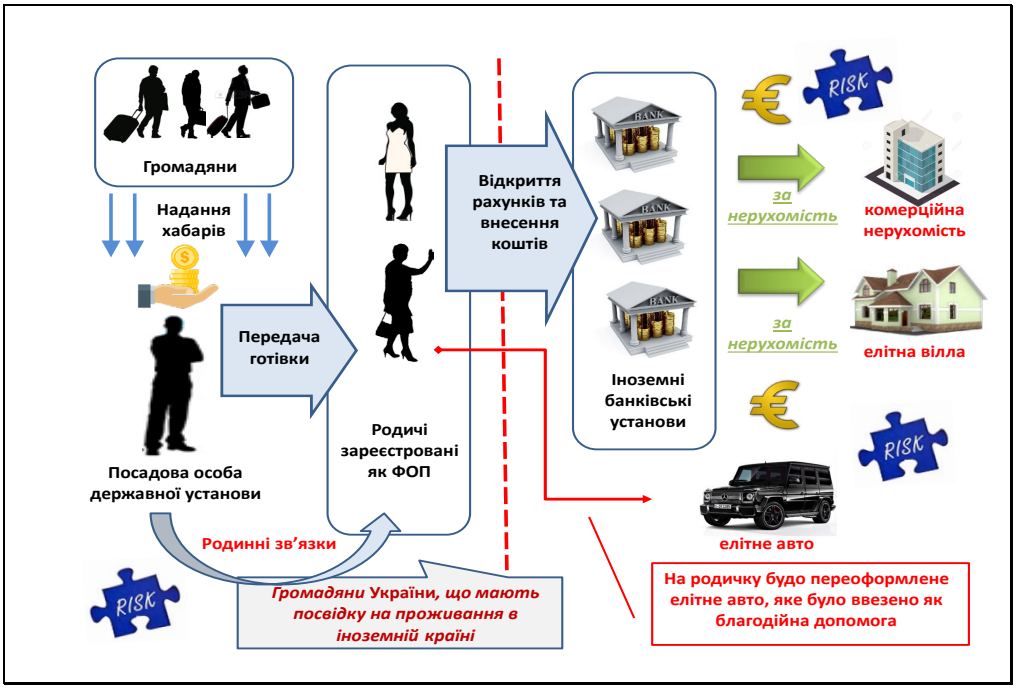
З метою приховування джерел походження коштів, **Родичі** подали податкову звітність фізичних осіб-підприємців із завищеними доходами у десятки разів.

Надалі, **Родичі** відкрили власні рахунки в іноземних банках різних країн, на які здійснили внесення готівкових коштів, за рахунок яких здійснили оплату за комерційну нерухомість та коштовну віллу.

Крім того, на одного з **Родичів** було переоформлено елітний автомобіль, який було ввезено на територію України як благодійна допомога від однієї з іноземних благодійних організацій.

Таким чином, виявлено схему, спрямовану на приховування джерел походження коштів, попередньо отриманих внаслідок вчинення протиправного діяння **Посадовою особою** державної установи.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.4.2. Легалізація (відмивання) доходів, одержаних корупційним шляхом

Держфінмоніторингом з урахуванням інформації правоохоронного органу, виявлено схему, яка була направлена на приховування джерел походження коштів, одержаних корупційним шляхом.

Посадова особа державної установи при виконанні своїх службових обов'язків отримувала хабарі від громадян України, та організувала схему легалізації незаконних доходів через своїх **Родичів** та **Пов'язаних осіб**, які оформлені як фізичні особи-підприємці.

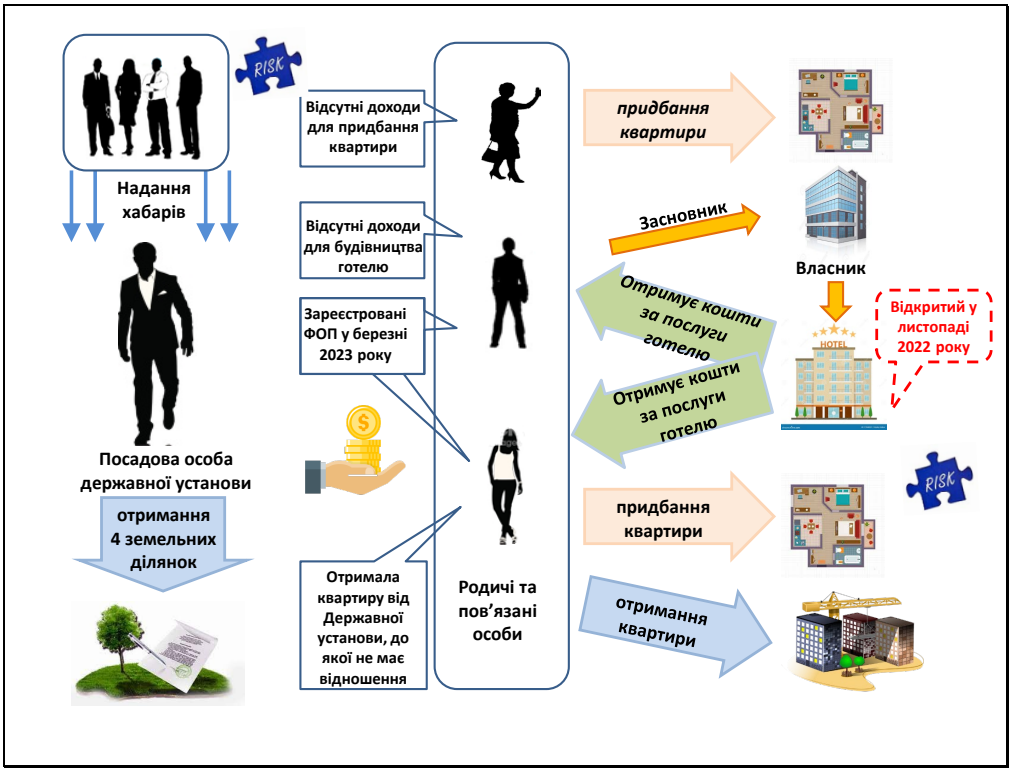
Відомо, що **Пов'язана особа** та **Дочка посадової особи** отримували кошти на рахунки фізичних осіб-підприємців у вигляді розрахунків за послуги, надані **Готелю преміумкласу**, який був відкритий у листопаді 2022 року. Встановлено, що **Пов'язана особа** володіє часткою Компанії, якій належить зазначений **Готель преміумкласу**, при відсутності відповідних доходів для будівництва.

Донька Посадової особи та **Пов'язана особа** зареєстровані як фізичні особи-підприємці навесні 2023 року.

Крім того, встановлено, що **Донька Посадової особи** придбала квартиру та отримала у власність ще одну квартиру від Державної установи, хоч і немає до неї ніякого відношення. Мати **Посадової особи** також, не маючи відповідних доходів, придбала ще одну квартиру. Сама **Посадова особа** отримала у власність 4 земельні ділянки.

Таким чином, дії здійснені **Посадовою особою**, членами родини та пов'язаними з ним особами мають ознаки незаконного збагачення, оскільки їх доходи та витрати не відповідають офіційно задекларованим доходам.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.4.3. Приховування джерел походження коштів, ймовірно отриманих від здійснення протиправної діяльності

Держфінмоніторингом, з урахуванням інформації підрозділу фінансової розвідки іноземної країни, виявлено приховування джерел походження коштів, ймовірно отриманих від здійснення протиправної діяльності колишнім народним депутатом України **Громадянином А**.

Встановлено, що на рахунки **Громадянина А**, відкриті за кордоном, надходять значні суми коштів як заробітна плата від **Компанії-нерезидента**, засновником якої є особа, пов'язана з **Громадянином А**.

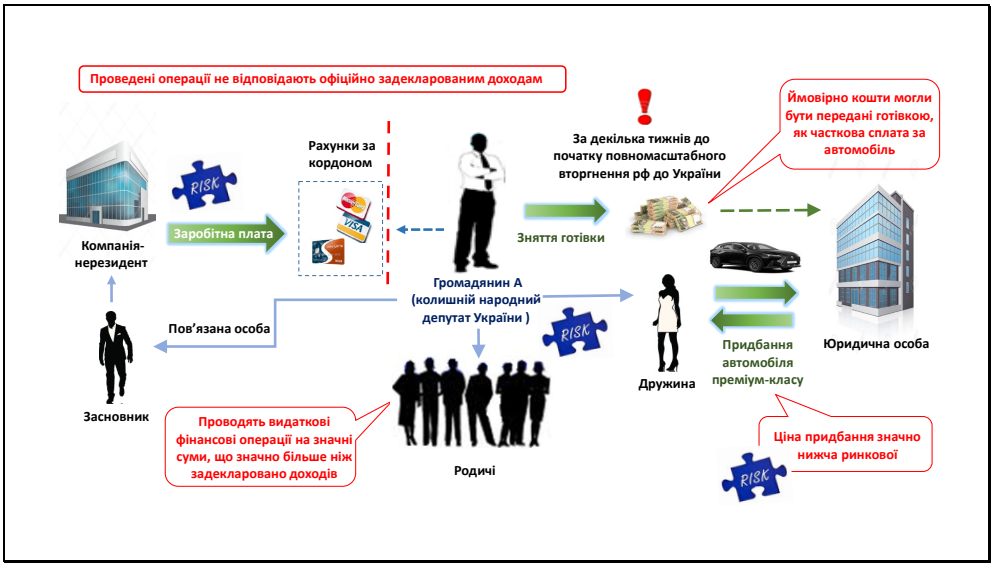
Крім того, встановлено, що **Громадянин А** за декілька тижнів до початку повномасштабного вторгнення росії до України зняв готівкові кошти з власного рахунку у значній сумі, при цьому не маючи достатніх задекларованих доходів для внесення коштів.

В той самий час його дружиною придбано автомобіль преміумкласу у **Юридичної особи** за ціною, значно нижчою ринкової. Існує ймовірність, що при оплаті за автомобіль частина коштів **Громадянином А** була передана **Юридичній Особі** готівкою.

Також, встановлено, що **Родичами Громадянина А** здійснюються видаткові фінансові операції на великі суми, значно більші, ніж офіційно задекларовані ними доходи.

Існують підозри, що проведені операції здійснені за рахунок приховуваних доходів **Громадянина А** та його **Родичів**, отриманих від здійснення протиправної діяльності.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.4.4. Використання номінальних власників

Держфінмоніторингом з урахуванням інформації, отриманої від правоохоронних органів, виявлено схему, пов'язану із внесенням готівки з невстановлених джерел особою, яка є пов'язаною з РЕР.

Встановлено, що **Громадянин А**, який є колишнім помічником екснародних депутатів України та екс-високопосадовців часів віктора януковича, протягом певного часу здійснював готівкові внески на власні рахунки у банківських установах в України на великі суми, які значно перевищують розмір офіційно задекларованих ним доходів.

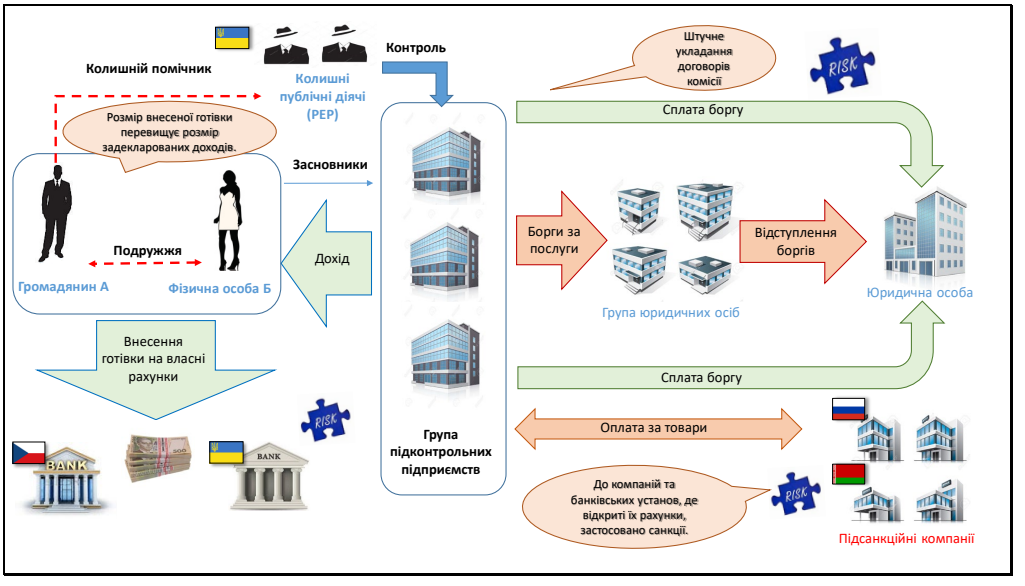
Крім того, за інформацією підрозділу фінансової розвідки іноземної країни **Фізична особа Б**, яка є дружиною **Громадянина А**, після початку повномасштабної агресії внесла значні суми готівкової валюти на власні рахунки в іноземній банківській установі та як джерело походження коштів зазначила дохід свого чоловіка.

Громадянин А та його дружина є номінальними власниками низки підприємств, хоча фактичний контроль за діяльністю цих підприємств здійснюється екснародними депутатами України.

Діяльність Групи підконтрольних вищезгаданим PEP підприємств пов'язана з ухиленням від сплати податків шляхом штучного збільшення своїх витрат внаслідок створення боргових зобов'язань за начебто отримані послуги та подальшою їх оплатою без економічного сенсу на користь сторонньої Юридичної особи на підставі договорів про відступлення прав вимоги. Крім того, встановлено, що одне з підконтрольних підприємств пов'язане зі сприянням в обході санкцій та намаганням продовжити співпрацю з підприємствами росії та білорусі.

Таким чином, є підстави вважати, що походження готівки **Громадянина А** пов'язане із незаконними доходами, отриманими від протиправної діяльності підконтрольних ексдепутатам підприємств.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.4.5. Приховування джерел походження коштів та майна

Держфінмоніторингом, з урахуванням інформації правоохоронного органу, виявлено схему приховування джерел походження коштів, отриманих внаслідок корупційних діянь.

Встановлено, що **Публічний діяч**, зловживаючи службовим становищем, через своїх родичів та водія здійснив придбання великої кількості коштовного рухомого та нерухомого майна, у тому числі на території іноземних країн.

При цьому офіційні доходи **Публічного діяча** та його близьких не могли дозволити такої кількості активів.

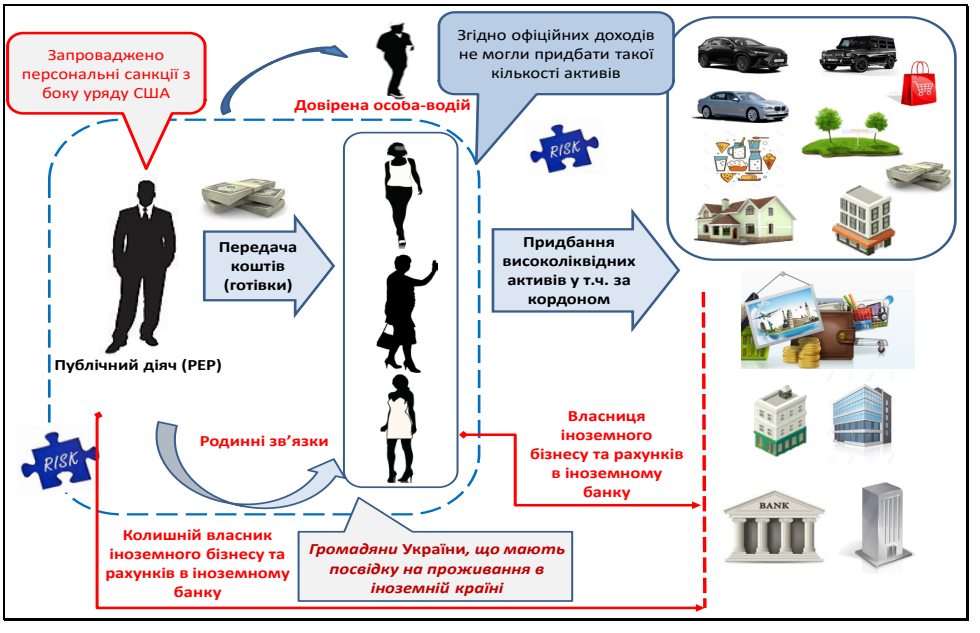
Для приховування джерел походження коштів, **Публічний діяч** реєстрував право власності на об'єкти рухомого та нерухомого майна на **Довірену особу-водія** та своїх **Родичів**. Дороговартісне його майно та родичів не зазначено у декларації **Публічного діяча** про майновий стан та доходи.

Також **Публічний діяч** володів бізнесом в іноземній країні та мав рахунки в іноземному банку. Пізніше бізнес було перереєстровано на родичку.

Слід зазначити, що до **Публічного діяча** запроваджено санкції з боку уряду США через протиправну діяльність на території іншої країни.

Таким чином, виявлено схему, спрямовану на приховування джерел походження коштів, закордонних рахунків, а також придбаного майна.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.4.6. Використання готівки для легалізації доходів, одержаних злочинним шляхом

Держфінмоніторингом, з врахуванням інформації, отриманої від правоохоронного органу, виявлено схему легалізації коштів отриманих з непідтверджених джерел.

Встановлено, що **Посадова особа Державної установи** та його **Цивільна дружина** здійснили вивезення готівкових коштів невідомого походження на територію іноземних держав, для подальшого внесення та перерахування на рахунки **Компанії-нерезидента**, як поповнення акціонерного капіталу та ведення господарської діяльності.

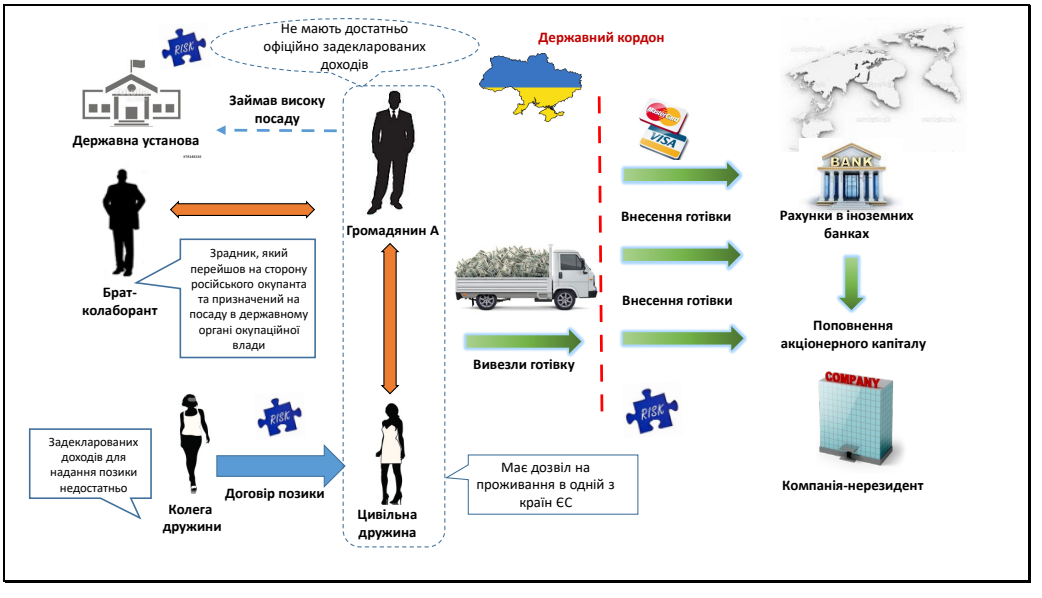
Посадова особа та його **Цивільна дружина** не мають достатньо офіційно задекларованих доходів.

Встановлено, що **Цивільною дружиною** отримано кошти як позику від **Колеги** у сумі, яка також не відповідає офіційно задекларованим доходам останньої.

Крім того, відомо, що рідний **Брат Посадової особи** – зрадник який перейшов на сторону російського окупанта та призначений на посаду в державному органі окупаційної влади.

Існують підозри, що кошти невідомого походження, які були вивезені за кордон, отримані внаслідок незаконної діяльності **Посадової особи** та його родичів.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.4.7. Приховування джерел походження коштів, ймовірно отриманих від здійснення протиправної діяльності

Держфінмоніторингом виявлено схему приховування джерел походження коштів, ймовірно отриманих від здійснення протиправної діяльності.

Встановлено, що на рахунки **Посадової особи** державної установи та його **Дружини**, відкриті в іноземних банківських установах вносяться готівкові кошти у значних розмірах. Надалі ці кошти використано як оплата за товари та послуги, перераховано на користь компаній, що здійснюють діяльність у галузі продажу нерухомості, частково знято готівкою за кордоном.

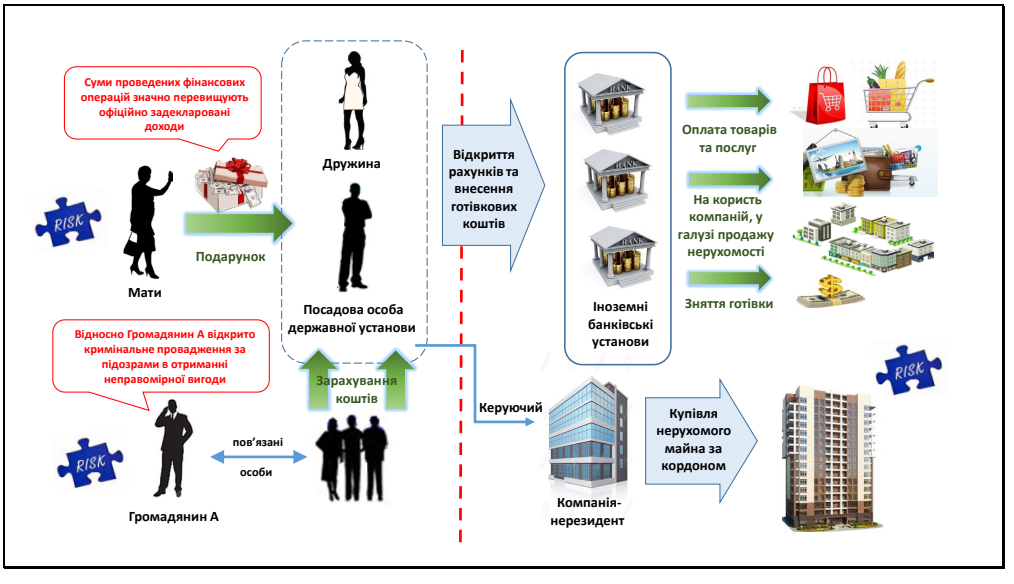
Джерелом походження значної кількості коштів **Посадовою особою** державної установи зазначено як подарунок від матері. При цьому відомо, що суми таких коштів значно більші від доходів, що були задекларовані ними.

Також відомо, що на рахунки **Посадової особи** зараховувались кошти від фізичних осіб, пов'язаних із **Громадянином А**, відносно якого відкрито кримінальне провадження за підозрами в отриманні неправомірної вигоди.

Також встановлено, що **Компанія-нерезидент**, де керуючим є **Посадова особа** державної установи, здійснила низку фінансових операцій, пов'язаних з купівлею нерухомого майна за кордоном.

Існують підозри, що проведені операції могли бути здійснені з метою приховування доходів **Посадової особи** державної установи та його родичів, отриманими від здійснення протиправної діяльності.

Правоохоронним органом здійснюється досудове розслідування.



РОЗДІЛ 5.5. ВИКОРИСТАННЯ НЕПРИБУТКОВИХ ОРГАНІЗАЦІЙ В НЕЗАКОННІЙ ДІЯЛЬНОСТІ ТА НЕЗАКОННЕ ЗАВОЛОДІННЯ ТА ПРИВЛАСНЕННЯ БЛАГОДІЙНОЇ ДОПОМОГИ

Використання неприбуткових організацій в незаконній діяльності є проблемою сьогодення. Це пов'язано з тим, що вони мають ряд переваг, які їх роблять привабливими для організованих злочинних груп. Зокрема, такі компанії мають легальний статус, що ускладнює їх ідентифікацію та розслідування. Крім того, вони мають доступ до значних фінансових ресурсів, які можуть бути використані для фінансування незаконної діяльності.

Одним із прикладів незаконної діяльності неприбуткових організацій є використання їх для фінансування терористичної діяльності росії. А саме використання для переказу грошових коштів та/або надання інших ресурсів терористичним організаціям або особам, що займаються дестабілізацією ситуації на території Україні.

Також, неприбуткові організації використовуються для відмивання коштів, отриманих від злочинної діяльності, шляхом перерахування їх як благодійні пожертви, в тому числі на підтримку армії.

Крім того, неприбуткові організації можуть використовуватися для обходу санкцій, наприклад, шляхом переказу грошей або товарів через країни, які не накладають санкції.

Іншими прикладами незаконної діяльності неприбуткових організацій є використання їх для пропаганди, шпигунства на користь росії тощо.

Слід зазначити, що після повномасштабного вторгнення, неприбуткові організації зіграли важливу роль у наданні гуманітарної допомоги та підтримки постраждалим в Україні від агресора. Однак, на жаль, незаконне заволодіння та привласнення благодійної та гуманітарної допомоги має місце під час війни.

Узагальнені типові приклади використання неприбуткових організацій в незаконній діяльності та незаконне заволодіння та привласнення благодійної допомоги, наведено нижче.

Приклад 5.5.1. Використання коштів злочинних організацій

Держфінмоніторингом з урахуванням інформації правоохоронного органу, виявлено схему, яка була направлена на приховування джерел походження коштів під прикриттям благодійної діяльності.

На рахунок **Релігійної установи** надходили кошти у вигляді благодійної допомоги від осіб які можуть бути причетними до діяльності, спрямованої на дестабілізацію суспільно-політичної обстановки в Україні та завдання шкоди національній безпеці України.

Надалі зазначені кошти перераховано під виглядом оплати за товари/роботи/послуги різним фізичним особам-підприємцям та переведено у готівку.

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

Привертає увагу, серед «благодійників» є підприємства які прямо або опосередковано пов'язані з **Проросійськими пропагандистами** та **Підсанкційними особами** та **Членом сім'ї РЕР, що знаходиться у розшуку**.

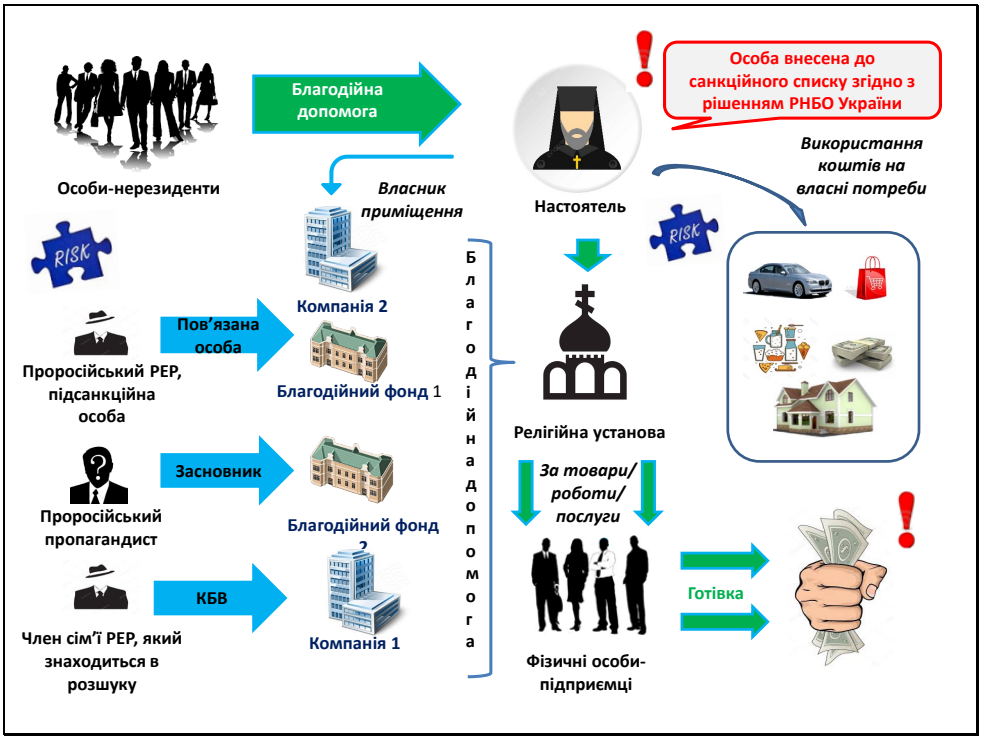
Відомо, що **Настоятель церкви** є власником приміщення одного з підприємств «благодійників».

Крім того, **Настоятель церкви** отримував благодійну допомогу від **Осіб-нерезидентів** як представник церкви та частину цих коштів використовував на власні потреби, у тому числі за кордоном.

Також, встановлено, що **Настоятель церкви** напередодні повномасштабного вторгнення відвідував та розраховувався за товари на території російської федерації.

До **Настоятеля церкви** застосовано обмежувальні заходи (санкції) згідно з Указом Президента України Про рішення РНБО «Про внесення змін до персональних даних спеціальних економічних та інших обмежувальних заходів (санкцій)».

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.5.2. Розкрадання бюджетних коштів, виділених на надання гуманітарної допомоги

Держфінмоніторингом з урахуванням інформації правоохоронного органу, виявлено схему, пов'язану із розкраданням бюджетних коштів, виділених на надання гуманітарної допомоги.

Встановлено, що кошти, виділені **Державним органом** на надання гуманітарної допомоги цивільному населенню в умовах воєнного стану в України, було перераховано на користь ряду **Громадських** та **Благодійних організацій**.

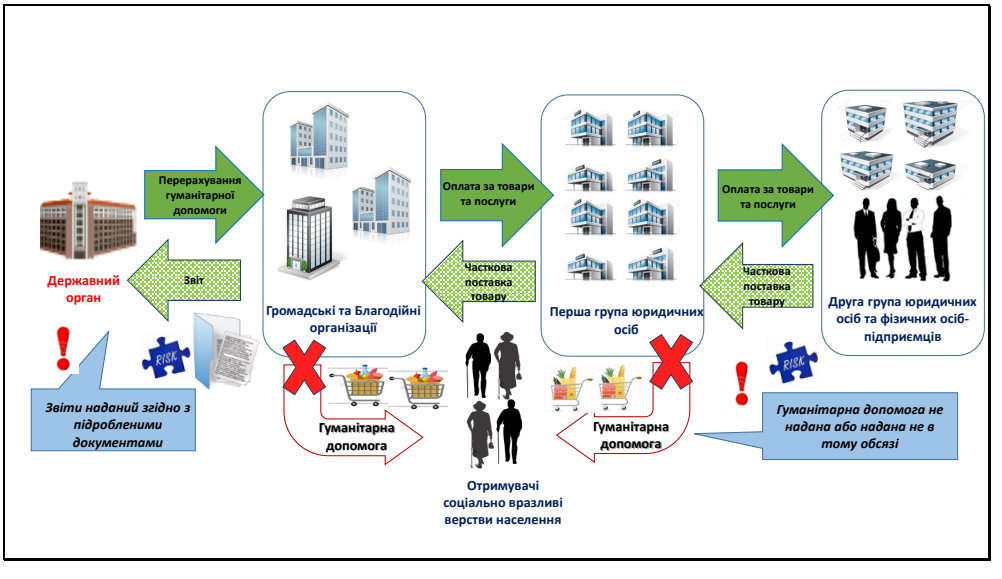
Надалі, бюджетні кошти у повному обсязі перераховано на **Першу групу юридичних осіб**, як оплата за товари та послуги. Отримані кошти, у свою чергу, перераховано на користь **Другої групи юридичних** та **Фізичних осіб-підприємців**, у тому числі з сумнівною репутацією.

При цьому, частково товари та послуги було надано кінцевим отримувачам як гуманітарну допомогу, частково гуманітарну допомогу було не надано зовсім або надано не в тому обсязі, в якому домовлялися з її отримувачами.

Громадськими та **Благодійними організаціями Державному органу** було надано Звіти про використання коштів для надання гуманітарної та іншої допомоги, сформовані на основі підроблених документів.

Таким чином, виявлено схему привласнення бюджетних коштів гуманітарного спрямування за участю неприбуткових організацій.

Правоохоронними органами здійснюється досудове розслідування.



Приклад 5.5.3. Шахрайська схема заволодіння коштами громадян, залученими через соціальні мережі

Держфінмоніторингом з урахуванням інформації правоохоронного органу, виявлено схему, яка була направлена на привласнення благодійних внесків з використанням підконтрольних благодійних організацій.

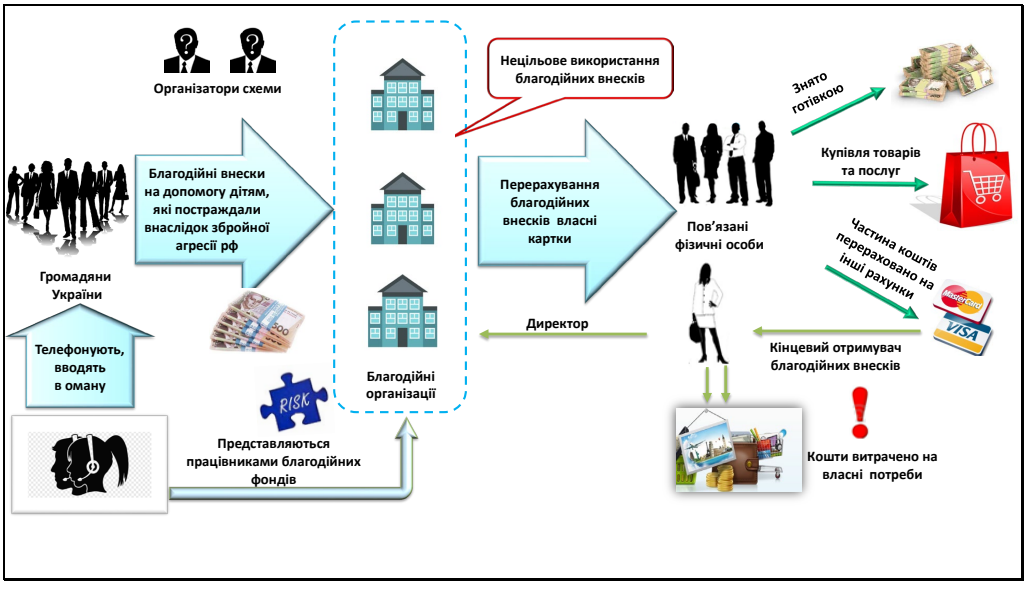
З початку повномасштабної військової агресії росії групою осіб організована діяльність «колл-центрів», головною задачею яких було телефонувати та відправляти повідомлення через соціальні мережі різним фізичним особам від імені **Благодійних фондів**, з проханням перерахувати кошти на рахунки зазначених організацій.

Встановлено, що на рахунки трьох **Благодійних фондів** від **Громадян України** було зараховано кошти на значні суми у вигляді благодійних внесків громадян для надання допомоги дітям, які постраждали внаслідок збройної агресії.

Надалі, отримані благодійні кошти було направлено на рахунки ряду **Пов'язаних фізичних осіб**, за нібито поставлені товари/послуги. Далі кошти, які було зараховано на картки вищезазначених **Пов'язаних фізичних осіб**, було знято готівкою, спрямовано на купівлю товарів/послуг та інші перекази. Частину коштів було перераховано на платіжку картку **Керівника** однієї з **Благодійних організацій**, які було витрачено на особисті потреби.

Таким чином, групою фізичних осіб було реалізовано шахрайську схему заволодіння коштами громадян шляхом переведення на власні платіжні картки.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.5.4. Привласнення благодійної допомоги з використанням компаній-оболонок

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

Держфінмоніторингом, з урахуванням інформації підрозділу фінансової розвідки іноземної країни, виявлено схему ймовірного привласнення коштів, одержаних як благодійна допомога, з подальшою їх легалізацією.

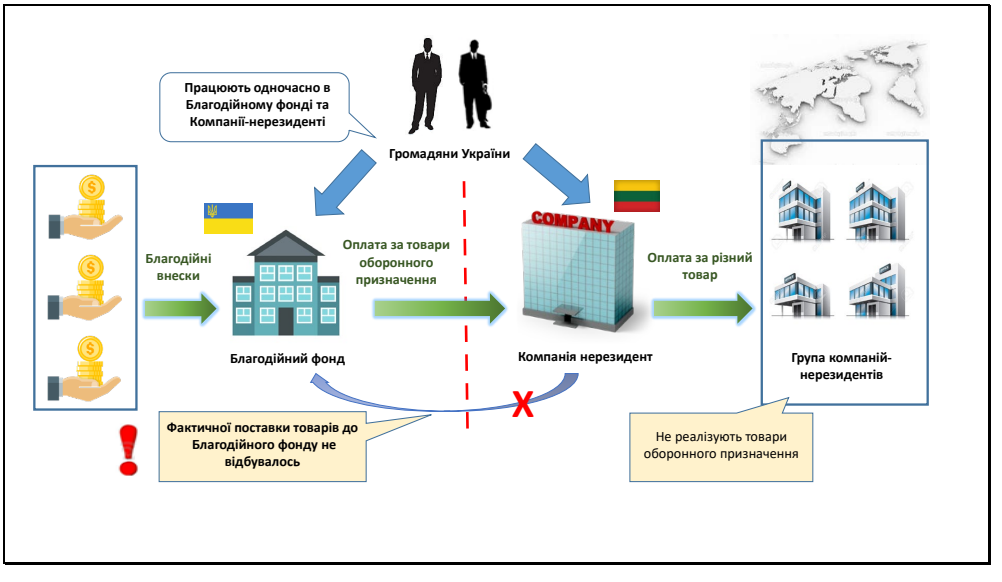
Встановлено, що після початку повномасштабної агресії росії на користь **Компанії-нерезидента** було перераховано кошти за продукцію оборонного призначення від українського **Благодійного фонду**, одержані як благодійна допомога. При цьому у **Компанії-нерезидента** відсутні будь-які контракти чи транспортні документи, які б підтверджували відвантаження/розвантаження даного виду товару. Продукція оборонного призначення, за яку **Благодійний фонд** перерахував кошти, на територію України не постачалась.

Також встановлено, що надалі **Компанією-нерезидентом** отримані кошти перераховано **Групі компаній-нерезидентів**, як оплату за товар, що не пов'язаний з продукцією оборонного призначення.

Привертає увагу, що **Благодійний фонд** та **Компанія-нерезидент** мають зв'язок через двох громадян України, які працюють одночасно у двох зазначених компаніях.

Є підстави вважати, що **Компанія-нерезидент** використовується з метою легалізації доходів, одержаних злочинним шляхом.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.5.5. Шахрайська схема незаконного привласнення за участю організованої злочинної групи

Держфінмоніторингом, з урахуванням інформації правоохоронного органу, виявлено організовану злочинну групу, діяльність якої спрямована на незаконне заволодіння та привласнення благодійної допомоги.

Встановлено, що **Члени злочинної групи** організували збір коштів на власні рахунки під виглядом благодійної допомоги, у тому числі для потреб ЗСУ.

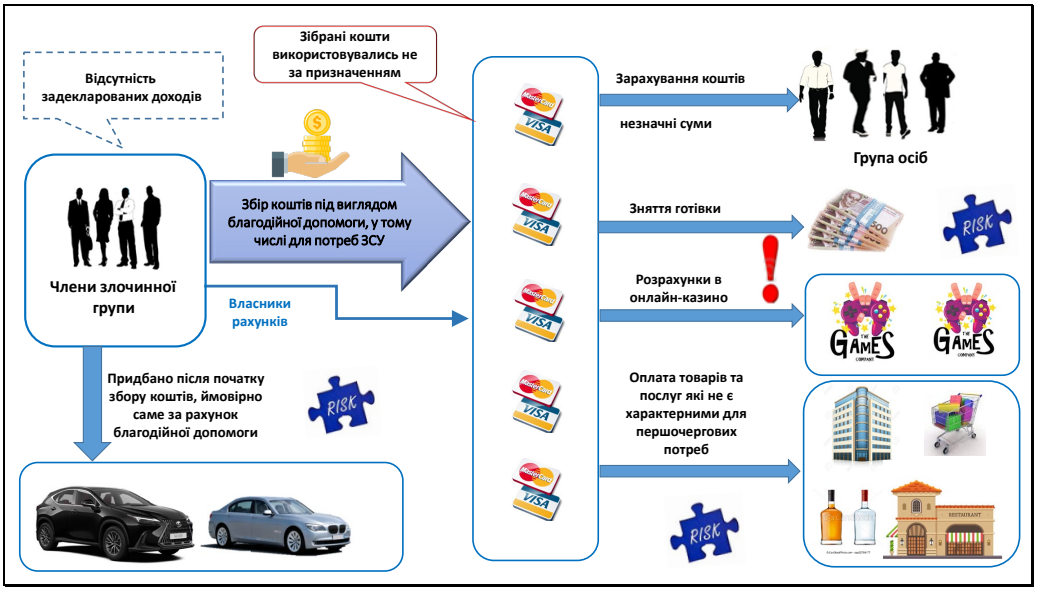
Зібрані кошти використовувались не за призначенням, а для забезпечення власних потреб, а саме:

- перераховувались незначними сумами на користь **Групи осіб**;
- обготівковувались;
- спрямовувались для розрахунків в онлайн-казино;
- перераховувались як оплата товарів та послуг, які не є характерними для першочергових потреб (оплата розважальних сервісів, готелів, ресторанів, придбання алкогольних напоїв та інше).

Крім того, встановлено, що у період після початку збору коштів **Члени злочинної групи** придбали автомобілі преміумкласу.

Враховуючи відсутність у **Членів злочинної групи** задекларованих доходів, ймовірно, що транспортні засоби придбавались саме за рахунок благодійної допомоги.

Правоохоронним органом здійснюється досудове розслідування.



РОЗДІЛ 5.6. ТРАНСКОРДОННЕ ВІДМИВАННЯ ДОХОДІВ

Повномасштабна збройна агресія російської федерації проти України та введений воєнний стан призвели до виникнення труднощів та проблем в усіх сферах національної економіки, а особливо у сфері зовнішньоекономічної діяльності країни. Найважливішою перешкодою для експорту та імпорту товарів стало обмеження логістичних напрямів торгівлі. На півночі та сході були перекриті шляхи до білорусі та росії, на півдні були заблоковані українські морські порти, тож західний напрямок став єдиним для зовнішньої торгівлі, але при цьому мав обмежену пропускну спроможність через перенавантаження.

Завдяки ініціативі про створення «зернового коридору», яка була реалізована влітку 2022 року була вирішена одна із логістичних проблем для українського експорту, що дало змогу зберегти статус України на світових ринках як великого постачальника агропродукції, а також зменшити обвал економіки, адже постачання за межі України зернових є одним з основних джерел експортного валютного виторгу.

Разом з цим, дуже гостро постає питання боротьби з тіньовим експортом агропродукції з України, наслідком чого є неповернення валютної виручки в Україну. Відповідно до оцінок НБУ, у 2022-2023 роках (до 20 вересня) обсяг валютної виручки від агроекспортерів, яка не надійшла у встановлені законом строки, становить близько 2 млрд дол (еквівалент 80 млрд грн). Сумарний обсяг грошей, які експортери не завели в Україну, НБУ оцінив 8 млрд доларів.

Крім того, проблемою залишається виведення валютних коштів за межі України без фактичного постачання товарів та зовнішньоекономічні операції з компаніями-нерезидентами, контроль за діяльністю яких опосередковано здійснюється представниками країни-агресора.

Узагальнені типові приклади відмивання доходів в зовнішньоекономічній сфері наведено нижче.

Приклад 5.6.1. Відмивання коштів з використанням рахунків компанії-оболонки

Держфінмоніторингом, з урахуванням інформації підрозділу фінансової розвідки іноземної країни, виявлено схему щодо ймовірного відмивання державних коштів з використанням рахунків компанії-нерезидента.

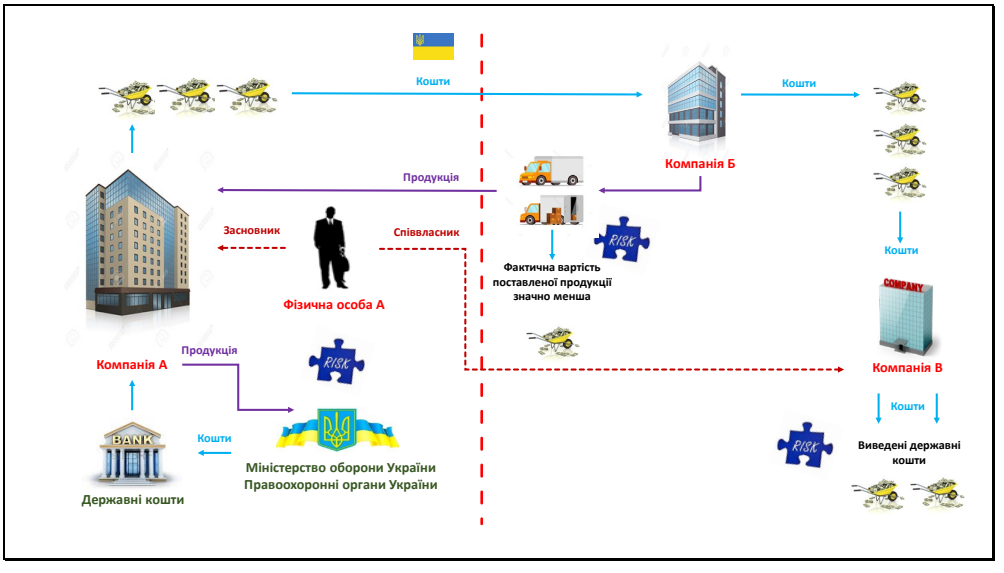
Встановлено, що українське підприємство – **Компанія А** протягом декількох років перераховувало кошти на користь **Компанії-нерезидента** як передоплата за тепловізійне та оптичне обладнання. Відомо, що серед замовників вказаної продукції були, у тому числі правоохоронні органи України.

Також встановлено, що протягом того ж часу на територію України від **Компанії-нерезидента** було ввезено певну кількість зазначеної продукції. Проте, загальна сума фактично імпортованого обладнання становила в декілька разів менше від суми коштів, перерахованих на користь **Компанії-нерезидента**.

Також, встановлено, що частину отриманих коштів **Компанія-нерезидент** надалі перераховувала на користь іншої **Компанії-нерезидента**, яка не має відповідних ресурсів (працівників, приміщення та обладнання) для виготовлення складно-технічних виробів. Співвласником **Компанії В** та засновником **Компанії А** є одна особа - **Фізична особа А**.

Таким чином, здійснені фінансові операції можуть бути пов'язаними із протиправним виведенням державних коштів за кордон України з подальшою легалізацією.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.6.2. Схема незаконного експорту продукції за підробленими документами

Держфінмоніторингом з урахуванням інформації підрозділу фінансової розвідки іноземної країни, виявлено схему незаконного експорту продукції без зарахування валютної виручки.

Встановлено, що українське підприємство – **Компанія А** експортувало сільськогосподарську продукцію на користь компанії-нерезидента **Компанії Б**. Однак, грошові кошти за експортовану продукцію на користь **Компанії А** сплачено не було.

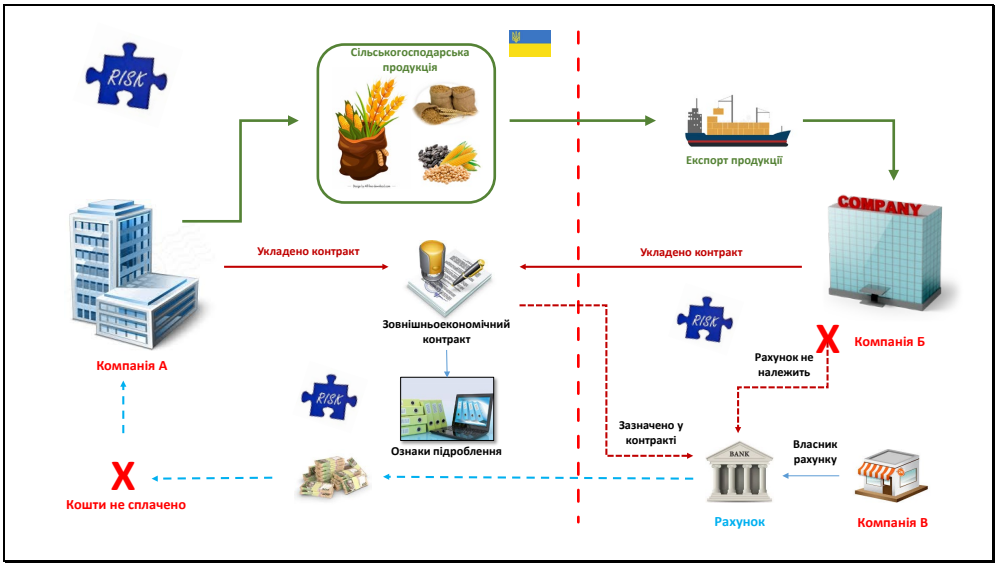
Укладений контракт між **Компанією А** та **Компанією Б** мав ознаки підроблення (печатки та підписи накладались з використанням комп'ютерної техніки).

За інформацією підрозділу фінансової розвідки іноземної країни встановлено, що рахунки **Компанії Б**, зазначені у зовнішньоекономічному контракті, фактично належать іншій компанії-нерезиденту **Компанії В**, яка

працює у сфері надання рекламних послуг і не здійснює експортно-імпортних операцій.

Компанією Б надалі реалізовано сільськогосподарську продукцію на користь реальних зернотрейдерів, а отримані кошти використано для розрахунків за межами України.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.6.3. Схема шахрайства з коштами компанії-нерезидента

Держфінмоніторингом, з урахуванням інформації правоохоронного органу, виявлено схему незаконного заволодіння коштами компанії-нерезидента шахрайським шляхом з метою подальшої легалізації.

Встановлено, що українським **Підприємством А** було укладено зовнішньоекономічний контракт з **Компанією-нерезидентом** на постачання на його користь технологічного обладнання на велику суму. **Компанією-нерезидентом** було здійснено попередню оплату згідно з умовами контракту, проте постачання обладнання на її користь не відбулось.

Натомість отримані кошти посадовими особами **Підприємства А** було використано на власний розсуд, зокрема, на купівлю для себе та своїх родичів коштовної елітної нерухомості, на поточні витрати підприємства, на заробітну плату та фінансову допомогу тощо.

Таким чином, посадовими особами **Підприємства А** здійснено шахрайське заволодіння коштами **Компанії-нерезидента** та легалізовано шляхом придбання нерухомості.

Правоохоронним органом здійснюється досудове розслідування.

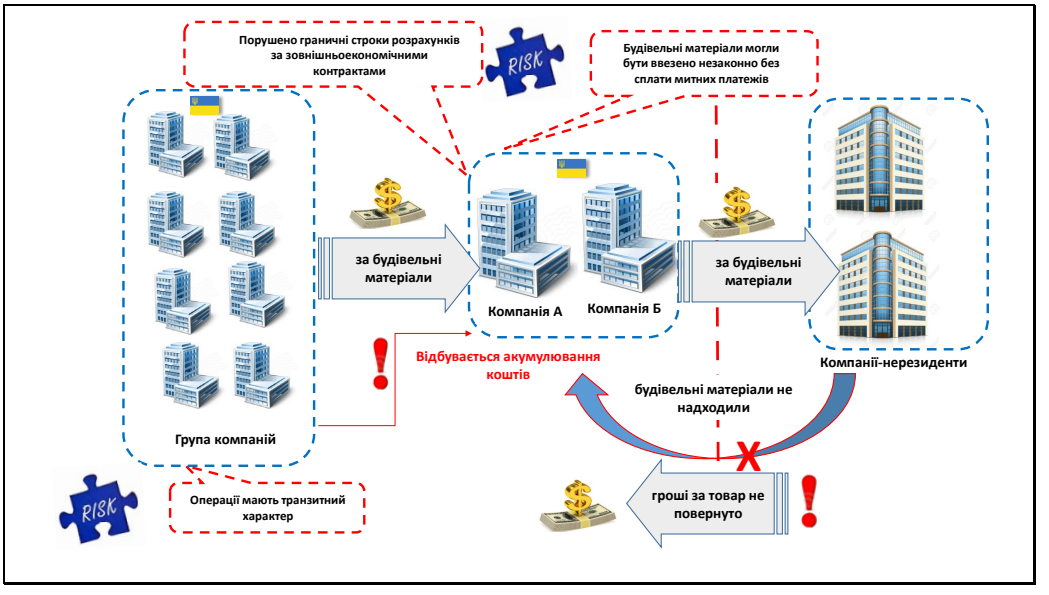
Приклад 5.6.4. Схема виведення коштів за кордон із використанням безтоварних операцій

Держфінмоніторингом, виявлено схему щодо ймовірного відмивання коштів **Групою компаній** з використанням рахунків компанії-нерезидента шляхом здійснення безтоварних операцій.

Групою компаній з ознаками фіктивності протягом певного періоду часу здійснювалися транзитні фінансові операції, які на кінцевому етапі акумулювались на рахунках **Компанії А та Компанії Б** як оплата за будівельні матеріали.

Надалі, закумульовані кошти на рахунках **Компанії А та Компанії Б** перераховано на користь двох **Компанії-нерезидентів** як оплата за будівельні матеріали, але товар на митну територію України не постачався, гроші **Компаніями-нерезидентами** повернуто не було. Не виключено, що товар міг бути ввезений незаконно, без сплати обов'язкових платежів.

Правоохоронним органом здійснюється досудове розслідування.



РОЗДІЛ 5.7. ВИКОРИСТАННЯ ГОТІВКОВИХ КОШТІВ В СХЕМАХ ВІДМИВАННЯ ДОХОДІВ

Доходи від незареєстрованої, забороненої, злочинної діяльності 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.

В умовах відкритої збройної агресії з боку росії готівкові кошти можуть використовуватись для фінансування терористичних актів, диверсійних заходів, колабораційної 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.

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.

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

Приклад 5.7.1. Легалізація злочинних доходів, отриманих від незаконної діяльності

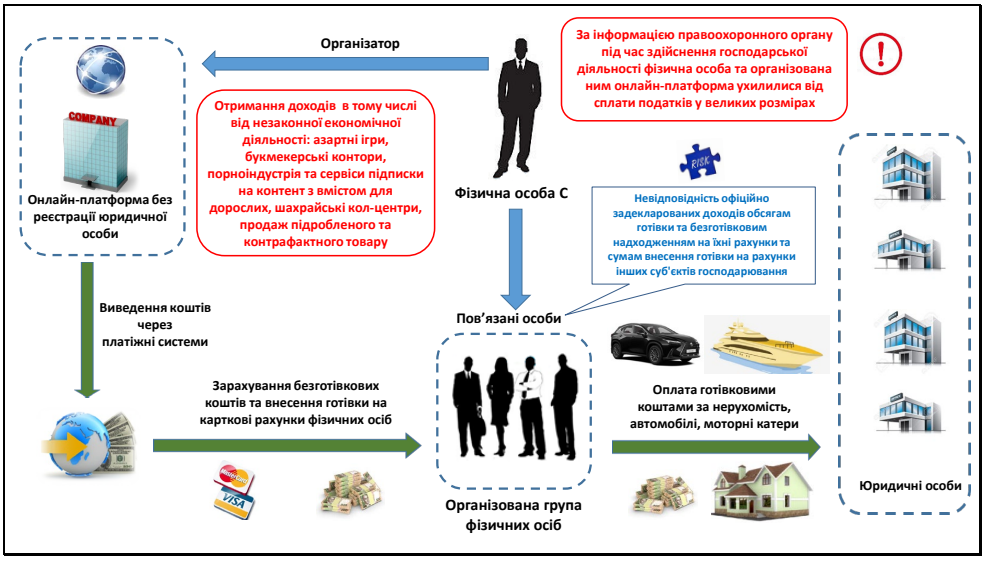
Держфінмоніторингом, з врахуванням інформації отриманої від правоохоронного органу, виявлено схему легалізації злочинних доходів, отриманих від здійснення прихованої (незареєстрованої) господарської діяльності.

Фізичною особою С організовано роботу **Онлайн-платформи**, яка здійснювала господарську діяльність без юридичного оформлення та реєстрації юридичної особи. Діяльність **Онлайн-платформи** передбачала в тому числі залучення клієнтів-юзерів до незаконної економічної діяльності, а саме: азартні ігри, букмекерські контори, порноіндустрія, сервіси підписки на контент з вмістом для дорослих, шахрайські кол-центри, продаж підробленого та контрафактного товару.

Доходи одержані від незаконної діяльності **Онлайн-платформи** виводились через платіжні системи на користь підконтрольної **Групи фізичних осіб**. Зазначені особи у свою чергу здійснювали поповнення рахунків готівковими коштами, а також придбання за готівку рухомого та нерухомого майна, як в Україні, так і за кордоном, що не відповідає обсягу задекларованим ними доходів.

За інформацією правоохоронного органу під час здійснення господарської діяльності **Фізична особа С** та організована ним **Онлайн-платформа** ухилилися від сплати податків у великих розмірах.

Правоохоронним органом здійснюється досудове розслідування.



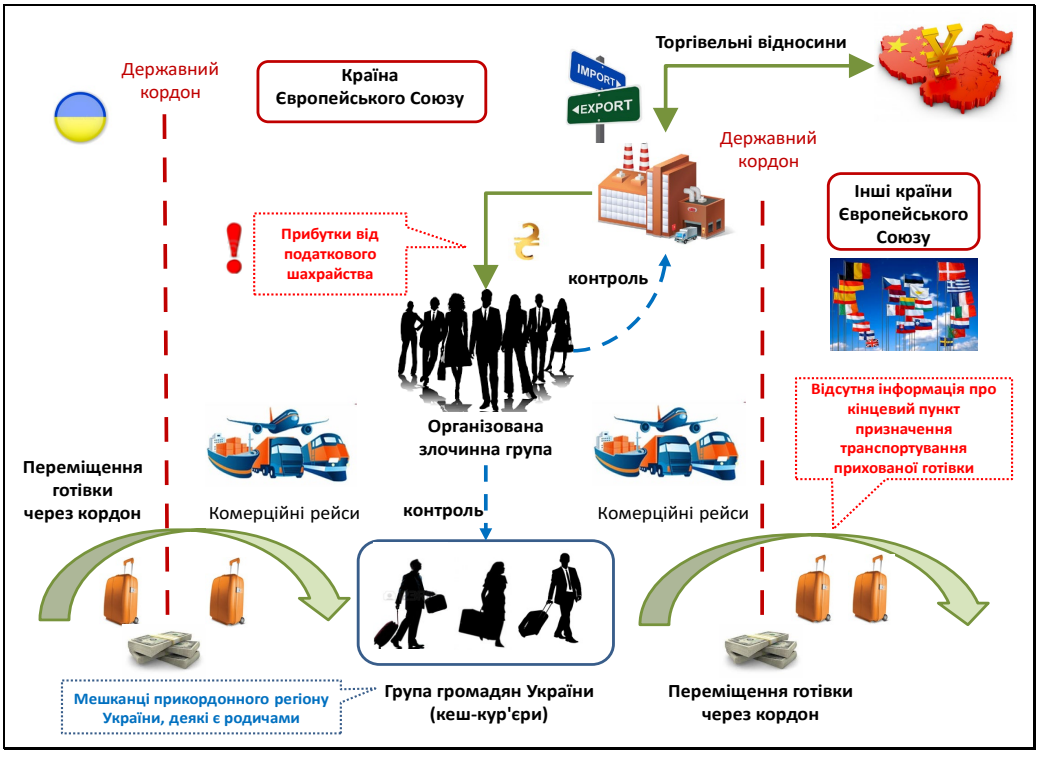
Приклад 5.7.2. Залучення громадян України до перевезення готівкових коштів, отриманих від податкового шахрайства (кеш-кур'єри)

Держфінмоніторингом, з врахуванням інформації ПФР іноземної країни, виявлено **Групу громадян України**, які виступали кеш-кур'єрами для міжнародної злочинної організації, яка отримує значні прибутки від податкового шахрайства.

Організація використовує розгалужену мережу кур'єрів, переважно громадян України, які комерційними рейсами перевозять готівку, заховану в їх зареєстрованому багажі. Ці особи подорожують групами до п'яти осіб і пов'язані між собою тим, що подорожували разом, також через можливі родинні зв'язки між деякими з них. Виявлено, що всі особи, які залучені в процес злочинної схеми як кеш-кур'єри, проживають в одному прикордонному регіоні України.

Діяльність зазначеної групи кеш-кур'єрів виявлена на території однієї з країн Європейського Союзу. При цьому, надалі готівка вивозилась за межі країни та інформація про кінцевий пункт призначення транспортування прихованої готівки відсутня.

Правоохоронним органом здійснюється досудове розслідування.



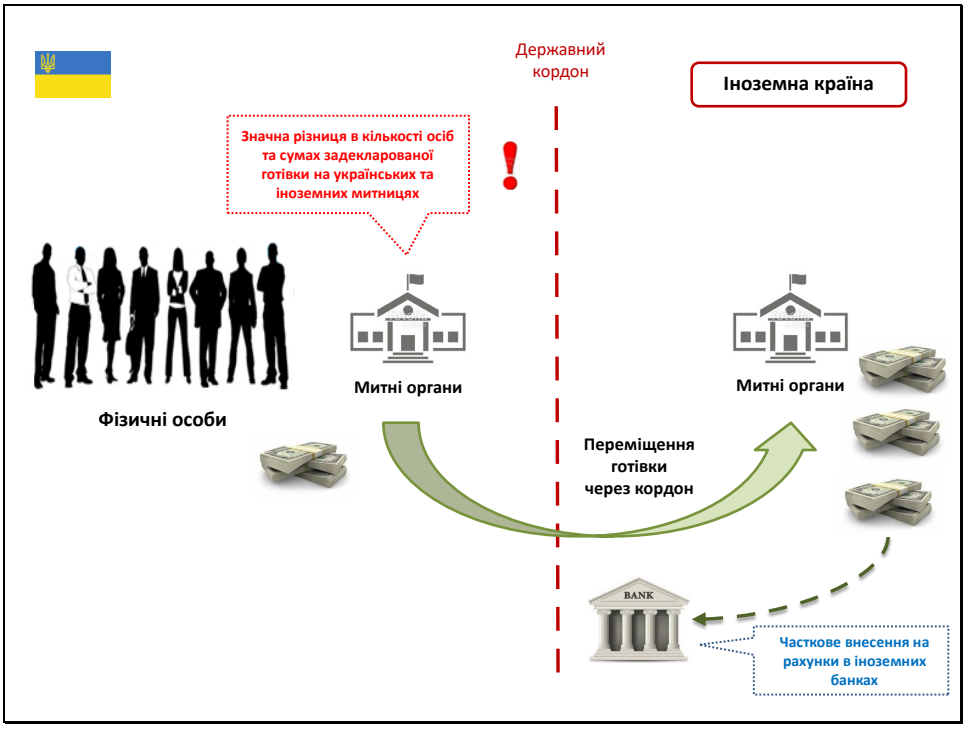
Приклад 5.7.3. Переміщення готівкових коштів за межі України без письмового декларування

Держфінмоніторингом виявлено схему переміщення готівкових коштів за межі України без письмового декларування.

Так, Держфінмоніторингом за результатами порівняння інформації, отриманої від ПФР іноземної країни про переміщення готівкових коштів фізичними особами з території України, а також інформації отриманої від митниць, виявлено значну різницю в кількості осіб та сумах коштів, які підлягали декларуванню. Встановлено, що кількість осіб, яка зафіксована на українських митницях та суми коштів, які особи декларували, в рази менші від зафіксованих на іноземних митницях.

Надалі частина готівкових коштів вносилась на рахунки в іноземних банках.

Правоохоронним органом здійснюється досудове розслідування.



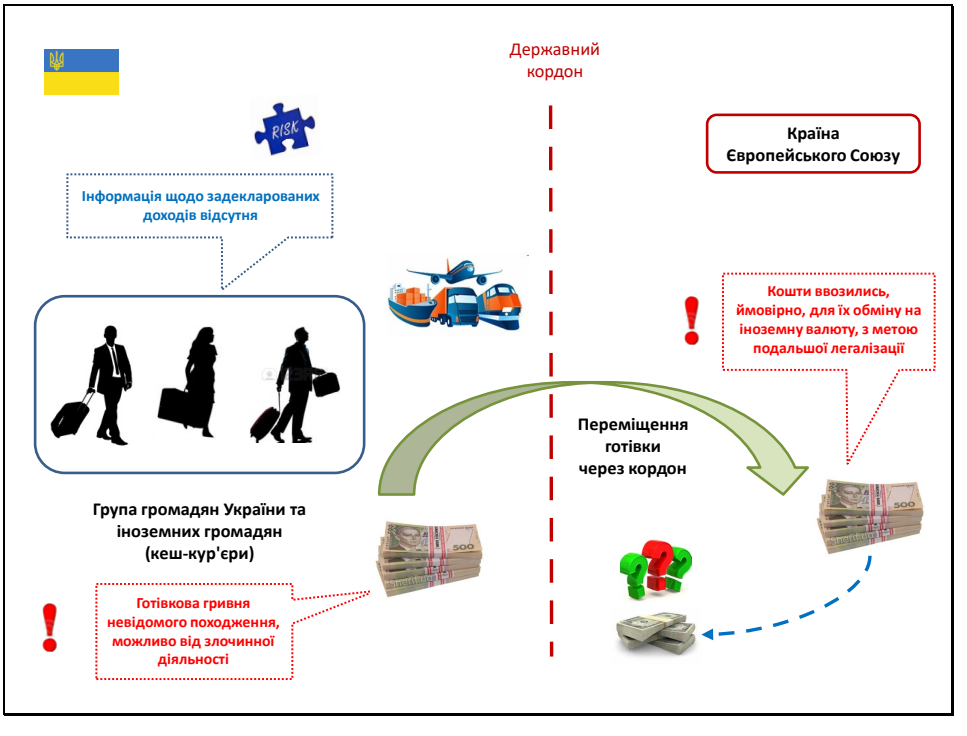
Приклад 5.7.4. Залучення громадян України до перевезення готівкових коштів невідомого походження (кеш-кур'єри)

Держфінмоніторингом, з врахуванням інформації ПФР іноземної країни, виявлено **Групу громадян України** та **іноземних громадян**, які виступали кеш-кур'єрами для перевезення готівкових коштів невідомого походження.

Встановлено, що **Група громадян України** та **іноземних громадян** здійснювали ввезення на територію однієї з країн Європейського Союзу готівкової гривні в значних сумах. Кошти, ймовірно, походять від злочинної діяльності та переміщуються через кордон для обміну на іноземну валюту з метою їх подальшої легалізації.

Інформація щодо доходів, задекларованих учасниками групи, у Держфінмоніторингу відсутня.

Правоохоронним органом здійснюється досудове розслідування.



РОЗДІЛ 5.8. ВІДМИВАННЯ ДОХОДІВ ВІД НЕЗАКОННОГО ЗАВОЛОДІННЯ КУЛЬТУРНИМИ ЦІННОСТЯМИ

Проблема незаконної торгівлі культурними цінностями має загальносвітове значення охоплює розгалужену мережу посередників, консультантів, зберігачів, підставних компаній і неприбуткових організацій, проведення фіктивних продажів та аукціонів для приховування особи справжніх учасників операцій з культурними цінностями.

Поширене також використання офшорних зон, як місць проведення відповідних операцій, із залученням підставних компаній і трастів, що може супроводжуватись ухиленням від сплати податків. Крім того, на нелегальному ринку культурних цінностей досить широко використовують розрахунки готівкою.

Серед предикатних злочинів, які генерують доходи з використанням культурних цінностей слід виділити: підроблення, шахрайство, крадіжки, пограбування тощо.

В Україні діяльність представників кремлівського режиму на тимчасово окупованих територіях спричинила безпрецедентну хвилю злочинів проти культурної спадщини. Мали місце масові викрадення об'єктів культурної спадщини. Відповідні діяння розглядаються як воєнні злочини. Паралельно на тимчасово окупованих територіях активізувалась «чорна археологія». Все це активізує нелегальний ринок культурних цінностей як в Україні, так і за кордоном.

Частина незаконних переміщень культурних цінностей з окупованих територій відбувається під виглядом між музейної передачі експонатів та маскується під їх «порятунок» з широким використанням засобів масової інформації (дезінформації). Існує високий ризик потрапляння цінних українських експонатів з російських музеїв на нелегальні ринки.

Відомо, що чимало представників кремлівського режиму, що належать до так званих «олігархів», на яких накладені санкції Україною та країнами партнерами володіють значними колекціями культурних цінностей, частина з яких має сумнівне походження.

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

Приклад 5.8.1. Схема незаконного заволодіння та переміщення за межі України з метою подальшої реалізації викрадених об'єктів матеріальної культури

Держфінмоніторингом, з врахуванням інформації отриманої від правоохоронного органу та іноземного ПФР, 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.

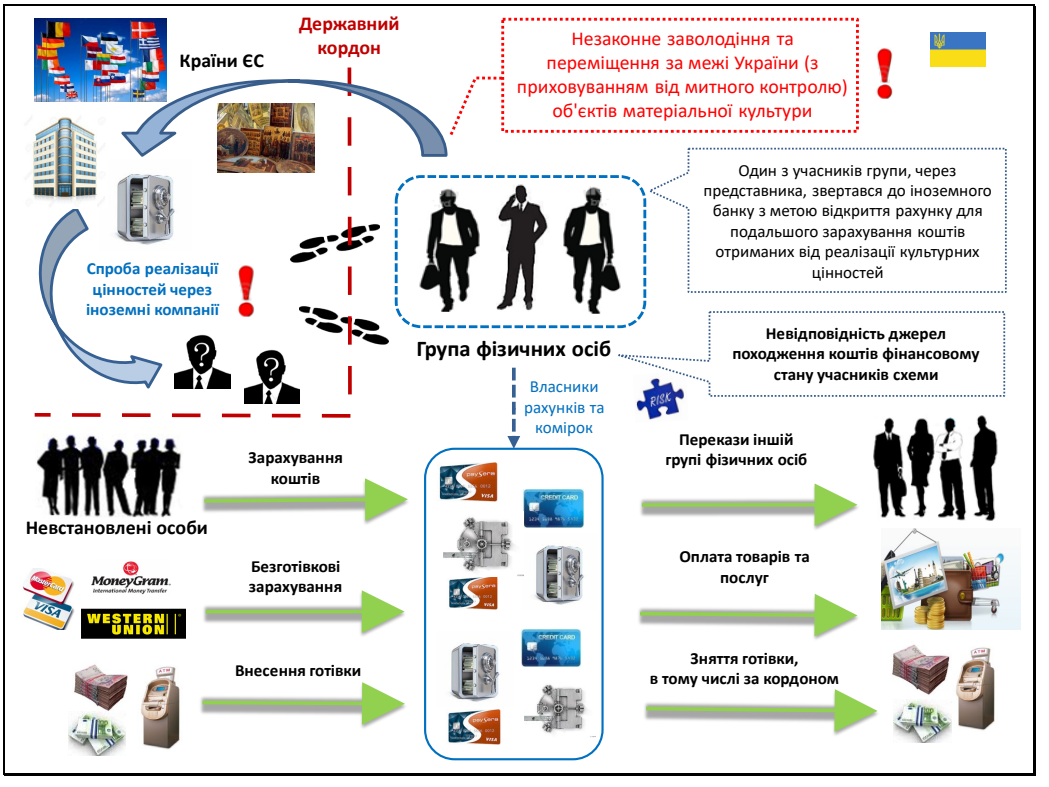
За наявною інформацією, **Групою фізичних осіб** на території країн Європейського союзу здійснювались дії, спрямовані на продаж культурних цінностей, які попередньо незаконно були вивезені з території України. До реалізації культурних цінностей особи також намагалися залучати пов'язані іноземні компанії. Крім того, відомо, що один з учасників **Групи фізичних осіб**, через представника, звертався до іноземного банку з метою відкриття рахунку для подальшого зарахування коштів, отриманих від реалізації культурних цінностей.

За результатами аналізу Держфінмоніторингом встановлено, що на рахунки зазначеної **Групи фізичних осіб** зараховувались безготівкові (у т. ч. з використанням систем міжнародних переказів) та готівкові кошти від значної кількості встановлених та невстановлених фізичних осіб.

Надалі, отримані кошти **Групою фізичних осіб** використовувались для придбання товарів/послуг, поповнення рахунків значної кількості інших осіб, переведення в готівку, в тому числі за кордоном.

У співпраці з іноземним ПФР виявлено частку викрадених культурних цінностей у банківській комірці банку іноземної компанії.

Правоохоронним органом здійснюється досудове розслідування.



РОЗДІЛ 5.9. ВІДМИВАННЯ ДОХОДІВ ОТРИМАНИХ ВІД ШАХРАЙСЬКИХ ДІЙ ТА КІБЕРЗЛОЧИНІВ

За наявною інформацією за 9 місяців 2023 року в Україні зареєстровано понад 80 тисяч кримінальних правопорушень пов'язаних з шахрайськими діями (ст. 190 КК України). Значний сплеск шахрайських дій спостерігається з середини 2022 року, що значною мірою пов'язане з початком повномасштабних бойових дій на території України. Під час війни шахраї використовують вразливість громадян, їх складний психоемоційний стан та матеріальні труднощі.

Найбільш розповсюдженими наразі є шахрайство при купівлі чи продажу товарів в Інтернеті, злам аккаунтів 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.

Особливо кричущими є факти шахрайства щодо військовослужбовців та їх родичів, а також осіб постраждалих від бойових дій. Це, зокрема:

- псевдоевакуація цивільних осіб з зони бойових дій;
- шахрайство при наданні в оренду або продажу житла внутрішньо переміщеним особам;
- продаж гуманітарної допомоги;
- псевдоволонтерська діяльність;
- виманювання коштів за надання інформації про осіб, які перебувають в полоні або вважаються безвісти зниклими;
- шахрайське заволодіння коштами, отриманими у вигляді державної допомоги родинам загиблих та безвісти зниклих військових.

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

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

Приклад 5.9.1. Шахрайське заволодіння коштами фізичних осіб з подальшою конвертацією в іноземні валюти та виведенням за межі України

За результатами аналізу інформації отриманої від банківської установи Держфінмоніторингом було виявлено фінансові операції, проведені **Фізичною особою Б**, характер яких свідчить про причетність до шахрайських дій.

На рахунки **Фізичної особи Б** проводились зарахування численних P2P переказів, які надалі списувались за допомогою Інтернет платформ, некоректна робота яких налаштована таким чином, щоб вводити в оману фінансові установи.

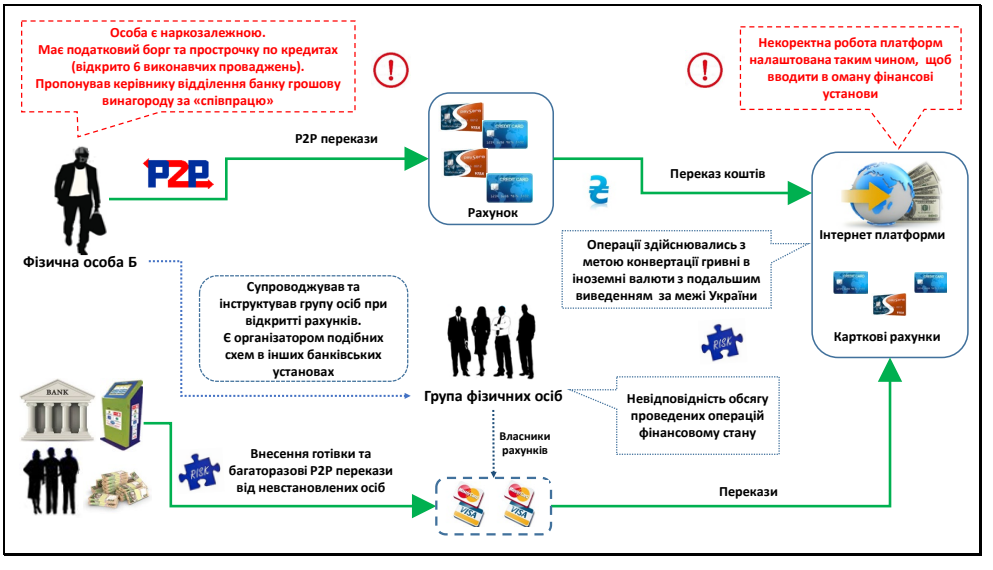
За наявною інформацією операції здійснювались з метою конвертації гривні в іноземні валюти з подальшим виведенням за межі України.

Аналогічні операції проводились **Групою фізичних осіб**, яких при відкритті рахунків супроводжувала та інструктувала **Фізична особа Б**. Під час відкриття рахунків **Фізична особа Б** поводилась роздратовано та пропонувала керівнику банку грошову винагороду за «співпрацю». Наявна інформація, що **Фізична особа Б** є організатором подібних схем в інших банківських установах.

Привертає увагу, що **Фізична особа Б** є наркозалежною, а також має податковий борг та прострочку по кредитах (відкрито 6 виконавчих проваджень).

Зважаючи на характер операцій (перекази що здійснюються, в основному дистанційно та через термінали самообслуговування) та значну кількість відправників коштів, існують підозри, що вищезазначені надходження коштів на рахунки, можуть бути пов'язані з легалізацією (відмиванням) доходів, одержаних злочинним шляхом.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.9.2. Відмивання доходів, з використанням віртуальних активів та шкідливого програмного забезпечення

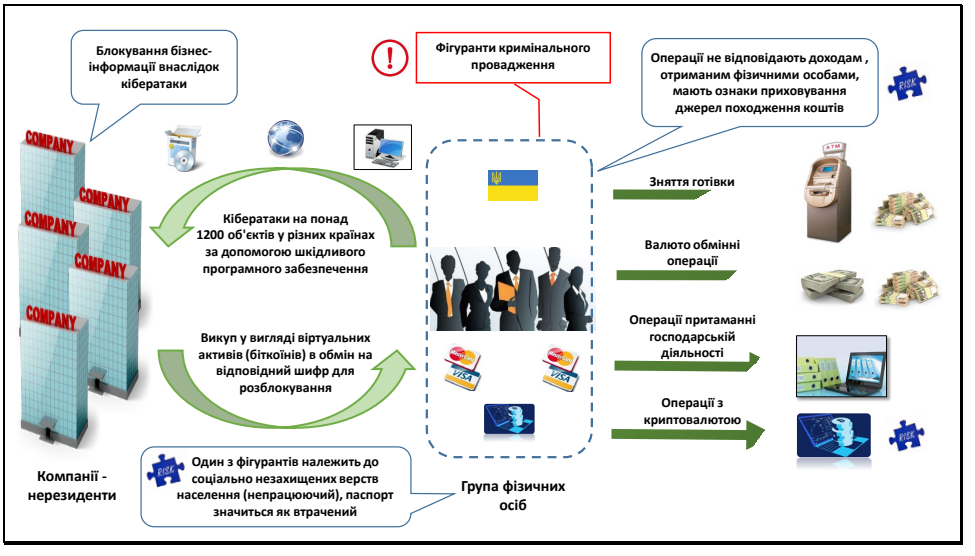
Держфінмоніторингом від правоохоронного органу отримано інформацію щодо проведення досудового розслідування відносно **Групи фізичних осіб**, яка може бути причетна до здійснення кібератак на понад 1 200 об'єктів у різних країнах за допомогою шкідливого програмного забезпечення. Надалі, шахраї вимагали сплатити викуп у вигляді віртуальних активів (біткоїнів) в обмін на відповідний шифрувальний ключ для розблокування даних.

Встановлено, що по рахунках **Групи фізичних осіб** проводяться операції, які не відповідають доходам, отриманих даними особами та мають ознаки приховування джерел походження коштів.

Так, **Групою фізичних осіб** здійснено фінансові операції на значні суми, які притаманні комерційній діяльності, операції з зарахування на карткові рахунки через провайдерів послуг з переказу електронних грошей та зарахування, які мають зв'язок з обміном/продажем криптовалюти, операції з обміну та обготівковування валюти, електронних коштів та криптовалют з використанням заборонених в Україні платіжних систем.

Один з фігурантів належить до соціально незахищених верств населення (безробітний), а його паспорт значиться як втрачений.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.9.3. Шахрайське заволодіння коштами з використанням підроблених довіреностей

Держфінмоніторингом було виявлено фінансові операції, проведені за участю **Групи фізичних осіб**, пов'язані з зарахуванням останніми безготівкових та готівкових коштів на рахунки, відкриті **Громадянином К**.

За наявною інформацією **Громадянин К** фігурує в кримінальному впровадженні щодо шахрайства у сфері соціальних виплат. Встановлено, що клієнт займався організацією отримання соціальних виплат для ВПО та мешканців ТОТ, без фактичного в'їзду вказаних осіб на територію України, в окремих випадках – щодо померлих.

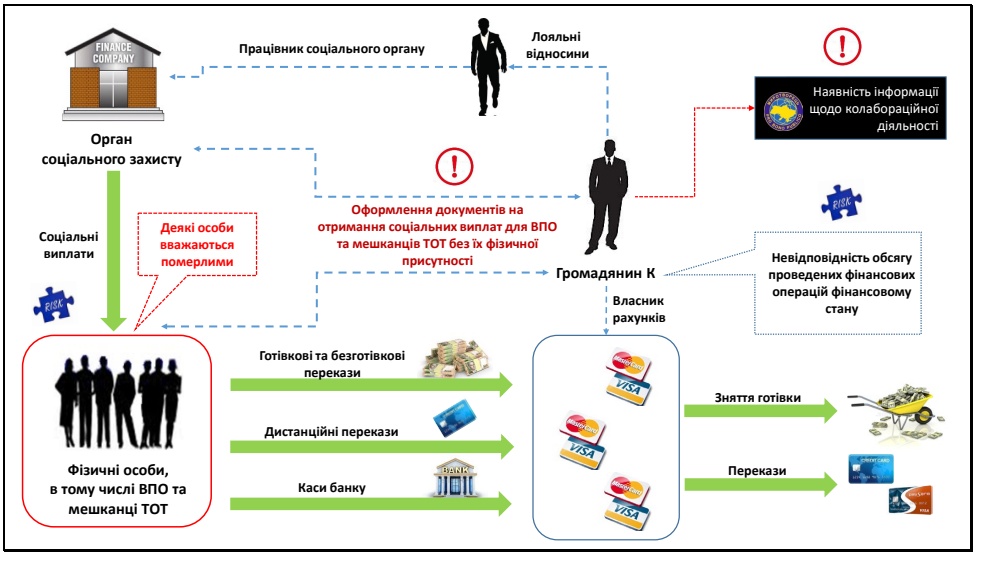
Громадянин К з використанням своїх зв'язків здійснював пошук осіб, які мають право на соціальні виплати, отримував копії документів, з використанням довіреностей на право представляти їх інтереси. Подавав

документи до органів соціальної підтримки, де мав лояльних працівників, які порушуючи порядок приймали від нього заяви та видавали відповідні довідки.

Надалі кошти, отримані **Громадянином К** від **Групи фізичних осіб**, переводились у готівку та перераховувались на користь невстановлених осіб.

Крім того, наявна інформація щодо причетності **Громадянина К** до колабораційної діяльності.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.9.4. Схема шахрайського заволодіння коштами фізичної особи з використання фішингу

Держфінмоніторингом з врахуванням інформації, отриманої від правоохоронного органу та банківських установ встановлено, що рахунки **Громадянина К** використані для шахрайського заволодіння грошовими коштами потерпілої особи, отриманими останньою у вигляді допомоги родині безвісти зниклого військового, з наступною їх легалізацією на користь третіх осіб.

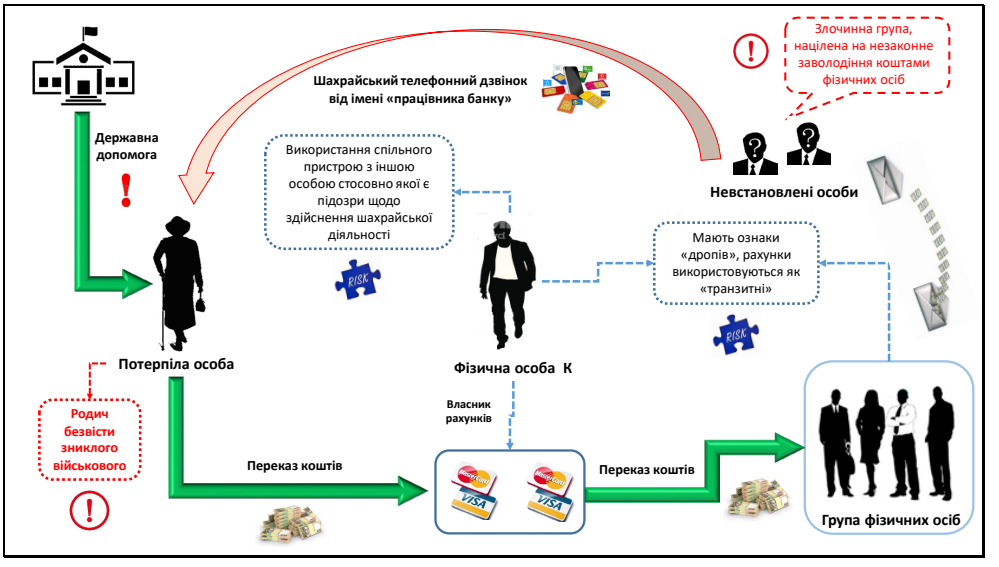
Потерпіла особа будучи введена в оману телефонним дзвінком від невідомої особи, яка представилась працівником банку, переказала кошти на карткові рахунки **Громадянина К**. Надалі отримані кошти транзитом були переведені на рахунки інших осіб.

Громадянин К та кінцеві отримувачі коштів мають ознаки «дропів», а їх рахунки та платіжні картки використовуються як «транзитні» для викрадених шахраями коштів.

Крім того, виявлено, що вхід до особистого кабінету **Громадянина К** здійснювався з пристрою спільного з іншою особою, стосовно якої також є підозри щодо здійснення шахрайської діяльності.

Вказане свідчить про функціонування організованої злочинної групи, націленої на незаконне заволодіння коштами фізичних осіб.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.9.5. Схема шахрайського заволодіння коштами фізичних осіб під виглядом залучення інвестицій

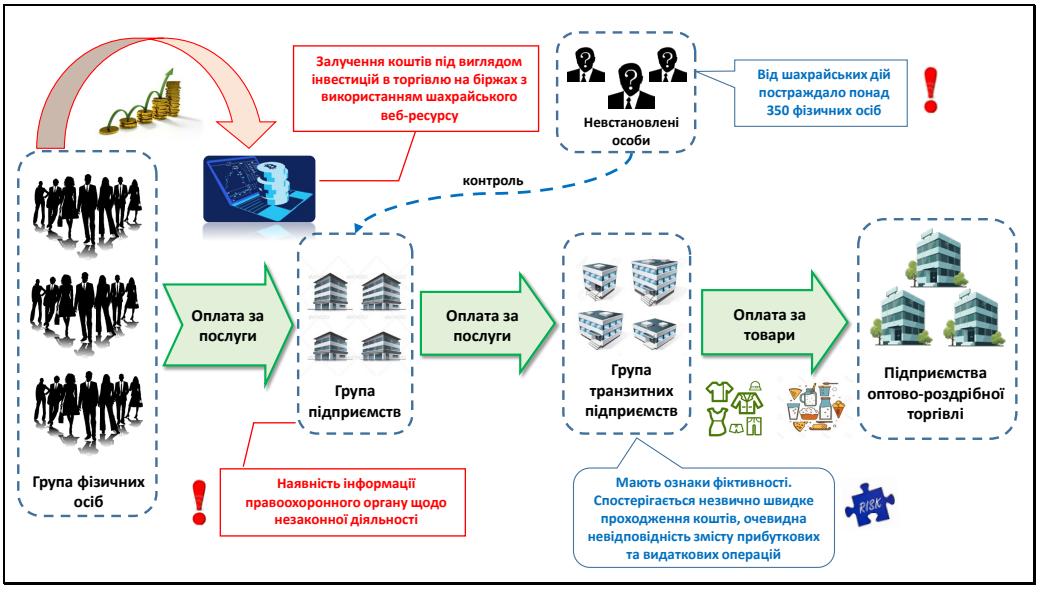
Держфінмоніторингом, з урахуванням інформації, отриманої від правоохоронного органу, виявлено «інвестиційну» шахрайську схему з використанням електронно-обчислювальної техніки.

За результатами аналізу встановлено, що шахраї під виглядом залучення «інвестицій» в торгівлю на біржах заволоділи коштами понад **350 фізичних осіб**. Клієнти залучались до «інвестування» за допомогою спеціально розробленого вебресурсу, а кошти виводились на **Групу підконтрольних підприємств**.

Надалі кошти були перераховані через **Групу «транзитних» підприємств** (з ознаками фіктивності) на користь групи інших компаній, які здійснюють оптово-роздрібну торгівлю і які можуть мати приховану готівку.

По **групі «транзитних» підприємств** спостерігається незвично швидке проходження коштів, очевидна невідповідність змісту прибуткових та видаткових операцій.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.9.6. Шахрайське заволодіння коштами фізичних осіб з використанням методів соціальної інженерії

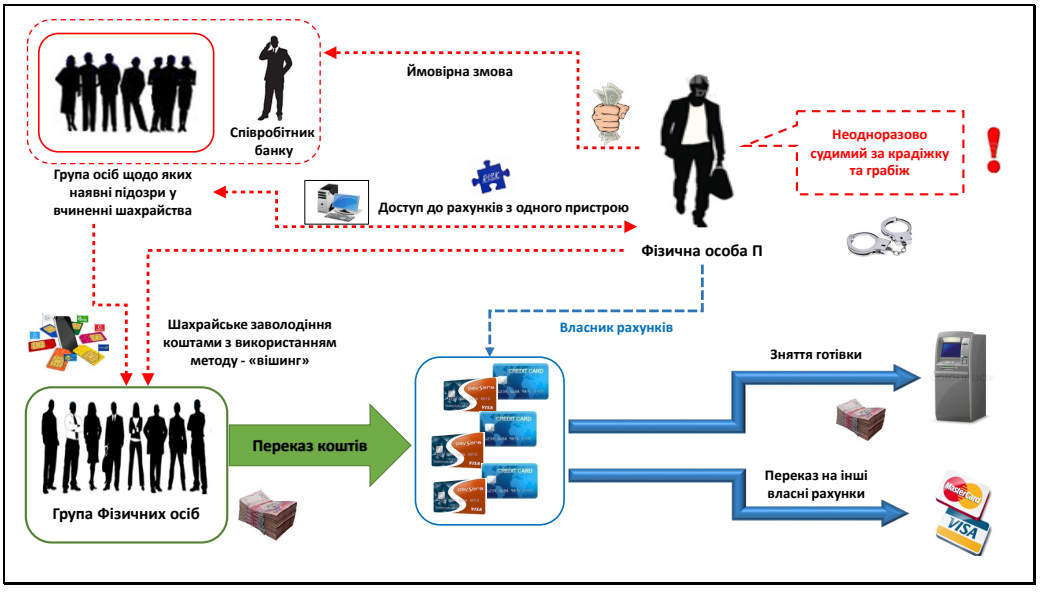
Держфінмоніторингом виявлено схему шахрайського заволодіння коштами фізичних осіб з використанням методу соціальної інженерії – «вішинг».

Встановлено, що рахунки, відкриті **Громадянином П** (неодноразово судимий за крадіжку та грабіж) використовувались для шахрайського заволодіння грошовими коштами фізичних осіб. Надалі кошти переводились в готівку та переказувались на інші власні рахунки, з метою приховування (маскування) джерела походження таких коштів.

Існує ймовірність, що шахрайське заволодіння коштами було організоване заздалегідь, шляхом змови невстановлених осіб та співробітника одного з банків, в якому було відкрито рахунок потерпілої особи.

Крім цього, оскільки підключення до рахунку **Громадянина П** здійснювалося з пристрою, який використовувався для підключення до рахунків ряду інших осіб, щодо яких наявні підозри у вчиненні шахрайства, ймовірно, що шахрайські дії вчинялися злочинним організованим угрупуванням.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.9.7. Заволодіння даними фізичних осіб шляхом злому сторінки в соціальній мережі

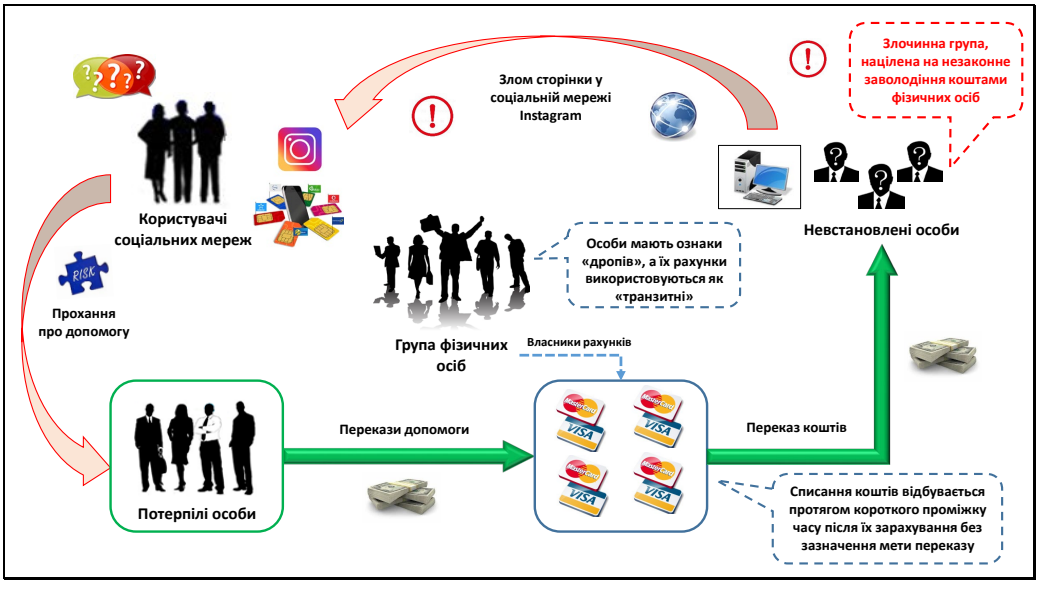
Держфінмоніторингом з врахуванням інформації, отриманої від правоохоронного органу та банківських установ встановлено, що карткові рахунки **Групи фізичних осіб** використані для шахрайського заволодіння грошовими коштами, з наступною їх легалізацією на користь невстановлених осіб.

Потерпілі особи, будучи введені шахраями в оману, здійснювали перекази у вигляді надання допомоги за реквізитами розміщеними на зламаних сторінках їх знайомих в соціальній мережі «Instagram».

Зазначені **фізичні особи** мають ознаки «дропів», а їх рахунки та платіжні картки використовуються як «транзитні» для викрадених шахраями коштів. Списання коштів відбувається протягом короткого проміжку часу після їх зарахування без зазначення мети переказу.

Вказане може свідчити про функціонування організованої злочинної групи, націленої на незаконне заволодіння коштами фізичних осіб.

Правоохоронним органом здійснюється досудове розслідування.



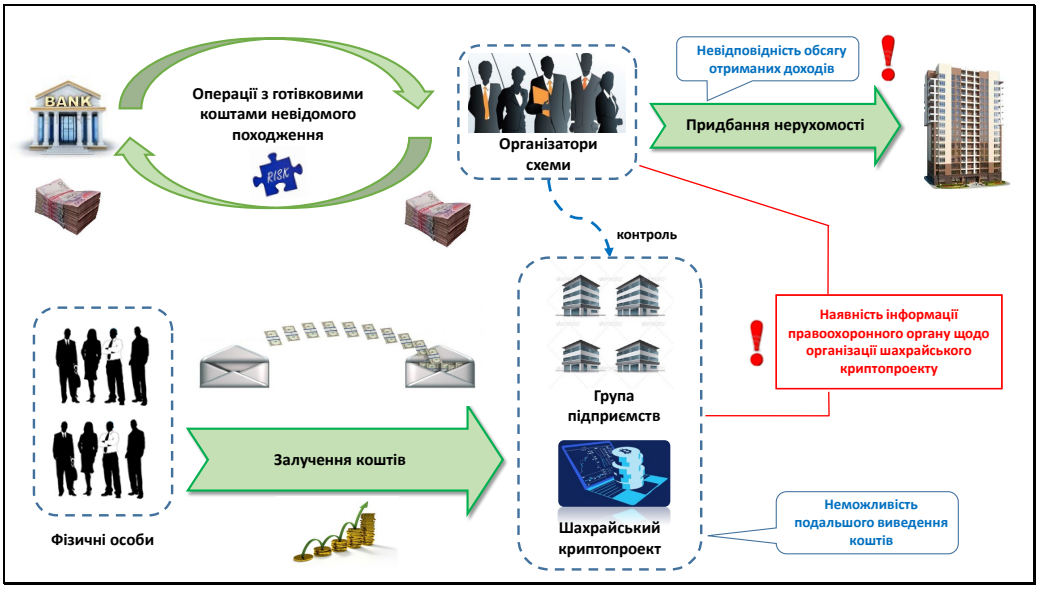
Приклад 5.9.8. Схема заволодіння коштами фізичних осіб з використанням фінансової піраміди

Держфінмоніторингом, з урахуванням інформації, отриманої від правоохоронного органу, виявлено схему заволодіння коштами фізичних осіб з використанням шахрайського криптопроєкту.

За результатами аналізу встановлено, що шахраями для залучення коштів фізичних осіб створено блокчейн-проєкт, організований за принципом фінансової піраміди. При цьому подальше виведення коштів з проєкту для інвесторів є неможливим.

Привертає увагу, що організаторами шахрайської схеми проводились операції з готівковими коштами невідомого походження. Надалі кошти спрямовувались на придбання нерухомості. Сума таких операцій значно перевищує обсяг задекларованих доходів.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.9.9. Шахрайське заволодіння майном померлих іноземних громадян за підробленими документами

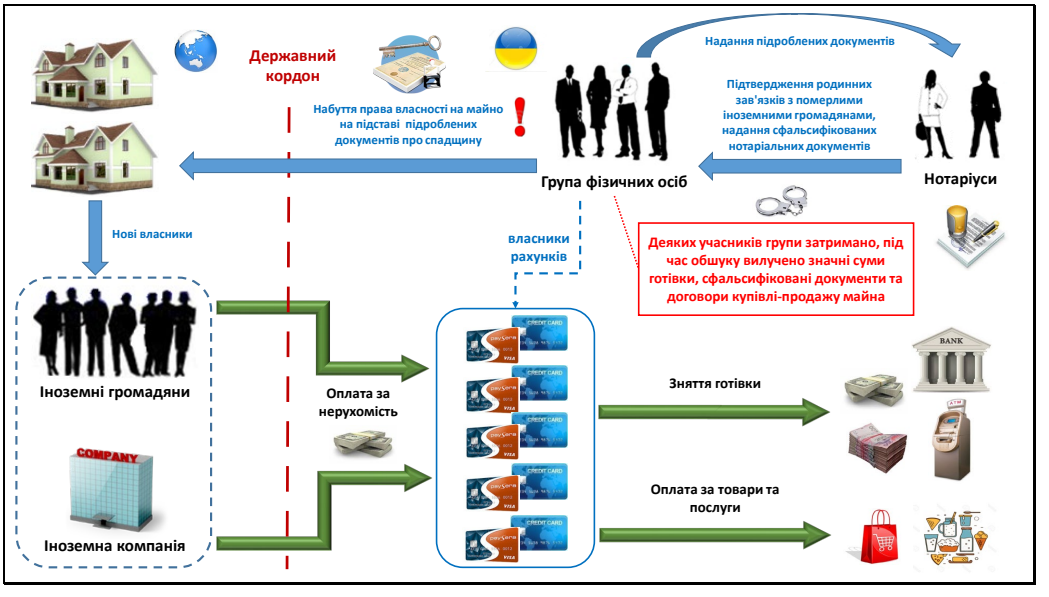
Держфінмоніторингом, за результатами аналізу інформації, отриманої від правоохоронного органу та банківської установи, було виявлено фінансові операції, які пов'язані з акумулюванням коштів, отриманих з-за кордону, ймовірно у шахрайський спосіб, на рахунках **Групи фізичних осіб – громадян України** та з подальшою їх легалізацією.

Так, від іноземної компанії та іноземних громадян на рахунки **Групи фізичних осіб** було зараховано кошти як оплата за нерухоме майно, право власності на яке було отримане на підставі підроблених документів про спадщину. Встановлено, що **Групою фізичних осіб** подавались нотаріусам підроблені документи щодо родинних зв'язків з померлими іноземними громадянами з метою оформлення документів на спадщину. Надалі, учасники групи набували право власності на нерухоме майно на підставі сфальсифікованих документів та здійснювали його продаж новим власникам.

Незаконно отримані **Групою фізичних осіб** кошти було переказано між власними картками, конвертовано в гривню, здійснено розрахунки за товари/послуги, а основна частина коштів знята готівкою.

Деяких учасників групи було затримано, а під час обшуку вилучено значні суми готівки, сфальсифіковані документи та договори купівлі-продажу нерухомого майна.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.9.10. Схема легалізації доходів від онлайн-шахрайства

Держфінмоніторингом від іноземного ПФР отримано інформацію про підозрілі фінансові операції, проведені по рахунках **Компанії-нерезидента**, власниками якої є **громадяни України**.

Так, на рахунок **Компанії-нерезидента** протягом короткого періоду часу зараховано значні за розміром підозрілі перекази від фізичних та юридичних осіб. Кошти зараховувались переважно від фізичних осіб, громадян України та Туреччини. Надалі кошти, майже у повному обсязі, перераховано на рахунок **Компанії-нерезидента** в іншу юрисдикцію. Економічна доцільність проведених операцій є сумнівною.

Привертає увагу, що рахунки компанії відкриті в двох іноземних фінансових установах, а не в країні реєстрації. Існує підозра, що рахунок **Компанії-нерезидента** використовувався для зберігання, нашарування та виплати грошей, отриманих від онлайн-шахрайства.

При цьому, діяльність **Компанії-нерезидента** не відповідає задекларованій при реєстрації (продаж текстилю) та, ймовірно, пов'язана з криптоторгівлею.

Крім того, у відкритих джерелах знайдено інформацію щодо продажу **Компанії-нерезидента** за 400 дол США як інтернет-магазину.

Правоохоронним органом здійснюється досудове розслідування.

Приклад 5.9.11. Схема шахрайського заволодіння коштами фінансових посередників

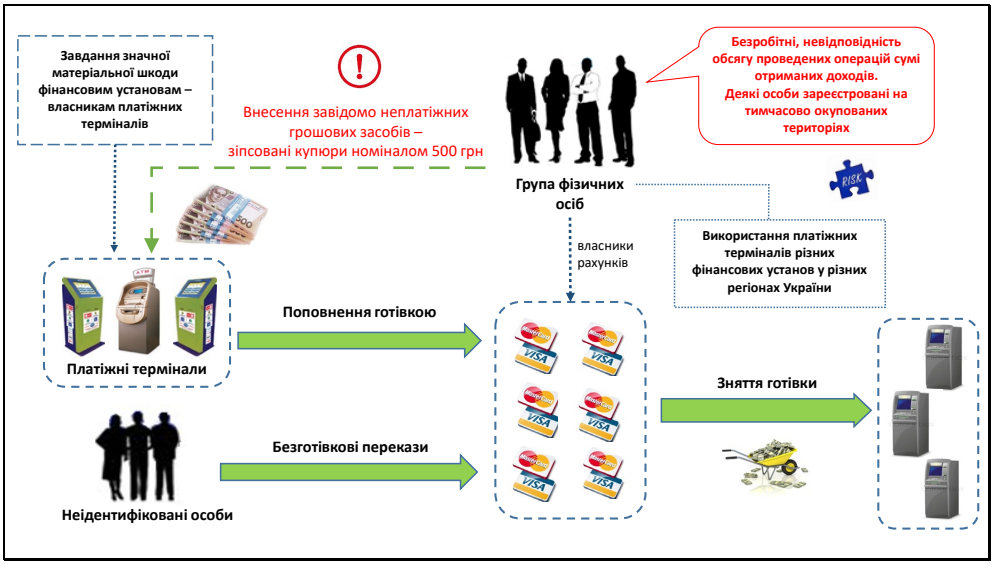
Держфінмоніторингом, за результатами аналізу фінансових операцій та додаткової інформації, отриманої від банку, виявлену схему заволодіння **Групою фізичних осіб** коштами фінансових посередників у шахрайський спосіб.

Так, **Група фізичних осіб** використовуючи платіжні термінали різних фінансових установ, розташовані в різних регіонах України, вносили на рахунки свідомо неплатіжні засоби (пошкоджені купюри номіналом 500 грн) та надалі знімали кошти готівкою через банкомати, чим завдали значної фінансової шкоди власникам платіжних терміналів.

Крім того, на рахунки **Групи фізичних осіб** здійснювались безготівкові перекази від неідентифікованих клієнтів.

Задіяні у шахрайській схемі **Фізичні особи** є безробітними, обсяг проведених операцій не відповідає сумі отриманих доходів. Деякі **Фізичні особи** зареєстровані на тимчасово окупованих територіях.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.9.12. Обготівковування коштів невідомого походження

Держфінмоніторингом виявлено схему, яка була направлена на обготівковування коштів невідомого походження.

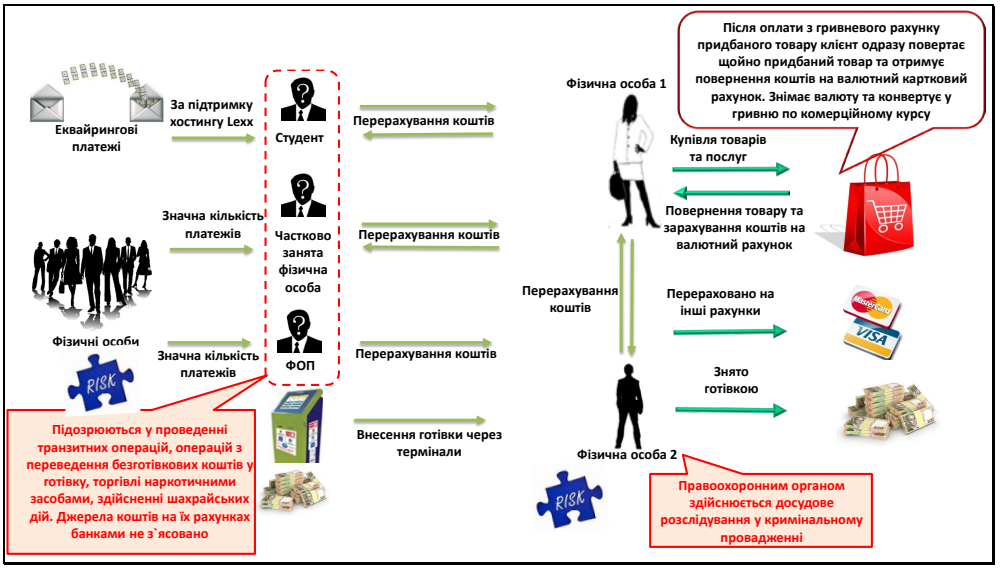
Відомо, що на рахунки **Фізичної особи 1** та **Фізичної особи 2** зараховувались кошти від значної кількості третіх осіб, в т.ч.: **Студента**, **Частково зайнятої фізичної особи** та **ФОП,** перераховувались зі своїх інших рахунків та зараховувались готівкою.

В свою чергу вищезазначені кошти **Студент** та **ФОП** попередньо отримували на карту від різних фізичних осіб, без зазначеної мети. **Частково зайнята фізична особа** отримувала зарахування еквайрингових платежів за підтримку хостингу Lexx (що не існує).

Надалі, **Фізичною особою 1** та **Фізичною особою 2** кошти частково обготівковано, інша частина переказана на значну кількість платіжних карток. Також за частину коштів придбано товари, які було повернуто, а кошти зараховано на валютний рахунок по курсу НБУ. Далі **Фізична особа 1** знімає готівку з рахунку через касу банку та конвертує її в гривню по комерційному курсу.

Також відомо, що правоохоронним органом здійснюється досудове розслідування щодо **Фізичної особи 2.**

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.9.13. Заволодіння чужим майном шахрайським шляхом

Держфінмоніторингом, з врахуванням інформації отриманої від правоохоронного органу, виявлено схему заволодіння чужим майном шахрайським шляхом під приводом продажу товарів військового призначення.

Встановлено, що на рахунки **Фізичної особи А** та інших підконтрольних їй осіб було зараховано значні суми коштів від волонтерів, військових та благодійних фондів як оплата за квадрокоптери. Всупереч 100% передоплати товар не був поставлений.

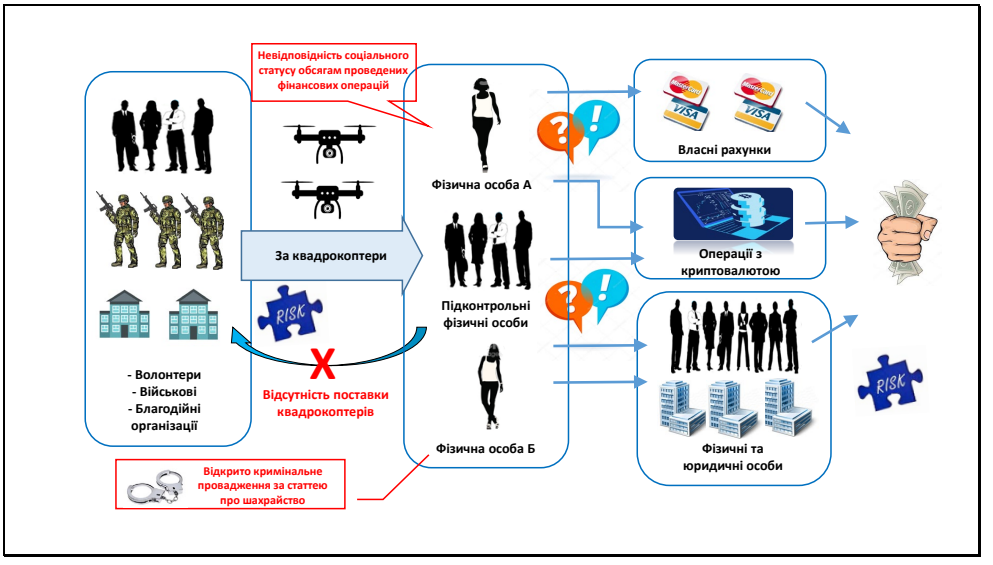
Надалі, кошти з рахунків **Фізичної особи А** частково були перераховані на власні карткові рахунки та на користь **Групи фізичних та юридичних осіб**.

Відомо, що **Фізична особа А** з метою легалізації вищезазначених коштів здійснювала операції з купівлі-продажу криптовалюти, яку перераховувала на власні криптогаманці та підконтрольних їй осіб.

Однією з підконтрольних **Фізичній особі А** осіб - **Фізичною особою Б** під час війни було відкрито салон краси, а також вона має довіреність на вчинення будь-яких дій від імені **Фізичної особи А**. Крім того, відомо, що відносно **Фізичної особи Б** відкрито кримінальне провадження за підозрами у шахрайських дій під час пандемії.

Існують підозри, що проведені операції могли бути здійснені з метою заволодіння чужим майном шляхом обману чи зловживання довірою (шахрайство) та приховування, маскування джерел походження коштів.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.9.14. Відмивання коштів невідомого походження, отриманих, у тому числі, шахрайським шляхом

Держфінмоніторингом з урахуванням інформації виявлено схему, яка була направлена на відмивання коштів невідомого походження, отриманих, у тому числі шахрайським шляхом.

Відомо, що на рахунки двох **Фізичних осіб** зараховувались великі суми кошти з різних джерел: готівкою, перераховування зі своїх інших рахунків, від операцій купівлі-продажу криптовалюти, як перекази від третіх осіб. В свою чергу, на рахунки третіх осіб кошти зараховувались внаслідок великої кількості P2P переказів від значної кількості кореспондентів та вносились на рахунки готівкою.

Частина отриманих коштів була переведена в іноземну валюту за допомогою циклічних операцій з використанням послуги Apple Pay: відразу після оплати товару з гривневого рахунку через pos-термінал, **Фізична особа** повертає щойно придбаний товар та за допомогою Apple Pay (але вже прив'язаного до валютного карткового рахунку, відкритого в українському банку), отримує повернення коштів в іноземній валюті по курсу НБУ.

Таким чином **Фізична особа** конвертує гривню невідомого походження у валюту по банківському курсу. Далі **Фізична особа** знімає готівку через касу банку, конвертує її у гривню по комерційному курсу, вносить на рахунок та повторює подібну операцію.

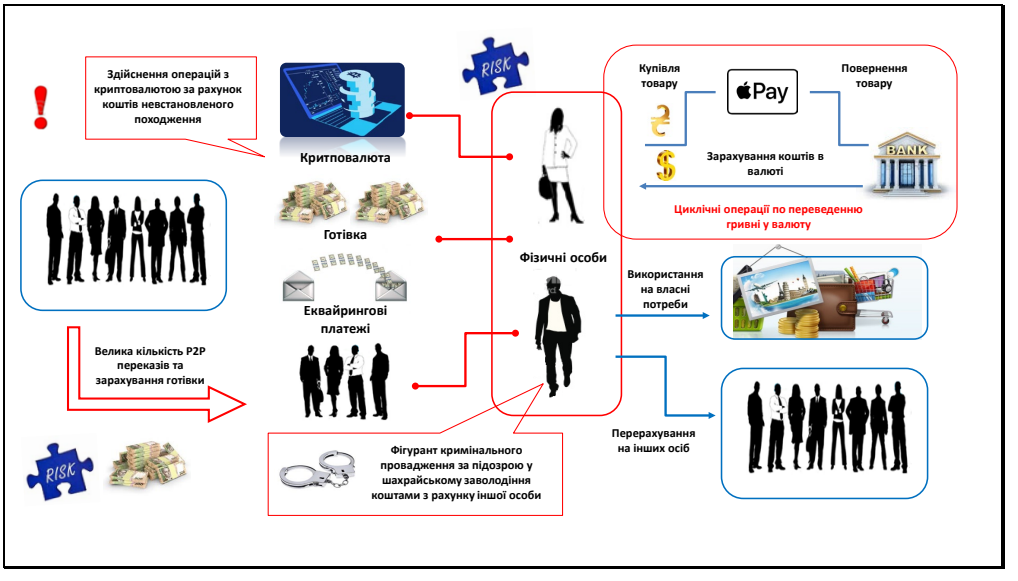
Інша частина коштів була використана **Фізичними особами** на оплату товарів та послуг для власних потреб та перерахована на користь інших осіб.

Привертає увагу, що більшість фізичних осіб, залучених до проведення фінансових операцій, не мають офіційно задекларованих доходів, які б дозволили проводити операції на значні суми.

Також відомо, що відносно однієї з **Фізичних осіб** правоохоронним органом здійснюється досудове розслідування у кримінальному провадженні за підозрою у шахрайському заволодінні коштами іншої особи шляхом несанкціонованого доступу до системи дистанційного банківського обслуговування рахунку.

Таким чином, існують підозри, що **Фізичні особи** є учасниками схемних операцій з грошовими коштами незаконного походження, отриманих, у тому числі від шахрайських дій.

Правоохоронним органом здійснюється досудове розслідування.



РОЗДІЛ 5.10. ВІДМИВАННЯ ЗЛОЧИННИХ ДОХОДІВ ІЗ ВИКОРИСТАННЯМ ВІРТУАЛЬНИХ АКТИВІВ ТА ЧЕРЕЗ ГРАЛЬНИЙ БІЗНЕС

На сьогодні в Україні лише впроваджується нормативна база щодо обігу цифрових валют, діяльності криптобірж та особливостей оподаткування операцій з віртуальними активами.

Водночас ринок обігу віртуальних активів та гральний бізнес, належить до високоризикованих сфер діяльності, які потребують особливої уваги контролюючих та правоохоронних органів.

Так, криптовалюти можуть використовуватись для обходу санкцій, виведення коштів за кордон, фінансування терористичної діяльності, приховування доходів від незаконного грального бізнесу, торгівлі зброєю, наркотиками та іншими забороненими речовинами.

Перевагами використання цифрових валют залишаються висока анонімність та швидкість переказу коштів, як в межах країни, так і за кордон,

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

децентралізація платежів, обмежене регулювання або його відсутність в деяких юрисдикціях.

Своєю чергою, гральний бізнес найчастіше залучений до схем ухилення від сплати податків, до яких можуть бути залучені банківські установи шляхом створення спеціальних програмно-апаратних механізмів, заміни платіжних документів та міскодингу (вид шахрайства в банківській еквайринговій мережі, який полягає в підміні призначення платежу).

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

Приклад 5.10.1. Легалізація (відмивання) доходів шляхом через криптоактиви

Держфінмоніторингом, виявлено схему легалізації (відмивання) доходів, шляхом отримання віртуальних активів від **Криптовалютних бірж росії** попри наявні санкції.

Встановлено, що **Криптовалютна біржа** на території України отримувала кошти у вигляді віртуальних активів від значної кількості контрагентів, серед яких наявні регулярні перекази від **Криптовалютних бірж росії** та **Даркнет-майданчиків**.

Відомо, що на вищезазначені **Криптовалютні біржі росії** та **Даркнет-майданчики** було накладено спеціальні заходи, які забороняли здійснювати перекази коштів за їх участю. Проте, в обхід санкцій **Криптовалютними біржами росії** уже після накладення відповідних санкцій створено нові адреси для проведення діяльності та здійснення переказів на територію України.

Крім того, українська **Криптовалютна біржа** отримувала віртуальні активи від ряду неліцензованих P2P-майданчиків та OTC-обмінників, які окрім України діють на території росії, Казахстану та інших центральноазіатських країн. При цьому, ці P2P-майданчики надають незаконні послуги обміну криптовалюти на фіатні кошти з використанням банківських карток підсанкційних російських банків, казахських банків, а також найбільших українських банків, що створює значні ризики використання **Криптовалютної біржі України** з метою обходу санкцій, накладених та фінансовий ринок росії, можливості фінансування колабораціонізму в Україні тощо.

Водночас, **Криптовалютні біржі росії** проводили значну кількість транзакцій з іранськими криптовалютними біржами, а також з незаконними «міксерами», через які відмивало кошти злочинне хакерське угрупування Lazarus Group, яке підтримується Північною Кореєю та діє в її інтересах. Таким чином, наявні підозри причетності **Криптовалютної біржи росії** також до порушення Резолюцій ООН та Рекомендацій FATF, що стосуються Ірану та Північної Кореї.

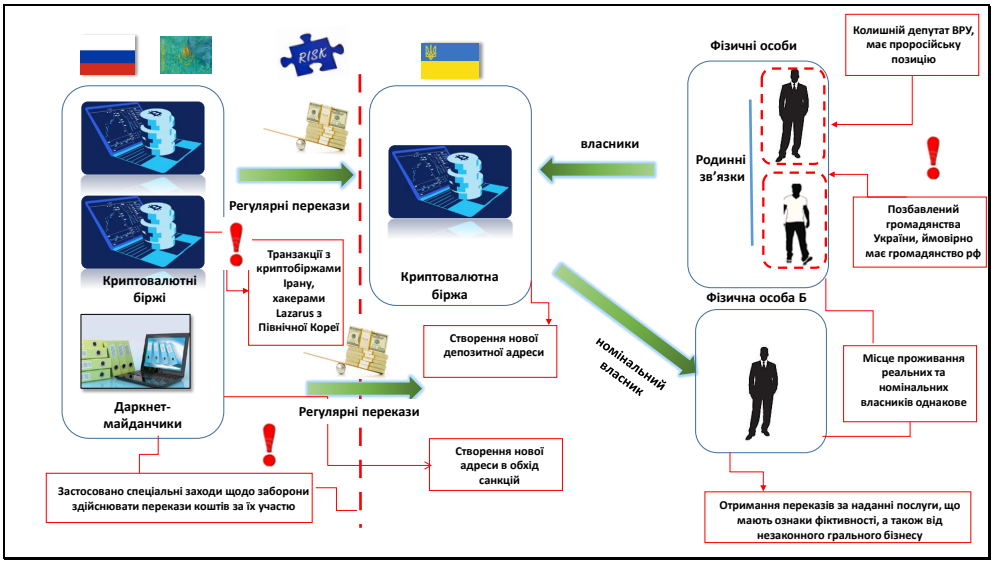
Як стало відомо, реальними власниками **Криптовалютної біржі України** є **Фізичні особи**, які пов'язанні між собою родинними зв'язками, один з яких є колишнім депутатом та має проросійську позицію, а інший позбавлений громадянства України через ймовірне набуття російського громадянства.

Також, встановлено, що **Фізична особа Б** є номінальним керівником **Криптовалютної біржі** України, яка володіє банківськими рахунками на території України та інших країн.

Переважним джерелом походження коштів на українському рахунку **Фізичної особи Б** є перекази від компаній, які фігурували в інших розслідуваннях щодо їх причетності до діяльності конвертаційних центрів та професійних майданчиків для відмивання коштів. Кошти надходили як оплата за послуги з розробки програмного забезпечення компанії-нерезидента, яка має ознаки фіктивності, а також перекази від компаній, пов'язаних з діяльністю незаконного грального бізнесу в Україні.

Існують підозри вважати, що **Криптовалютна біржа** на території України здійснює протиправну діяльність, шляхом співпраці з **Криптовалютними біржами росії** та **Даркнет-майданчиками**, з метою обходу санкцій та відмивання коштів злочинного походження.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.10.2. Ухилення від сплати податків шляхом організації діяльності нелегального пункту обміну криптовалют

Держфінмоніторингом, з урахуванням інформації правоохоронного органу, виявлено схему ухилення від сплати податків шляхом організації діяльності нелегального пункту обміну криптовалют.

Встановлено, що на рахунок **Юридичної особи А** здійснено зарахування готівкових коштів від **Групи фізичних осіб** як торгівельну виручку, що не відповідає основному виду діяльності компанії. Надалі дані кошти були перераховані на користь **Групи юридичних осіб**.

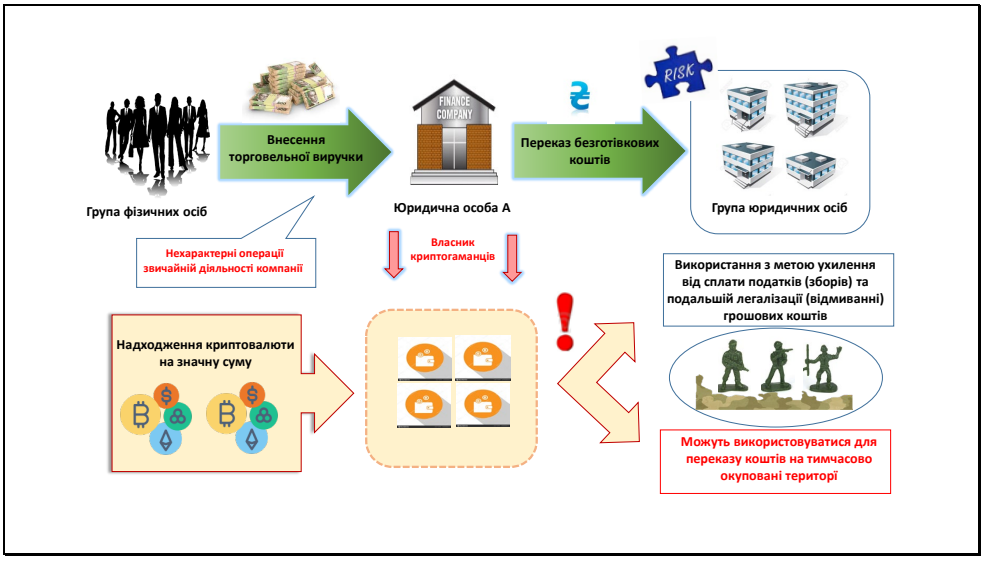
Водночас виявлено надходження на криптогаманці криптовалюти на значну суму, які належать **Юридичній особі А** та використовуються з метою надання послуг з переведення криптовалюти у готівку (як на території України, так і за кордоном).

Є підстави вважати, що криптогаманці **Юридичної особи А** використовуються у протиправній схемі здійснення незаконної діяльності з ухилення від сплати податків (зборів) та подальшій легалізації (відмиванні) грошових коштів.

Привертає увагу, що діяльність вказаного пункту обміну криптовалют також розповсюджувалась на тимчасово окуповані території.

Крім того, за наявною інформацією від правоохоронного органу та з відкритих джерел встановлено, що вказані операції з криптовалютою можуть бути пов'язані з фінансуванням незаконних збройних формувань.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.10.3. Фінансування незаконних воєнізованих угрупувань з використанням криптовалюти

Держфінмоніторингом, з урахуванням інформації правоохоронного органу, виявлено схему, пов'язану з обігом криптовалюти, яка може використовуватись для фінансування незаконних воєнізованих угрупувань.

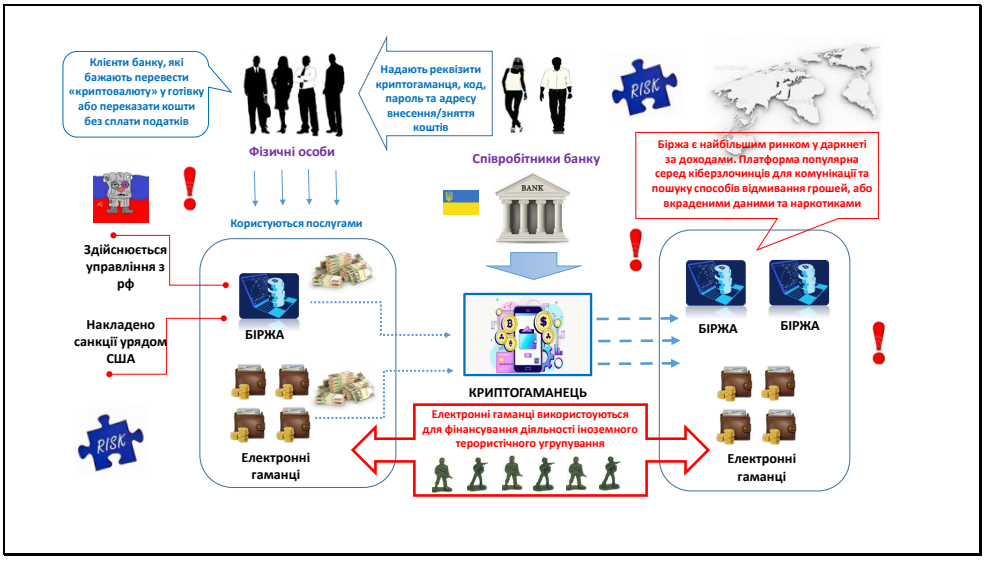
Встановлено, що у вказаній протиправній схемі використовувався **Криптогаманець**, інформацію про який (реквізити, коди, паролі, адресу) надавали співробітники українського **Банку** своїм клієнтам, які бажали перевести криптовалюту в готівку або переказати її, уникаючи сплати податків.

В більшості випадків зарахування коштів на **Криптогаманець** відбувалося через спеціальні обмінники з **Електронних гаманців,** які, у тому числі використовуються для фінансування терористичної діяльності, або від підсанкційної **Біржі** (зареєстрована в одній з країн Євросоюзу, але її IT-інфраструктура знаходиться на території росії).

Надалі кошти з **Криптогаманця** перераховувались на користь **Іноземного воєнізованого угрупування** з Ближнього сходу або на електронні гаманці, зареєстровані на різних криптовалютних біржах. Одна з них є найбільшим ринком у даркнеті за доходами. Платформа популярна серед кіберзлочинців для комунікації та пошуку способів відмивання грошей, або вкраденими даними та наркотиками.

Таким чином, виявлено схему пов'язану із впровадженням незаконної діяльності, ухилення від сплати податків, зборів (обов'язкових платежів) та подальшим фінансуванням воєнізованих угрупувань та терористичних організацій за сприянням працівників одного з українських банків.

Правоохоронними органами здійснюється досудове розслідування.



Приклад 5.10.4. Легалізація (відмивання) доходів шляхом придбання криптовалюти

Держфінмоніторингом, з урахуванням інформації підрозділу фінансової розвідки іноземної країни, виявлено схему легалізації (відмивання) доходів, отриманих від здійснення протиправної діяльності, шляхом придбання віртуальної валюти – bitcoin (BTC).

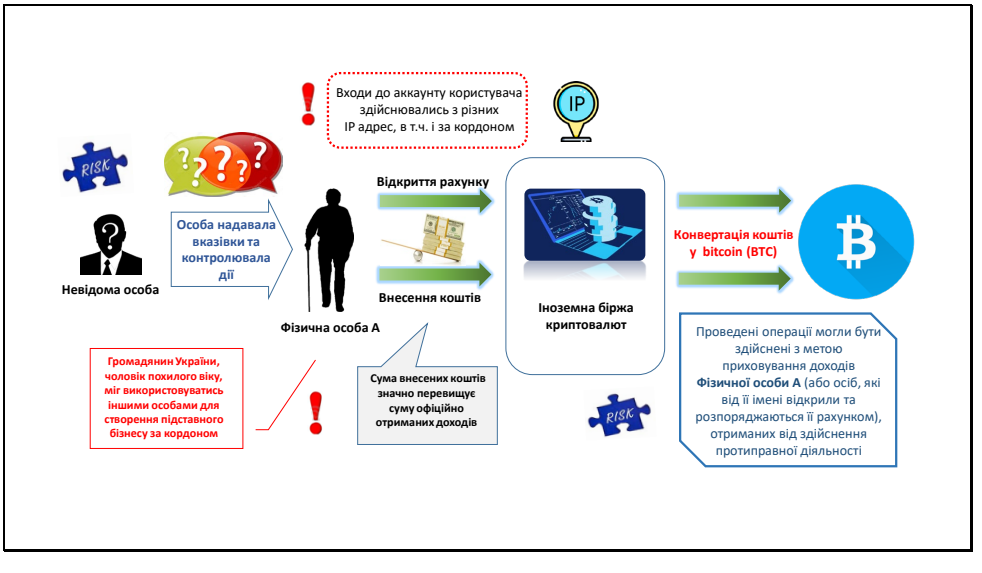
Встановлено, що **Фізичною особою А** було відкрито рахунок у біржі криптовалют за кордоном, на який внесено значну суму коштів, яка значно перевищує суму офіційно отриманих доходів цією особою. Кошти було конвертовано у віртуальну валюту – bitcoin (BTC).

Привертає увагу, що **Фізична особа А** є особою похилого віку. Крім того, під час процедури ідентифікації особистості при відкритті рахунку, була присутня стороння невідома особа, яка надавала вказівки **Фізичній особі А** та контролювала її дії. Привертає увагу й те, що для входу в аккаунт користувача використовувались різні IP адреси, в т.ч. і за кордоном.

Як стало відомо, **Фізична особа А** могла використовуватися для створення підставного бізнесу за кордоном та приховування схеми з відмивання коштів.

Існують підозри, що проведені операції могли бути здійснені з метою приховування доходів **Фізичної особи А** (або осіб, які від її імені відкрили та розпоряджаються її рахунком), отриманих від здійснення протиправної діяльності.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.10.5. Міскодінг

Держфінмоніторингом, з урахуванням інформації правоохоронного органу, виявлено схему використання карток **Групи фізичних осіб** для поповнення ігрових акаунтів незаконних казино в мережі Інтернет та інших неліцензованих платіжних сервісів.

Встановлено, що від великої кількості **Фізичних осіб** незначними сумами зараховуються кошти у безготівковій/готівковій формах, через транзитні банківські рахунки та банківські термінали, на карткові рахунки **Групи фізичних осіб**, де акумулюються.

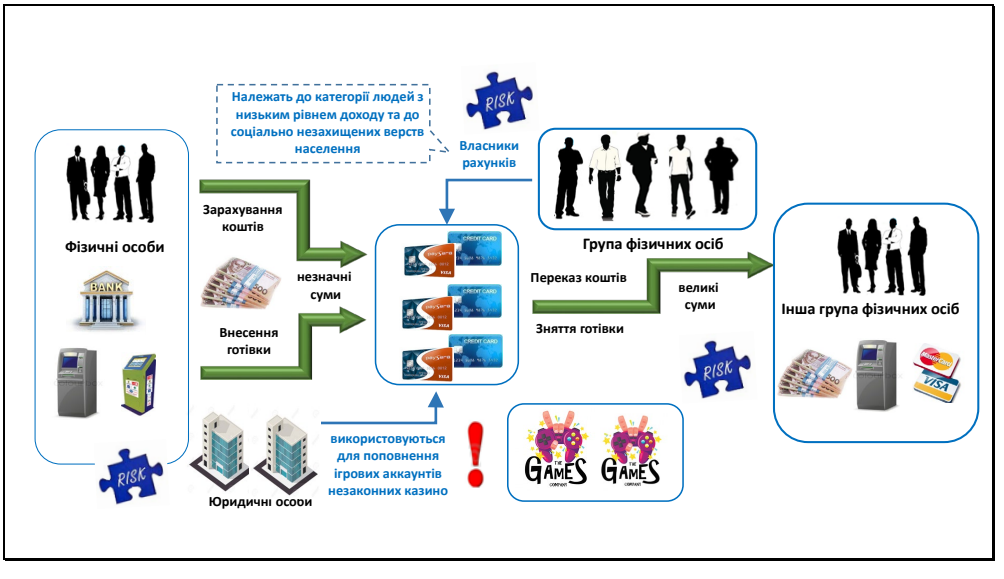
При цьому, **Група фізичних осіб** належить до категорії людей з низьким рівнем доходу (студенти, жінки, які перебувають у декретній відпустці, пенсіонери) або тимчасово безробітні.

Надалі, кошти перераховуються **Іншій групі осіб** у безготівковій/готівковій формах значно більшими сумами.

Крім того, за наявною інформацією від правоохоронного органу карткові рахунки **Групи фізичних осіб** використовуються для поповнення ігрових аккаунтів незаконних казино в мережі Інтернет та інших неліцензованих платіжних сервісів.

Є підстави вважати, що карткові рахунки **Групи фізичних осіб**, використовуються **Юридичними особами** в схемі незаконної організації та проведення азартних ігор, ймовірно за допомогою міскодингу (маніпуляції банківськими системами для приховування реального походження платежів).

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.10.6. Легалізація (відмивання) доходів, ймовірно отриманих від здійснення протиправної діяльності

Держфінмоніторингом за результатами аналізу інформації, отриманої від компанії, що здійснює діяльність з організації та функціонування мережі гральних автоматів, виявлено схему легалізації (відмивання) доходів, ймовірно отриманих від здійснення протиправної діяльності.

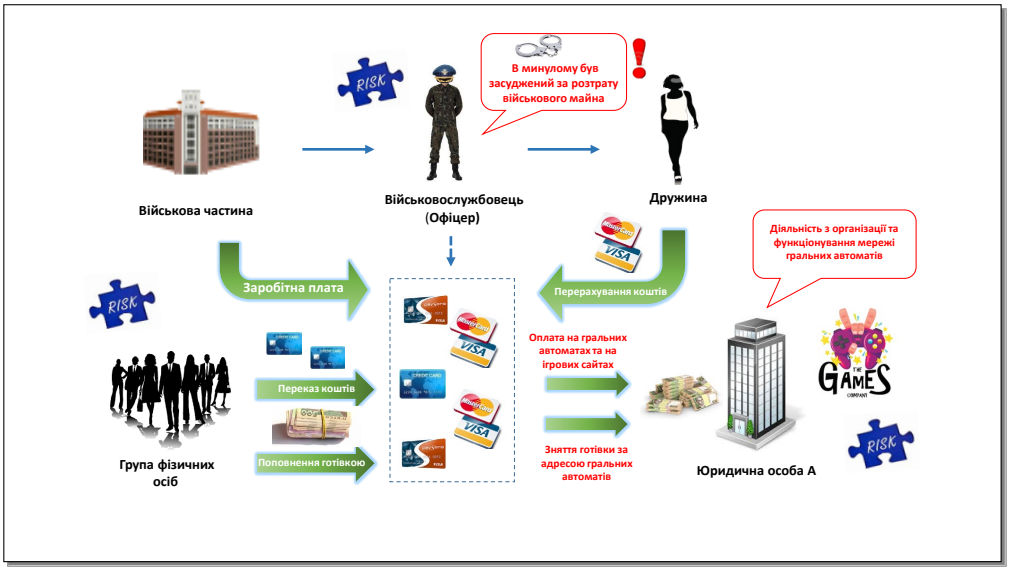
З карткових рахунків **Військовослужбовця (офіцера)** систематично здійснюється перерахування коштів у значних розмірах як оплата на гральних автоматах та на ігрових сайтах на користь **Юридичної особи А**, яка володіє мережею гральних автоматів.

На карткові рахунки **Військовослужбовця** (близько 20 карток) окрім заробітної плати та переказів від дружини, систематично зараховуються кошти з карток значної кількості фізичних осіб. Також, здійснюється готівкове поповнення карткового рахунку різними фізичними особами в різних містах однієї області. Надалі ці кошти використовуються для оплати азартних ігор або знімаються готівкою через банкомат за адресою розташування залу гральних автоматів.

Військовослужбовець проживає та відвідує заклади гральних автоматів на території області, що межує з областями, в яких ведуться активні бойові дії. Також встановлено, що **Військовослужбовець** в минулому був засуджений за розтрату військового майна.

Існують підозри, що кошти, які зараховуються на рахунки **Військовослужбовця** від третіх осіб та використовуються для оплати азартних ігор можуть мати сумнівне походження.

Правоохоронним органом здійснюється досудове розслідування.



РОЗДІЛ 5.11. ВІДМИВАННЯ ДОХОДІВ ВІД ТОРГІВЛІ ЛЮДЬМИ ТА НАРКОТИЧНИМИ ЗАСОБАМИ

Торгівля людьми, втягнення в проституцію та торгівля наркотичними засобами – злочини, які мають вкрай негативний та масштабний вплив на різноманітні сфери життя суспільства (економічну, соціальну, демографічну тощо).

Така діяльність, як правило, входить до сфери впливу організованої злочинності та має міжнародний характер. Як показує практика, злочинні групи є високоорганізованими, мають ієрархічну структуру з чітким розподілом функцій та обов'язків, мають транснаціональний характер.

Відмивання злочинних доходів від торгівлі людьми та наркотичними засобами відбувається із залученням фінансових посередників та офшорних юрисдикцій, а також шляхом використанням сучасних платіжних технологій, криптовалют та інших віртуальних активів.

Частина коштів, отримана від незаконної діяльності, спрямовується на створення корумпованих зв'язків в державних органах.

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

Приклад 5.11.1. Легалізація (відмивання) доходів, ймовірно отриманих від торгівлі людьми

Держфінмоніторингом виявлено підозрілі фінансові операції, проведені по рахунках/платіжних картках, відкритих **Фізичною особою А** та **Фізичною особою Д**.

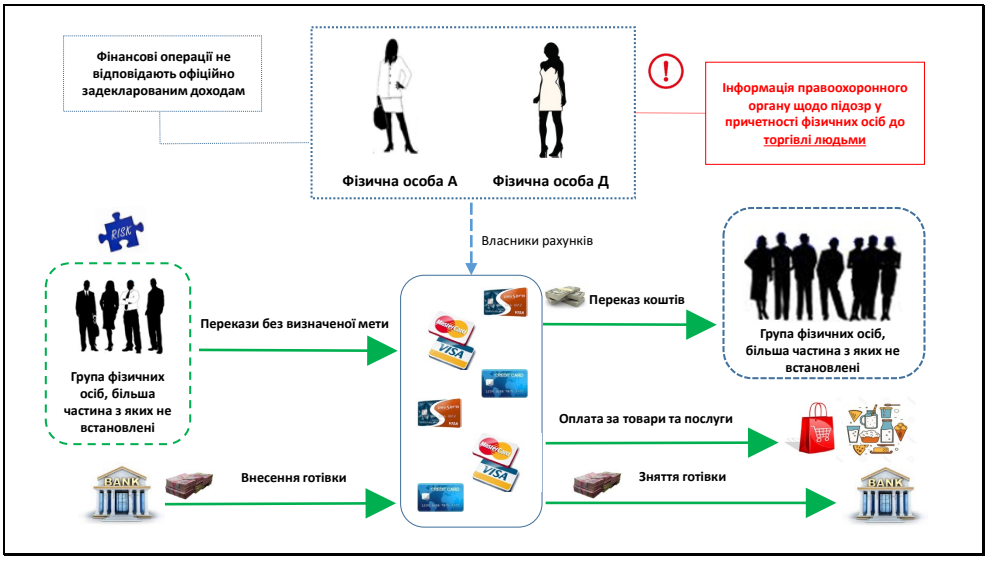
На рахунки кошти вносились готівкою, а також проводились багаторазові, у великих обсягах зарахування безготівкових коштів з невизначеними призначеннями платежів від значної кількості неідентифікованих фізичних осіб.

Надалі кошти з рахунків знімались готівкою, використовувались для придбання товарів та послуг, а також перераховувались на користь групи фізичних осіб, більша частина з яких не встановлені.

Обсяги фінансових операцій проведених по рахунках **Фізичних осіб А** та **Д** не відповідають обсягам отриманих ними доходів.

Привертає увагу наявна інформація від правоохоронного органу щодо підозр у причетності зазначених фізичних осіб до торгівлі людьми.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.11.2. Легалізація (відмивання) доходів, одержаних від торгівлі наркотиками

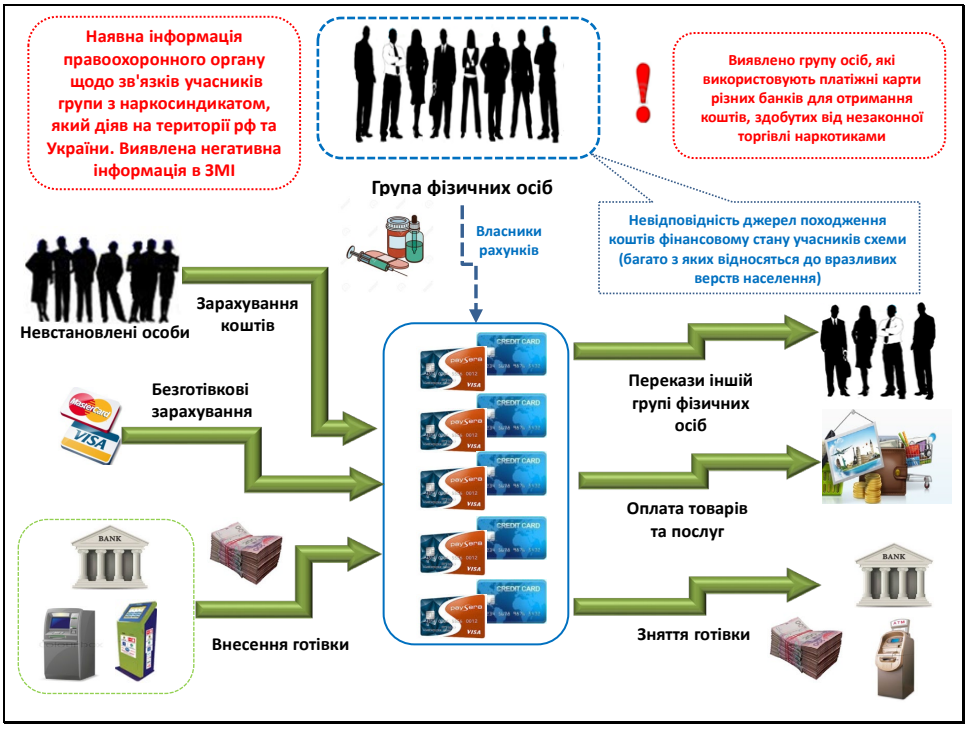
Держфінмоніторингом, з урахуванням інформації отриманої від правоохоронного органу, виявлено фінансові операції, пов'язані з акумулюванням коштів, отриманих від **групи невстановлених осіб** на карткових рахунках **Групи фізичних осіб**, відкритих у різних банках, що можуть бути пов'язані із вчиненням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

Так, по картах **Групи фізичних осіб** спостерігалося надходження значних сум коштів (як в готівковій формі, так і в безготівковій формі), спрямованих на отримання доходу від злочинної діяльності, ймовірно від прихованої діяльності. Надалі, кошти переважно перераховано іншій групі фізичних осіб, частково знято готівкою або списано як оплату за товари та за послуги.

Відносно **Групи фізичних осіб** наявна інформація правоохоронного органу щодо зв'язків з наркосиндикатом, який діяв на території росії та України. Щодо окремих осіб присутня негативна інформація в ЗМІ.

Враховуючи вищенаведене, у Держфінмоніторингу є підстави вважати фінансові операції, пов'язані із використанням рахунків/карток **Групи фізичних осіб**, такими, що спрямованні на вчинення злочинних дій, які стосуються торгівлі наркотиками та їх подальшої легалізації.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 5.11.3. Легалізація (відмивання) доходів, одержаних шляхом втягнення осіб в заняття проституцією

Держфінмоніторингом від правоохоронного органу отримано інформацію щодо проведення досудового розслідування відносно **Групи фізичних осіб**, які причетні до втягнення жінок в заняття проституцією.

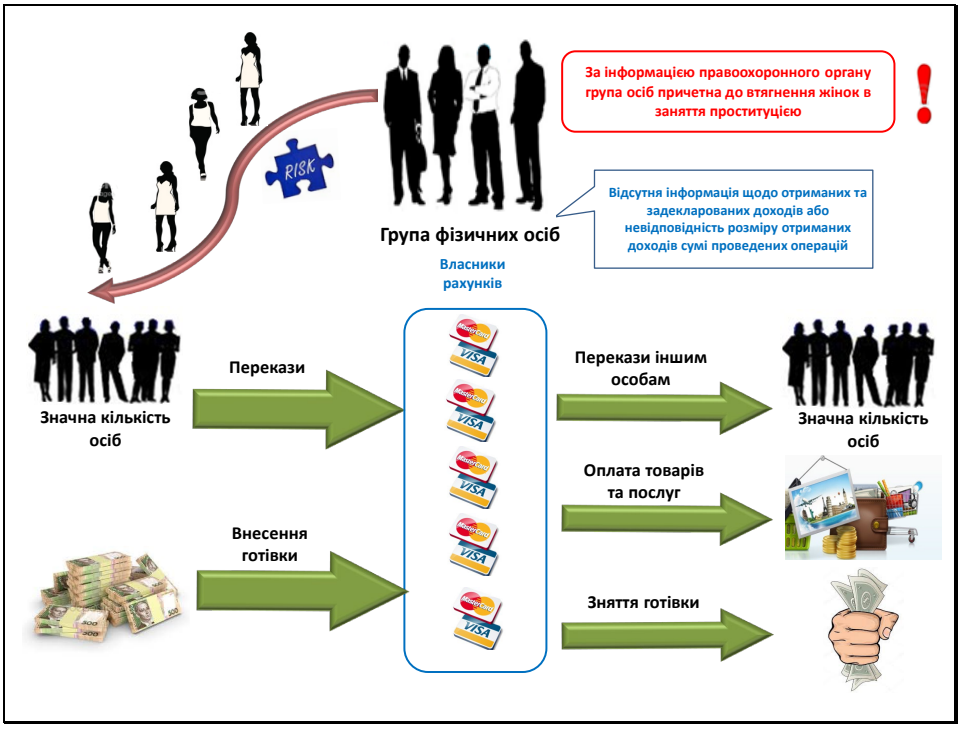
Держфінмоніторингом встановлено, що на карткові рахунки **Групи фізичних осіб** зараховувались безготівкові та готівкові кошти від значної кількості фізичних осіб.

Надалі, отримані кошти **Групою фізичних осіб** використовувались для придбання товарів/послуг, поповнення рахунків значної кількості інших осіб, переведення в готівку.

Фінансові операції **Групи фізичних осіб** мають ознаки приховування джерел походження коштів.

При цьому, щодо вищезазначеної **Групи фізичних осіб** відсутня інформація про отримання та декларування доходів або існує невідповідність розміру отриманих доходів сумі проведених ними операцій.

Правоохоронним органом здійснюється досудове розслідування.



РОЗДІЛ VI. ОСНОВНІ ІНСТРУМЕНТИ, ІНДИКАТОРИ ТА СПОСОБИ ЗЛОЧИНІВ ВІЙНИ ТА ВІДМИВАННЯ ЗЛОЧИННИХ ДОХОДІВ

Війна в Україні залишається найбільшим викликом та загрозою для країни в цілому так і для економіки.

В умовах триваючої війни та падіння економіки, населення та бізнес продовжують використовувати послуги, що надаються дистанційно та з використанням безконтактних засобів здійснення платежів.

Основними факторами трансформації злочинів під час війни залишається зміна умов життєдіяльності та пристосування до нового укладу життя. Наразі змінилось співвідношення видів злочинів, їх учасників та сфер, в яких вони вчиняються.

Збільшення міжнародної фінансової підтримки України призвело до збільшення інтересу злочинців до даного джерела коштів. Зростання сум природно призводить до збільшення кількості злочинів, особливо в умовах війни фінансові злочини завжди збільшуються.

Окреме важливе питання це видатки військового призначення. Доступність та унеможливлення повного контролю над видатками на оборону та обігом товарів військового спрямування спричиняє активізацію злочинності у цій сфері.

Зловживання у сфері благодійної діяльності залишається актуальним. Шахрайство на довірі населення прогресує в умовах війни. Активізація

вчинення кіберзлочинів, в тому числі кібертероризм, є характерними для воєнного стану.

Розуміння інструментів, індикаторів та способів вчинення злочинів сприятиме їх упередженню та виявленню.

6.1. Операції високого ризику

Серед основних груп операцій високого ризику, що можуть свідчити про ведення незаконної діяльності, можна виділити наступні:

а) **фінансування тероризму** – фінансування осіб, які організовують, забезпечують та провокують військову агресію з боку росії та білорусі;

б) **розкрадання державних коштів** – 100% передплата за оборонними контрактами та відсутність постачання, або постачання товарів низької якості чи іншої номенклатури;

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

г) **фіктивна благодійність** – збір коштів на неіснуючі благодійні програми та проєкти.

6.2. Основні ризикові фінансові операції та способи їх здійснення

Серед ідентифікованих схем злочинної діяльності можливо виділити наступні ризикові фінансові операції та способи їх здійснення:

- фінансування 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;
- здійснення готівкових операцій на тимчасово окупованих територіях через банківські термінали, які обліковуються за підприємцями, що зареєстровані на території, підконтрольній Україні;
- значні перерахування від великої кількості осіб (з тимчасово окупованих територій) на карткові рахунки однієї особи, з ймовірним незаконним обміном української валюти на російські рублі;
- розрахунки за імпортовані товари російського походження через треті країни в обхід національних та міжнародних фінансових обмежень;
- перерахування коштів за оборонну продукцію на користь сумнівних компаній-нерезидентів, які ніколи не займались товарами військового призначення;
- привласнення бюджетних коштів шляхом підробки документів щодо якості товарів, та постачання на державне підприємство засобів захисту нижчої категорії;
- перерахування коштів від державних підприємств та бюджетних організацій на користь юридичних осіб, які не є виробниками відповідної продукції, з метою завищення вартості контракту;

- перерахування бюджетних коштів на користь новостворених фізичних осіб – суб'єктів підприємницької діяльності призначення яких не відповідає їх профілю діяльності;
- участь фізичних осіб – суб'єктів підприємницької діяльності, які пов'язані родинними зв'язками з профільним чиновником державної установи, в розрахунках за державними контрактами;
- заволодіння коштами державного підприємства шляхом незаконного оформлення правочину;
- залучення у схеми розрахунків з бюджетними коштами юридичних осіб, які надають послуги «зустрічних потоків», «скруток» та «прихованого» обготівковування;
- придбання дороговартісних активів та здійснення значних готівкових/безготівкових операцій ТОП-військовопосадовцями, народними депутатами України, іншими національними публічними діячами та особами, пов'язаними з ними через корупційні доходи;
- збір грошової допомоги через благодійні фонди/неприбуткові організації та приватних осіб під «фейкові» благодійні проєкти (підтримка ЗСУ, лікування військових та дітей тощо);
- фінансові операції благодійних фондів та громадських організацій, не відповідає їх профілю діяльності;
- оформлення фіктивних зовнішньоекономічних контрактів з експорту зернових та не повернення валютної виручки;
- перерахування валюти за межі України без фактичного постачання товарів;
- заволодіння коштами компанії-нерезидента з подальшим придбанням коштовної елітної нерухомості;
- проведення готівкових операцій від здійснення прихованої (не зареєстрованої) підприємницької діяльності;
- викрадення коштів через кібератаку за допомогою шкідливого програмного забезпечення;
- шахрайське заволодіння коштами фізичних осіб з використанням методу соціальної інженерії – «вішинг»;
- шахрайство з коштами фізичних осіб, отриманих у вигляді допомоги родинам загиблих та безвісти зниклих військових, а також коштами для виплат окремим групам осіб постраждалих від війни;
- шахрайське заволодіння коштами фізичних осіб від псевдо «інвестування»;
- співпраця криптовалютної біржі України з криптовалютними біржами росії в обхід обмежень та санкцій;
- необґрунтовано велика кількість вхідних платежів фізичних осіб та переказ на купівлю криптоактивів;

- фінансування незаконних воєнізованих угрупувань через криптовалюту;
- зарахування коштів сумнівного походження на користь суб'єктів грального бізнесу;
- маніпуляції банківськими системами для приховування реального походження платежів (міскодинг);
- надходження готівкових коштів від торгівлі наркотиками та проституції;
- незаконне заволодіння та переміщення культурних цінностей за межі України;
- відмивання коштів, отриманих від реалізації предметів культурної спадщини.

6.3. Основні інструменти у виявлених схемах відмивання злочинних доходів

За результатами дослідження встановлено наступні основні інструменти, що використовувались у типових схемах відмивання злочинних доходів:

- відсутність постачання при 100% передоплаті;
- підміна (заміна) номенклатури товарів;
- використання підроблених документів;
- завищення/заниження вартості товарів/робіт/послуг;
- залучення фіктивних суб'єктів господарювання та компаній-нерезидентів;
- залучення пов'язаних фізичних осіб-суб'єктів підприємницької діяльності;
- незаконні правочини;
- оплата брокерських послуг;
- здійснення транзитних операцій;
- використання «скруток» та «зустрічних потоків»;
- використання «міскодингу»;
- придбання коштовних елітних активів;
- використання підставних осіб;
- використання готівки;
- відступлення прав вимог;
- надання/повернення фінансової допомоги;
- використання третіх країн для розрахунків з росією;
- неповернення валютної виручки;
- використання суб'єктів грального бізнесу;
- використання торговельних операцій для відмивання коштів;
- надання незаконних послуг через професійні мережі з відмивання коштів;
- операції з криптовалютою;
- використання шкідливих програм;

- викрадення даних;
- злом акаунтів користувачів;
- соціальна інженерія.

6.4. Індикатори підозрілості учасників

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

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 рахунків українських виробників сільськогосподарської продукції, виробничі потужності яких знаходяться на окупованих територіях;
- клієнтом є НПО, яка збирає пожертви та перераховує їх одним і тим же особам або іншим НПО;
- особи, що переміщують валютні кошти за нетиповими маршрутами та з непідтверджених джерел;

Санкції

- щодо особи прийнято рішення про застосування санкцій;
- особа сприяє обходу санкційного режиму;

Релігійні організації

- причетність до релігійної організації що пропагандує російські наративи;

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 статутом (малозабезпечені, жебраки) або молодого віку (до 20 років) або похилого (після 75 років);
- фізичні особи проживають на тимчасово окупованих територіях;
- виробничі потужності знаходяться на тимчасово окупованій території;

КБВ, посадові особи

- невідповідність КБВ;
- неможливість визначення реального КБВ внаслідок складної структури власності;
- номінальні власники;
- фізичні особи є кінцевими бенефіціарними власниками чи входять до посадово-засновницького складу великої кількості юридичних осіб;
- засновником/керівником є особа, яка належить до соціально вразливих верств населення (студенти, пенсіонери, особи, які отримують соціальну допомогу тощо), особи зі спеціальним статутом (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;
- 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;

Господарська діяльність учасника

- новостворений суб'єкт підприємницької діяльності;
- незначний статутний капітал;
- відсутність найманих працівників або незначна кількість працівників;
- юридична особа часто здійснює зміну назви або засновницько-посадовий склад;
- відсутність основних засобів, виробничих потужностей, складських приміщень та інших активів;
- ліквідація суб'єкта господарювання одразу після здійснення платежу;
- не є виробником товарів;
- відсутність ліцензій/дозволів на окремі види діяльності;
- відсутність орендних платежів;
- реєстрація за місцем масової реєстрації;
- наявність значної кількості рахунків в різних банківських установах;

Кримінальна історія

- клієнт або його контрагенти є фігурантами кримінальних проваджень;

Негативна інформація щодо учасника

- щодо особи отримано звернення від фізичних та юридичних осіб, фінансових посередників та 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;

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;

Тендер

- у більшості тендерних закупівлях (в аукціонах) беруть участь пов'язані між собою учасники;
- надання особою права користування рахунком третім особам для проведення сумнівних операцій.

6.5. Індикатори підозрілості фінансових операцій (діяльності)

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

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;
- операції з ресурсами, що походять з окупованих територій (корисні копалини, руда, зерно тощо);
- транскордонні перекази до країни, про яку відомо, що вона підтримує (є нейтральною) збройну агресію росії;

Загальні індикатори

- значні суми перерахувань за надані послуги, вартість яких важко оцінити;
- 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;

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;
- тривалий час значний залишок коштів на рахунку, що сформований за рахунок бюджетних грошей;

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 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);

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»;
- коригування дій учасників фінансових операцій («фіктивних» учасників) з єдиного центру прийняття рішення;

ФО з фіктивними іноземними компаніями

- наявні ознаки «фіктивності» іноземної компанії;
- 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 карткових рахунків;

- проведення необґрунтовано великої кількості операцій чи на значні суми між фізичною особою та суб'єктами грального бізнесу;
- здійснення операцій з готівкою, обсяг яких не відповідає офіційно задекларованим доходам;

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;

Шахрайство

- фінансові операції клієнта пов'язані з шахрайством;

Криптовалюта

- фінансові операції клієнта з придбання криптовалюти мають сумнівне джерело походження.

6.6. Найпоширеніші способи легалізації (відмивання) злочинних доходів

За результатами дослідження встановлено наступні основні способи легалізації (відмивання) злочинних доходів та фінансування тероризму (сепаратизму):

Бюджет

- 100% передоплата за оборонними контрактами, без фактичного постачання товарів, з подальшим виведенням на сумнівні компанії-нерезиденти та власні депозити;
- перерахування коштів за оборонну продукцію на користь сумнівних компаній-нерезидентів, які ніколи не займались товарами військового призначення;
- транзитний характер перерахувань бюджетних коштів за підробленими документами;
- перерахування коштів державних підприємств та бюджетних організацій через ланцюг суб'єктів господарювання, які не є виробниками відповідної продукції, з метою завищення вартості товарів;
- перерахування бюджетних коштів на користь новостворених фізичних осіб – суб'єктів підприємницької діяльності призначення яких не відповідає їх профілю діяльності, з метою подальшого обготівковування;
- участь фізичних осіб – суб'єктів підприємницької діяльності, які пов'язані родинними зв'язками з профільним чиновником державної установи, в розрахунках за державними контрактами, з подальшим обготівковуванням;

- примусове списання коштів з рахунків державного підприємства шляхом незаконного оформлення правочину, з подальшим перерахуванням за кордон;
- перерахування бюджетних коштів на користь осіб які надають «послуги» з відмивання коштів та сприяння від ухилення від сплати податків через механізм «зустрічних потоків» та «скруток» з подальшим обготівковуванням;

Корупція

- придбання дороговартістних активів, здійснення значних готівкових операцій ТОП-високопосадовцями або афільованими з ними особами за рахунок коштів з непідтверджених джерел;

Готівка

- кеш-кур'єри;
- внесення готівкових коштів з використанням декількох рахунків у різних банківських установах та наданням одних і тих же документів та інформації про власні доходи для підтвердження джерела походження коштів;
- зарахування коштів на користь фізичних осіб та фізичних осіб-суб'єктів підприємницької діяльності з подальшим обготівковуванням;
- надання послуг з обготівковування на тимчасово окупованій території України;

Благодійна діяльність

- збір благодійних внесків на користь Благодійного фонду, з подальшим виведенням на пов'язаних осіб фонду;
- збір коштів на карткові рахунки фізичних осіб, з подальшим використанням на власні потреби (обготівковування, онлайн-казино, готелі, ресторани);
- перерахування коштів Благодійним фондом на рахунок компанії-нерезидента за продукцію оборонного призначення, і яка не була поставлена;
- перерахування коштів Благодійного фонду на користь компаній з ознаками фіктивності, з подальшим виведенням на користь компаній, що надають послуги з «прихованого обготівковування»;

ЗЕД

- здійснення експортних операцій без повернення валютної виручки;
- виведення коштів на користь сумнівних нерезидентів, які не мають відповідних ресурсів (працівників, приміщення та обладнання) для виконання умов контракту;

Шахрайство

- заволодіння коштами через некоректну роботу інтернет платформ з подальшим виведенням за кордон;
- викрадення коштів за допомогою шкідливого програмного забезпечення;

- заволодіння коштами фізичних осіб з використанням методу соціальної інженерії – «вішинг»;
- заволодіння коштами фізичної особи шляхом злому сторінки в соціальній мережі;
- заволодіння коштами померлих громадян;
- заволодіння коштами фізичних осіб під виглядом інвестицій в криптопроєкт;
- шахрайство з коштами фізичних осіб, шляхом викрадання даних;
- введення в оману фізичних осіб з метою здійснення «інвестицій» у фінансову піраміду;

Культурні цінності

- легалізація коштів від незаконного переміщення та реалізації культурних цінностей;

Наркотичні речовини та проституція

- використання карткових рахунків соціально вразливих верств населення для проведення фінансових операцій з коштами, здобутих від незаконного обігу наркотичних (психотропних) речовин та торгівлі людьми;

Гральні заклади

- приховування доходів від діяльності віртуальних гральних закладів.

6.7. Найпоширеніші способи фінансування війни та тероризму

До найпоширеніших методів фінансування війни та тероризму (сепаратизму) можливо віднести наступні:

Готівка

- добровільна передача власних готівкових коштів фізичними особами представникам терористичних та/або сепаратистських організацій;
- використання фіктивних фінансових структур для отримання готівкових коштів;
- використання банкоматів для зняття коштів з банківських рахунків третіх осіб;
- використання пошкоджених купюр в терміналах самообслуговування, з метою отримання готівки через банкомати;

Картки

- перерахування коштів на карткові рахунки членів терористичних угрупувань та осіб, які організовують, забезпечують та провокують військову агресію з боку росії;
- фінансування тероризму та колабораційної діяльності шляхом значної кількості переказів по карткових рахунках соціально вразливих фізичних осіб ;
- використання дебетових карток;

Окупована територія

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

НПО

- перерахування благодійних внесків на користь Благодійних організацій, які мають проросійську позицію або пропагують російські наративи;
- фінансування релігійних організацій, що пропагують «руський мір»;

Обхід санкцій

- незаконне постачання товарів до росії через дружні до росії країни в обхід міжнародних та вітчизняних санкцій;
- діяльність постачальників послуг, пов'язаних з обігом віртуальних валют, що співпрацюють з криптобіржами та Даркнет-майданчиками росії;

ЗЕД

- здійснення міжнародних постачань з подальшим розрахунком на території інших країн;
- незаконний експорт сировини на користь підприємств росії через іноземну компанію, зареєстровану на території Євросоюзу;

Активи

- переєстрація підприємств, які знаходяться на тимчасово окупованій території за законодавством росії;
- надання у власність/користування активів, окупаційній «владі»;

Прямі злочини

- вчинення грабежів, розбоїв, викрадення людей з метою отримання грошових коштів за їх викуп;

Підробка документів

- списання коштів з рахунків фізичних осіб, які знаходяться на тимчасово окупованій території, та співпрацюють з окупаційною владою, на підставі підробних документів;

Криптовалюта

- використання криптовалюти для фінансування тероризму та колабораціонізму.

ВИСНОВОК

З метою зменшення вразливостей щодо легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансування тероризму та/або фінансування розповсюдження зброї масового знищення, або вчинення іншого кримінального правопорушення або діяння, фінансова система має сконцентруватись на підвищенні рівня виявлення, блокування фінансових операцій та діяльності причетних до цього осіб.

Активізація організованих злочинних груп в умовах війни є одним із найактуальніших викликів сьогодення.

Злочинці продовжують удосконалювати свою майстерність у схемах ВК/ФТ/ФРЗМЗ. Продовжується глобалізація процесів, оскільки постійно виникає потреба у зростанні фінансування окупаційних військ, терористичних угруповань, поширення сепаратистських ідей та пропаганди.

Фінансові інструменти для вчинення цих злочинів мають все більш витончений та складний характер.

Актуальними залишаються злочини війни та їх фінансування, а також суміжні з ними злочини.

Все це створює умови для послаблення економіки України. Отже, завданням системи ПВК/ФТ/ФРЗМЗ є запобігання та протидія здійсненню злочинів, що генерують кримінальні доходи.

Дієвим інструментом виявлення таких злочинів є дане типологічне дослідження.

Результати типологічного дослідження мають практичну складову та можуть бути використані в ході кримінальних розслідувань, оцінки бізнес-ризиків, клієнтських та технологічних ризиків, а також виконання поточного моніторингу на всіх стадіях обслуговування клієнта, та побудови заходів регуляторного впливу.

Також, типології можуть бути використані для розробки стратегій та планів з ПВК/ФТ/ФРЗМЗ та внесення змін до законодавства.

ДОДАТОК. АНАЛІТИЧНІ ІНСТРУМЕНТИ ДЛЯ КОНТРОЛЮ ТА МОНІТОРИНГУ

1. АНАЛІТИЧНІ ІНСТРУМЕНТИ

У своїй діяльності суб'єкти для здійснення первинного фінансового моніторингу використовують наступні джерела інформації:

- дані з державних реєстрів;
- дані з відкритих публічних джерел;
- публічні та адресні повідомлення правоохоронних органів;
- онлайн-сервіси перевірки компаній;
- результати журналістських розслідувань;
- офіційні документи Держфінмоніторингу та суб'єктів державного фінансового моніторингу тощо.

З метою проведення належної перевірки клієнта на етапі встановлення ділових відносин, а також більш детального поглибленого аналізу протягом обслуговування задля моніторингу фінансових операцій клієнтів суб'єкти первинного фінансового моніторингу також використовують:

- власні скорингові моделі задля запобігання встановлення ділових відносин із клієнтами, що мають ознаки сумнівності;
- власні скорингові моделі оцінки ризику ділових відносин з клієнтом відповідно до типу клієнта (юридична особа, фізична особа, фізична особа-підприємець);
- розроблені матриці розрахунку рівня ризику публічних осіб;
- скринінгові моделі виявлення потенційно високоризикових клієнтів;
- різноманітні звіти та власні сценарії відбору підозрілих фінансових операцій (діяльності).

Суб'єкти первинного фінансового моніторингу з метою виявлення підозрілих фінансових операцій створюють відповідні правила відбору операцій за наступними полями: дата здійснення операцій, призначення платежу, сума, рівень ризику, країна, інформація щодо типу рахунку тощо.

Також, такі суб'єкти здійснюють сценарний аналіз, що включає дослідження обігу активів в цілому та окремих фінансових операцій клієнтів в динаміці.

Суб'єкти первинного фінансового моніторингу додають до власних аналітичних систем додаткову інформацію щодо учасників операцій та іншу інформацію, яка може значно розширити перелік даних для аналізу.

Виявлення фінансових операцій, що підлягають фінансовому моніторингу, з використанням автоматизованих систем, які включають, зокрема, аналіз критеріїв ризику та індикаторів підозрілості фінансових операцій, є дуже важливим для виконання завдань суб'єктом первинного фінансового моніторингу.

Приклад реквізитів для встановлення сценарію відбору підозрілих фінансових операцій (діяльності)

Щодо профілю клієнта:

- країна реєстрація клієнта;
- розмір статутного капіталу суб'єкта господарювання;
- вид діяльності суб'єкта господарювання;
- кількість працівників суб'єкта господарювання;
- розмір доходів та сплачені податки суб'єкта господарювання;
- період діяльності юридичної особи/вік фізичної особи;
- інформація про кінцевого бенефіціарного власника, посадово-засновницький склад суб'єкта господарювання та їх участь в інших юридичних особах (резидентність);
- наявність зв'язків з країнами, які причетні до військової агресії проти України;
- інформація про зміни кінцевого бенефіціарного власника та посадово-засновницького складу суб'єкта господарювання;
- 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;
- наявність виробничих потужностей/торговельно-складських приміщень, інших активів, необхідних для ведення задекларованої господарської діяльності суб'єкта господарювання;
- потенційна сума (оборот) коштів, що може бути використаний суб'єктом господарювання за допомогою послуги (продукту).

Щодо фінансових операцій клієнта:

- кількість рахунків або платіжних карток суб'єкта господарювання;
- порівняння щодо обсягу дебетових та кредитових фінансових операцій за рахунком суб'єкта господарювання протягом одного дня/періоду;
- наявність змін в обсягах фінансових операцій, що здійснюються за рахунками клієнта суб'єкта господарювання;
- характер проведених фінансових операцій;
- інформація щодо використання сейфа клієнтом;
- IP-адреси для здійснення фінансових операцій клієнтом.

З метою виявлення фінансових операцій, що можуть бути пов'язані з ВК/ФТ/ФРЗМЗ більшість суб'єктів первинного фінансового моніторингу використовують програмні комплекси, які за відповідними алгоритмами (сценаріями) відбирають фінансові операції клієнтів.

Наприклад: значний відсоток готівки/фінансової допомоги в обороті, новостворений клієнт зі значним оборотом, новий клієнт для суб'єкта первинного фінансового моніторингу зі значним оборотом тощо.

Програмні комплекси для проведення фінансового моніторингу

B2:FinMon https://csltd.com.ua	Система фінансового моніторингу B2:FinMon призначена для автоматизації процесів в банку, пов'язаних із запобіганням фінансування терористичної діяльності та протидією легалізації доходів, отриманих злочинним шляхом.
АБС SCROOGE https://lime-systems.com	Система АБС Scrooge оптимізує роботу корпоративного і роздрібного бізнесу, казначейського управління, бухгалтерії банку, департаменту ризиків, фінансового моніторингу, автоматизує процес подання банківських звітів для регулятора, як за національними, так і за міжнародними стандартами фінансової звітності.
САБ SrBank https://soft-review.com.ua	САБ SrBank представлена двома основними рівнями в реалізації системи, перша частина відповідає за фронт-офісне обслуговування клієнтів та організацію цифрових каналів продажів, друга частина – це комплекс завдань з бек-офісного обслуговування, з виконанням регламентів, формуванням XML звітності на регуляторів, проведенням фінансового моніторингу, аналізу ризиків, контролю лімітів тощо.
AML.point https://aifintech.ua	AML.Point – це комплексне SaaS-рішення, яке інтегрується з обліковими системами для виконання вимог законодавства з фінмоніторингу «під ключ».

Зазначений перелік програмних рішень не є вичерпним чи остаточним та може бути розширений в залежності від розвитку ринку IT-продуктів в Україні для фінансового моніторингу.

Програмні рішення повинні допомогти забезпечувати своєчасне та в повному обсязі виконання обов'язків суб'єктами первинного фінансового моніторингу. Системи автоматизації сприяють функціонуванню належної системи управління ризиками ВК/ФТ/ФРЗМЗ.

2. ПУБЛІЧНІ ІНФОРМАЦІЙНІ РЕСУРСИ КОНТРОЛЮЮЧИХ (ДЕРЖАВНИХ) ОРГАНІВ ТА ПРИВАТНИХ ОРГАНІЗАЦІЙ

Використання автоматизованих процедур збирання та аналітичної обробки інформації з відкритих джерел є важливим кроком для підтримки прийняття управлінських рішень, підвищення рівня ПВК/ФТ/ФРЗМЗ.

Одержання додаткової інформації з публічних інформаційних ресурсів контролюючих (державних) органів та приватних організацій є важливим кроком для аналізу схем ВК/ФТ/ФРЗМЗ.

Базовим напрямком збору інформації залишається використання пошукових систем (Google та інші, такі як Bing і DuckDuckGo).

Звичайно, спрощує пошук інформації використання методик використання таких систем (застосування спеціальні пошукові оператори або функції) та розроблених спеціальних плагінів до таких систем). Ціль використання систем це отримати найбільш релевантні результати.

Держфінмоніторинг систематично проводить роботу щодо виявлення публічних інформаційних джерел для отримання додаткової інформації.

Деякі корисні посилання наведені у типологічних дослідженнях Держфінмоніторингу за минулі періоди. Корисні посилання зазначаються відповідно до тематики дослідження.

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.

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

Офіс Генерального прокурора України	**Список підозрюваних магістральної справи «24 лютого»**
https://gp.gov.ua/detectable	«Магістральна» кримінальна справа щодо повномасштабного вторгнення РФ в Україну.

Служба безпеки України	Розшук осіб, які звинувачуються у вчиненні злочинів проти основ національної безпеки.
https://ssu.gov.ua/u-rozshuku	

Реєстр російських воєнних злочинців	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.
https://rwc.shtab.net/	

Рух ЧЕСНО	**Реєстр зрадників** 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.
https://www.chesno.org	

2.2. Списки РБ ООН

	Зведений список Ради Безпеки ООН

Рада Безпеки ООН	Зведений перелік фізичних і юридичних осіб, до яких застосовуються заходи, введені Радою Безпеки ООН.
https://www.un.org/securitycouncil/content/un-sc-consolidated-list https://scsanctions.un.org/search/	

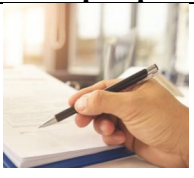
2.3. Дані щодо фізичних осіб

	**Дані щодо фізичних осіб**

http://wanted.mvs.gov.ua/searchperson https://data.gov.ua/dataset/7c51c4a0-104b-4540-a166-e9fc58485c1b	**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.

https://sis.nipo.gov.ua/uk/search/simple	Сервіс дозволяє здійснювати пошук відомостей про об'єкти промислової власності. API CIC створено для зручного вивантаження інформації щодо об'єктів промислової власності у форматі JSON та подальшого формування власних баз даних, аналізу даних, статистики тощо. Пошук здійснюється за даними заявника, винахідника, власника, представника.
YouControl https://youcontrol.com.ua	Система YouControl містить максимально повну інформацію про зв'язки контрагента (та пов'язаних з ним осіб) із національними публічними діячами. У спеціальній вкладці можна побачити перелік персон і подробиці про типи зв'язків і статуси.
Опендатабот https://opendatabot.ua	Реєстр національних публічних діячів (ПЕП) України сформований Опендатабот.

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://wanted.mvs.gov.ua/passport	Інформація про викрадені/втрачені/ недійсні паспорти громадян України.

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.

Національне агентство із питань запобігання корупції	**Портал «Війна і санкції»**
WAR & SANCTIONS https://sanctions.nazk.gov.ua	Портал створено Національним агентством із питань запобігання корупції та Міністерством закордонних справ України. Портал дозволяє поінформувати іноземні уряди та громадян про вже запроваджені санкції, залучити громадськість до глобальної кампанії із розширення санкційних списків щодо осіб, які підтримують війну, зокрема фінансово та інформаційно.

Міністерство фінансів США	
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	OFAC публікує список осіб і компаній, які належать, контролюються або діють за чи від імені цільових країн. Санкції, пов'язані з Україною та РФ. 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.

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
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	

ЄС розширив санкції у відповідь на визнання непідконтрольних уряду територій Донецької та Луганської «областей» України та введення російських збройних сил у ці райони.

Після 24 лютого 2022 року ЄС масово розширив санкції у відповідь на військову агресію росії проти України. Санкції введено з метою послабити економічну базу росії, позбавити її критичних технологій, ринків та суттєво обмежити її здатність вести війну.

Паралельно розширено режим санкцій ЄС щодо білорусі у відповідь на причетність країни до агресії росії проти України.

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**

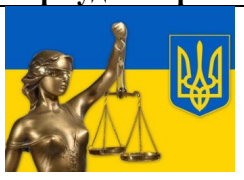
Реєстри Міністерства юстиції України	Оприлюднені дані з Єдиних та Державних реєстрів, що створюються відповідно до законодавства України.
https://nais.gov.ua/registers	
https://minjust.gov.ua/uniform_and_registry	Інформація про Єдині та державні реєстри.

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  https://reyestr.court.gov.ua/	Єдиний державний реєстр судових рішень.

Стан розгляду справ	
 https://court.gov.ua/fair/	Інформація щодо стадій розгляду судових справ.

2.9. Компанії, зареєстровані в України

Реєстраційні дані щодо компаній України	
Інтернет адреси https://youcontrol.com.ua https://opendatabot.ua https://finap.com.ua https://vkursi.pro https://ca.ligazakon.net https://clarity-project.info	Актуальні відомості та інформація щодо діяльності та даних суб'єктів господарювання, зареєстрованих в Україні.

Компанії, що мають власників з росії

Інтернет адреси	
YouControl https://youcontrol.com.ua/	YouControl містить експрес-аналіз зв'язків з агресором. У систему додано найбільш повним список діючих українських компаній (та пов'язаних з ними осіб), що мають прямі або приховані зв'язки з агресором (понад 20 тисяч). «Експрес-аналіз» YouControl містить унікальні фактори, націлені на миттєве виявлення у діяльності контрагентів зв'язків з росією, білоруссю, країнами, які надають зброю росії та/або підтримують її.

Інтернет адреси	
Опендатабот https://opendatabot.ua/open/russian-federation-business	Список компаній, які станом на 24 лютого 2022 року мали власника або бенефіціара з росії. Перевірка компанії на предмет російських засновників - є важливою процедурою перед укладанням будь-яких правовідносин. Для перевірки компанії введіть її назву або код ЄДРПОУ в Опендатабот – за наявності російських власників даний фактор буде відмічений у картці компанії.

2.10. Компанії, зареєстровані в Європейському Союзі

https://e-justice.europa.eu/content_find_a_company-489-en.do	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.

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/38576/EN/ beneficial_ownership_registers__search_for_beneficial_ownership_information

2.11. Компанії, зареєстровані в іноземних юрисдикціях

Інформаційні ресурси щодо 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	

YoucontrolWorld	Система для пошуку зв'язків між компаніями, побудови та візуалізації ділових зв'язків між компаніями та особами з інших країн.
YC World	
https://youcontrol.world	

https://www.occrp.org	**Центр з дослідження корупції та організованої злочинності**

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.

https://offshoreleaks.icij.org	**База даних офшорних витоків** База містить інформацію щодо офшорних компаній, фондів і трастів із розслідувань Pandora Papers, Paradise Papers, Bahamas Leaks, Panama Papers та Offshore Leaks.

https://riskcenter.dowjones.com	Рішення з управління ризиками та комплаєнсу. Ресурс для перевірки структури власності.

Dato Capital	Онлайн база про компанії та їх директорів.
en.datocapital.com	
База містить інформацію про компанії зареєстрованих в Нідерландах, Великій Британії, Гібралтарі, Іспанії, Панамі, Каймановых Островах, Люксембурзі, Британських Віргінських Островах, Мальті, Кюрасао.	

Bureau van Dijk Electronic Publishing	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.
https://www.bvdinfo.com	

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,	https://www.gov.uk/search-property-information-land-registry

Регіон (країна)	Опис	Адреса
	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/).	
Велика Британія	Інтерактивна мапа та база даних власників іноземних компаній.	http://www.private-eye.co.uk/registry
Велика Британія	У Великій Британії поліція має право встановлювати право власності на транспортний засіб через Національну базу даних поліції (Police National Database – PND). Державне агентство Великої Британії з реєстрації транспортних засобів і видачі посвідчень водія (UK Driver and Vehicle Licensing Agency – 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	У цій реєстраційній базі Сполученого Королівства	https://beta.companieshouse.gov.uk/

Регіон (країна)	Опис	Адреса
Північна Ірландія	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.	
Естонія	Безкоштовно: назва та організаційно-правова форма компанії, реєстраційний номер компанії, юридична адреса, розмір статутного капіталу, дата реєстрації та затвердження уставу, активна/неактивна, дати подання звітності до реєстру.	https://ariregister.rik.ee/lihtparing
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

Якщо суб'єкт пошуку займається транспортуванням або торгівлею товарами, такі бази даних можуть стати місцем для отримання даних про міжнародні поставки.

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.
ImportKey https://importkey.com/	

2.13. Відстеження літаків

	Літаки можна відстежувати за допомогою онлайн ресурсів. Аеродроми, куди та з яких летять літаки, можуть вказувати на розташування будинку для відпочинку неподалік.

Найпомітнішим ідентифікатором літака є його хвостовий номер, але літак може змінити своє «ім'я», і тоді його серійний номер (який ніколи не змінюється) є життєво важливим для ідентифікації його нового хвостового номера та продовження відстеження його переміщень.

Повітряне судно	База даних реєстрації повітряних суден.
http://www.airframes.org	

Повітряне судно	Бази фотографій повітряних суден.
https://www.planespotters.net https://www.jetphotos.com	

Відстеження польотів	Глобальна служба відстеження польотів, яка надає інформацію про літальні апарати у всьому світі в режимі реального часу.
https://www.flightradar24.com https://globe.adsbexchange.com https://www.radarbox.com https://www.flightaware.com/	

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://sanctions.nazk.gov.ua/osint/index	Osint-Трекер – іноземні реєстри та бази даних для пошуку активів підсанкційних осіб.
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/resurs/poisk-dannyh-o-korporaciah-i-ih-vladelcah/	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 (Paradise Papers, Panama Papers, Transborder corruption archive, 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
Financial Times	Почали стежити за найближчим оточенням керівництва росії та заможними олігархами.	https://www.ft.com
Wall Street Journal	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.