2025

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

Державна служба фінансового моніторингу України

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

Основним завданням Держфінмоніторингу є збір, обробка та аналіз фінансової інформації, зокрема щодо операцій, пов'язаних із відмиванням коштів, фінансуванням тероризму та фінансуванням розповсюдження зброї масового знищення.

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

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

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

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

ЗАТВЕРДЖЕНО
Наказ Державної служби
фінансового моніторингу України
22.12.2025 № 116

Типологічне дослідження на тему:
«Ризики та загрози легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансування тероризму в умовах військової агресії російської федерації – 2025»

Російська агресія проти України спричинила зростання нелегальних фінансових потоків і посилила загрози фінансовій безпеці. Війна продовжує підривати глобальну фінансову стабільність, посилює вразливість населення та ускладнює фінансовий моніторинг, створюючи сприятливе середовище для приховування злочинних доходів, розширення тіньової економіки та обходу санкцій.

У зв’язку з цим актуалізовано типологічне дослідження, що розкриває сучасні схеми відмивання коштів і фінансування тероризму в умовах війни, а також методи, інструменти й індикатори підозрілості.

У сфері фінансового моніторингу ризик-орієнтований підхід є ключовим інструментом для виявлення підозрілих операцій, формування обґрунтованих підозр щодо фінансових злочинів і розробки ефективних заходів запобігання та протидії їм.

Типологічне дослідження є важливим документом для виявлення та протидії злочинам, характерним у воєнний період. Типологічне дослідження може стати підґрунтям для ідентифікації та протидії поширенню злочинів, що можуть бути характерними під час війни. Дане дослідження також може бути корисним при здійсненні нагляду та внесенні змін до законодавства.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

Держфінмоніторинг	Державна служба фінансового моніторингу України
ВК	легалізація (відмивання) доходів, одержаних злочинним шляхом
ВК/ФТ/ФРЗМЗ	легалізація (відмивання) доходів, одержаних злочинним шляхом, фінансування тероризму та фінансування розповсюдження зброї масового знищення
ПВК/ФТ/ФРЗМЗ	протидія легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансування розповсюдження зброї масового знищення
КБВ	кінцевий бенефіціарний власник
КК України	Кримінальний кодекс України
НПО	неприбуткові організації
ПФР	підрозділ фінансової розвідки
білорусь (рб)	республіка білорусь
росія (рф)	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
OSINT	Аналіз інформації з відкритих джерел (Open Source Intelligence)

ВСТУП

Збройна агресія російської федерації проти України спричинила не лише масштабні безпекові та гуманітарні виклики, але й серйозні загрози для фінансової стабільності як на національному, так і на міжнародному рівнях. Війна трансформувала характер ризиків у сфері відмивання коштів, фінансування тероризму та розповсюдження зброї масового знищення, зробивши їх більш прихованими, технологічними та багатоканальними.

В умовах стрімкого зростання нелегальних фінансових потоків, поширення гібридних загроз і ускладнення фінансового моніторингу актуальним стало формування повної, достовірної та аналітично обґрунтованої карти ризиків. Типологічне дослідження Держфінмоніторингу за 2025 рік є відповіддю на новітні виклики й покликане виявити сучасні схеми легалізації злочинних доходів, механізми фінансування терористичної діяльності, а також способи обходу санкцій, що використовуються в умовах повномасштабної війни.

Дослідження базується на матеріалах, наданих суб'єктами фінансового моніторингу, правоохоронними та розвідувальними органами, а також на публікаціях авторитетних міжнародних структур – FATF, MONEYVAL, Європолу, Egmont Group, МВФ, Світового банку, Basel Institute та інших.

У фокусі дослідження – найбільш актуальні схеми фінансування тероризму та відмивання коштів як складові фінансування війни. Проаналізовано способи обходу санкцій, транскордонні операції, податкові та корупційні злочини, використання віртуальних активів, кіберзлочинність, тіньовий гральний бізнес, зловживання у сфері благодійності та діяльність неприбуткових організацій, а також операції, пов'язані з торгівлею зброєю, людьми та наркотиками.

Окрему увагу приділено трансформації інструментів злочинної діяльності – від традиційного обготівковування до високотехнологічних методів із використанням штучного інтелекту, криптовалют, децентралізованих фінансових систем (DeFi), а також інформаційних атак і пропаганди як елементів гібридної агресії.

Матеріали дослідження включають приклади реальних справ, типові схеми та набір індикаторів підозрілої діяльності, що можуть слугувати практичним інструментом для суб'єктів фінансового моніторингу, правоохоронців, регуляторів і аналітиків.

Актуальність дослідження зумовлена посиленням загроз для фінансової безпеки України в умовах воєнного стану та необхідністю впровадження сучасних підходів до протидії ВК/ФТ/ФРЗМЗ з урахуванням технологічних трансформацій і реалій воєнного часу.

РОЗДІЛ І. ЗАГАЛЬНІ ТЕНДЕНЦІЇ

1.1. Сучасні тенденції трансформації організованої злочинності

Сучасна організована злочинність характеризується високим рівнем адаптивності, транснаціональності та технологічної оснащеності.

В умовах повномасштабної війни, цифровізації економіки та зростання гібридних загроз злочинні мережі швидко трансформують свої структури, інструменти та моделі діяльності.

Європол здійснює підготовку EU-SOCTA 2025 як інструменту стратегічної оцінки загроз серйозної та організованої злочинності. Висновки EU-SOCTA 2025 (Europol) свідчать про зміну «ДНК» організованої злочинності, що проявляється у посиленні її дестабілізуючого впливу на держави, економіку та суспільство.

Нижче наведено ключові тенденції трансформації організованої злочинності у сучасних умовах.

Трансформація «ДНК» організованої злочинності та її дестабілізуючий вплив

Організована злочинність зазнає глибокої структурної трансформації, стаючи не лише кримінальною, а й системною загрозою для економіки, державного управління та суспільної стабільності. Злочинні мережі функціонують як гнучкі бізнес-структури, що генерують значні незаконні доходи, активно використовують корупцію та підривають довіру до державних інституцій. Водночас спостерігається зростання взаємодії між організованою злочинністю та гібридними загрозами, коли кримінальні мережі використовуються як інструмент зовнішнього впливу та дестабілізації.

Диджиталізація та «онлайн-укорінення» злочинної діяльності

Практично всі форми організованої злочинності мають цифровий вимір. Інтернет і цифрова інфраструктура перетворилися з допоміжного інструменту на повноцінне середовище вчинення злочинів. Кіберзлочини, онлайн-шахрайство, незаконна торгівля, вербування учасників, управління потоками коштів і комунікація між членами злочинних угруповань дедалі частіше здійснюються виключно онлайн, з мінімальною фізичною присутністю.

Прискорення злочинної діяльності завдяки ШІ та новітнім технологіям

Штучний інтелект, генеративні моделі, блокчейн і децентралізовані фінансові інструменти значно підвищили масштаб, швидкість і складність злочинних операцій. Злочинні мережі використовують ШІ для створення фішингових кампаній, deepfake-шахрайства, автоматизації кібератак, а також для обходу систем фінансового моніторингу. Це знижує поріг входу в злочинну діяльність і одночасно ускладнює її виявлення.

Залучення легального бізнесу до злочинної діяльності

Ключовою тенденцією є розвиток паралельних фінансових систем, що забезпечують відмивання доходів і фінансування злочинних мереж. Поряд із готівкою дедалі активніше використовуються криптовалюти, DeFi-платформи та спеціалізовані фінансові посередники. Одночасно посилюється проникнення у легальний бізнес через фіктивні компанії, логістичні, будівельні та сервісні структури, що стирає межу між легальною та нелегальною економікою.

Ескалація насильства

Організована злочинність дедалі частіше супроводжується насильством на замовлення, яке використовується як інструмент тиску, усунення конкурентів і контролю над кримінальними ринками. Така практика сприяє зростанню рівня небезпеки та ускладнює притягнення до відповідальності безпосередніх організаторів злочинної діяльності.

Використання підставних осіб («дропів») у злочинних схемах

Особливу загрозу становить залучення молоді та соціально вразливих осіб як виконавців, кур'єрів і підставних осіб («дропів»), переважно через соціальні мережі та месенджери. Це зменшує ризики кримінального переслідування організаторів злочинних схем та обумовлює необхідність посилення роботи правоохоронних органів з такими особами з метою встановлення і викриття організаторів.

1.2. Використання новітніх технологій для вчинення злочинів

У 2025 році технологічні інновації ще більш глибоко впливають на розвиток суспільства, економіки та безпеки. Цифровізація охоплює практично всі сфери життя, а технологія блокчейн залишається одним із ключових рушіїв цих змін. Вона використовується не лише у фінансовому секторі, а й у сфері ідентифікації особи та кібербезпеки.

Криптовалюти у 2025 році вже перестали бути виключно спекулятивним інструментом – вони інтегруються у платіжну інфраструктуру, використовуються у міжнародних розрахунках, а в окремих країнах – як офіційний платіжний засіб. Водночас уряди й міжнародні організації активно розробляють регуляторні рамки для ринку віртуальних активів, спрямовані на забезпечення прозорості, запобігання відмиванню коштів та фінансуванню тероризму.

Разом із тим, в Україні питання належного регулювання та нагляду за діяльністю провайдерів послуг, пов'язаних з обігом віртуальних активів (VASPs), залишається проблемним. Відсутність спеціального законодавства, відсутність повноцінної системи ліцензування та нагляду, а також обмежені можливості застосування ризик-орієнтованого підходу створюють вразливості, які активно використовуються злочинними угрупованнями.

Україна, яка одним із перших користувачів криптовалют, зараз має найвищу у світі частку користувачів криптовалют відносно чисельності населення. Одним із позитивних явищ використання криптовалют є допомога Україні.

Попри те, що інноваційні технології та публічні блокчейни забезпечують швидкі, дешеві й прозорі транзакції, злочинці також використовують криптовалюти для відмивання коштів та фінансування тероризму через їх транскордонність та швидкість.

FATF. У звіті FATF[1] щодо дотримання юрисдикціями Рекомендації 15 наголошується, що більшість країн досі не повністю впровадили стандарти щодо віртуальних активів і провайдерів таких послуг, тому потрібні рішучі дії для зміцнення глобальної системи протидії відмиванню коштів та фінансуванню тероризму.

У звіті зазначається, що загалом юрисдикції досягли прогресу з 2024 року у розробці або впровадженні регулювання у сфері протидії відмиванню коштів/фінансуванню тероризму та вживанні наглядових та правозастосовних заходів. Однак, FATF наголошує на необхідності подальшої роботи з ліцензування та реєстрації, а також на тому, що юрисдикції продовжують стикатися з труднощами у визначенні фізичних або юридичних осіб, які здійснюють діяльність VASP. 99 юрисдикцій ухвалили або перебувають у процесі прийняття законодавства.

Звіт також містить оновлену таблицю кроків, вжитих юрисдикціями Глобальної мережі FATF з суттєво важливою діяльністю VASP для регулювання VA/VASPS. Оскільки ці юрисдикції складають приблизно 98 відсотків світового ринку VA, забезпечення повного впровадження Стандартів FATF юрисдикціями цієї групи значно допоможе зменшити глобальні ризики загалом.

FATF визнає роль Chainalysis, Lukka Inc, Merkle Science та TRM Labs, які зробили свій внесок для зменшення глобальних ризиків.

Оскільки віртуальні активи за своєю суттю не мають кордонів, регуляторні прогалини в одній юрисдикції можуть мати глобальні наслідки. У звіті FATF висвітлюються нові ризики, що виникають внаслідок злочинної експлуатації віртуальних активів, зокрема:

- використання стейблкоїнів різними незаконними суб'єктами, включаючи суб'єктів Корейської Народно-Демократичної Республіки (КНДР), осіб, що фінансують терористів, та наркоторговців;

[1] Шосте оновлення щодо віртуальних активів (VA) та постачальників послуг з віртуальними активами (VASP).

- цього року КНДР здійснила найбільшу в історії крадіжку активів для VA, викравши 1,46 мільярда доларів у VASP ByBit. Повернуто лише 3,8% викрадених коштів, що підкреслює необхідність вирішення проблем повернення активів;
- FATF також відзначила значне зростання використання віртуальних помічників (VA) у шахрайстві та аферах.

Незаконні операції за участю криптобірж

У 2025 році для криптовалютних сервісів був більш складним, ніж попередні. Злом біржі ByBit КНДР на суму 1,5 мільярда доларів, найбільший злом в історії криптовалют.

Станом на кінець червня 2025 року з початку року було викрадено на 17% більше коштів, ніж у 2022 році, який раніше був найгіршим роком за всю історію спостережень. Якщо поточні тенденції збережуться, викрадені кошти з послуг можуть перевищити 4 мільярди доларів до кінця року.

Компрометація особистих гаманців зараз становить зростаючу частку загального обсягу крадіжок екосистеми. Фізичне насильство або примус проти власників криптовалют – показують кореляцію з коливаннями ціни біткойна.

Географічні тенденції

Станом на 2025 рік значна концентрація жертв викрадених коштів знаходилась в США, Німеччині, росії, Канаді, Японії, Індонезії та Південній Кореї.

У регіональному розрізі, Східна Європа, Близький Схід і Північна Африка (MENA) та Центральна Африка (CSAO) спостерігали найшвидше зростання загальної кількості жертв з першої половини 2024 року по першу половину 2025 року.

Також між регіонами виявилися помітні відмінності у типі викрадених активів, що, можливо, відображає основну тенденцію регіонального впровадження криптоактивів.

P2P-перекази та Даркнет

Перекази між фізичними особами напряму стали надзвичайно популярним інструментом для відмивання коштів, особливо у зв’язку зі зростанням популярності криптовалют. Зловмисники використовують P2P-перекази для «дроблення» великих сум на багато дрібних транзакцій між різними рахунками, що ускладнює їхнє відстеження.

Даркнет продовжує залишатися основним майданчиком для обміну незаконними товарами та послугами, а також для відмивання коштів. Завдяки високій анонімності, даркнет використовується для купівлі та продажу наркотиків, зброї та крадених фінансових даних.

Платежі в даркнеті здійснюються переважно анонімними криптовалютами, що значно ускладнює їхнє відстеження правоохоронними органами.

У 2022 році було ліквідовано один з найбільших маркетплейсів даркнету «Hydra», що є наявним прикладом боротьби урядів з цим явищем, але це не зупиняє його розвиток.

Використання Штучного Інтелекту (ШІ) та Deepfake

Зловмисники все частіше використовують ШІ для аналізу великих масивів даних, щоб знаходити слабкі місця у фінансовій системі та створюють переконливі профілі для підставних осіб. ШІ допомагає в автоматизації багатьох процесів, що робить схеми більш масштабними та складними.

Deepfake є одним із найнебезпечніших інструментів, що застосовуються для шахрайства. Технологія дозволяє імітувати голос та відеозображення керівників компаній, менеджерів або клієнтів. Злочинці використовують deepfake-дзвінки для того, щоб віддавати накази про переказ великих сум грошей на підставні рахунки, обманюючи співробітників, які вважають, що розмовляють зі своїм керівником. Це нова загроза, що вимагає впровадження додаткових біометричних методів перевірки та використання максимальної кількості індикаторів для виявлення нехарактерної поведінки.

1.3. Росія – держава-спонсор тероризму

Агресія росії як фактор дестабілізації міжнародної безпеки. Агресія та агресивна війна порушують норми міжнародного права та принципи Статуту ООН, а також суттєво підвищують ризики відмивання коштів, фінансування тероризму та розповсюдження зброї масового знищення.

Збройна агресія проти України призвела до вторгнення на суверенну територію, анексії частини територій, масованих ракетних обстрілів цивільної інфраструктури, актів ядерного шантажу та незаконного утримання тимчасово окупованих земель.

Росія як держава-спонсор тероризму ставить під загрозу не лише стабільність регіональної безпеки, але й глобальну фінансову та політичну стабільність.

У цьому контексті реакція міжнародної спільноти набуває конкретного вираження у рішеннях на рівні Європейського Союзу.

Європейська Комісія додала рф до переліку юрисдикцій з високим рівнем ризику для посилення міжнародної боротьби з фінансовими злочинами.

Європейська Комісія внесла росію до переліку країн з високим рівнем ризику зі стратегічними недоліками у своїх системах протидії відмиванню коштів і фінансуванню тероризму (ПВК/ФТ).

8 липня 2025 року Комісія ухвалила Делегований регламент (ЄС) 2025/1393. Цей Регламент зобов'язав Комісію до кінця 2025 року завершити перегляд третіх країн, які не внесені до переліку Групи з розробки фінансових заходів боротьби з відмиванням грошей (FATF), але членство яких призупинено. Метою є оцінити необхідність внесення змін до переліку ЄС у сфері ПВК на основі результатів цього перегляду.

Оскільки росія підпадає під сферу дії цього Делегованого регламенту, Комісія провела технічну оцінку з використанням чітко визначених методологій та із залученням інформації, зібраної з публічних джерел, від компетентних органів держав-членів та Європейської служби зовнішніх справ. За результатами цієї оцінки зроблено висновок, що росія відповідає критеріям для визначення її як третьої країни з високим рівнем ризику.

Відповідно до 4-ї Директиви про протидію відмиванню коштів (4AMLD) Комісія, таким чином, вживає заходів для збереження цілісності фінансової системи ЄС, додаючи росію до свого переліку юрисдикцій з високим рівнем ризику, які мають стратегічні недоліки у національних режимах ПВК/ФТ. Суб'єкти ЄС, на яких поширюється дія системи ПВК, зобов'язані проявляти посилену пильність під час здійснення операцій, пов'язаних із цими юрисдикціями.

Наступні кроки. Делегований регламент набуде чинності після перевірки та за відсутності заперечень з боку Європейського парламенту і Ради протягом одного місяця. Цей строк може бути продовжено ще на один місяць. Комісія відстежуватиме прогрес усіх країн, включених до переліку, та й надалі контролюватиме відповідні зміни.

Еволюція ризиків ВК/ФТ/ІЗ/ФРЗМЗ у контексті військової агресії. У 2022 - 2025 роках військова агресія російської федерації спричинила глибокі соціально-економічні зміни, що суттєво посилили та трансформували ризики у сфері ВК/ФТ/ІЗ/ФРЗМЗ, надавши їм системного й глобального характеру порівняно з 2020 - 2021 роками.

Основні чинники включають:

- масштабне руйнування економіки, інфраструктури та послаблення контролю на прифронтових територіях (створило умови для зростання тіньової економіки, контрабанди, обігу зброї, нелегального використання гуманітарної допомоги та розкрадання коштів);
- глибока гуманітарна криза та масова міграція (створило умови для торгівлі людьми та використання вразливих груп у фінансових схемах);
- посилення корупційних ризиків;
- цифровізація фінансової злочинності;
- зростання навантаження на правоохоронні й регуляторні інституції, що обмежує можливості своєчасного реагування на складні багатоканальні загрози.

Загрози, пов'язані з підтримкою росією тероризму

Основні загрози, пов'язані з підтримкою росією тероризму:

поширення терористичних актів та дестабілізація регіонів через підтримку збройних угруповань, що спричиняє гуманітарні кризи й масове переміщення населення;

цілеспрямовані кібератаки на критичну інфраструктуру як інструмент терору та тиску;

фінансування тероризму через тіньові канали та кримінальні схеми, що підривають фінансову стабільність;

анонімне фінансування. Використання криптовалют і DeFi-платформ для анонімного переказу коштів і уникнення контролю;

гібридна інформаційна війна, спрямована на маніпуляцію громадською думкою та легітимізацію терористичних дій;

використання інструментів для створення дезінформації. Застосування технологій штучного інтелекту (ШІ), включаючи deepfake-технології та бот-мережі, для формування фальшивих наративів і підриву міжнародного порядку.

Наративи агресора та трансформація схем ВК/ФТ

У 2022 - 2025 рр. російська федерація змінила інформаційну риторику, що дало змогу маскувати фінансові схеми під благодійність, релігійні проєкти та гуманітарну допомогу. Зафіксовано використання криптовалют, ботоферм, соцмереж і фейкових платформ для збору коштів, що сприяло відмиванню грошей та створенню тіньових економічних потоків.

Трансформація схем легалізації доходів. Зміни в риториці та використання нових технологій призвели до того, що фінансові злочини стали невіддільною частиною гібридної війни. Це проявилося в таких тенденціях:

Використання криптовалют: для анонімізації платежів, зібраних через фейкові кампанії, все частіше використовувалися віртуальні активи;

Колаборація з кіберзлочинцями: для фінансових маніпуляцій все частіше залучалися хакери, які атакували, зокрема банківські системи або онлайн-платформи для здійснення незаконних переказів;

Створення тіньових економічних систем: на окупованих територіях та через мережу «добровольчих» організацій створювалися паралельні фінансові потоки, які контролювалися злочинними угрупованнями під прикриттям «державних» чи «громадських» ініціатив.

Фінансування війни та фінансування тероризму

Розуміння джерел фінансування є ключовим для ефективного блокування каналів підтримки війни та посилення міжнародної протидії.

Основні джерела фінансування війни російської федерації проти України:

державний бюджет і підконтрольні ресурси – пряме фінансування збройної агресії, зокрема артилерійських обстрілів, ракетних атак, використання дронів-камікадзе, а також примусове залучення коштів через внутрішні податки та облігації. Використання офшорних схем.

прибутки від експорту енергоресурсів – доходи від продажу нафти, газу та вугілля, зокрема отримані за допомогою тіньових схем та/або типових механізмів обходу санкцій.

активи державних корпорацій і наближених до влади бізнес-структур – перерозподіл прибутків на користь військової машини через формально цивільні підприємства;

кримінальні канали та тіньові фінансові потоки – контрабанда, торгівля зброєю, фіктивні гуманітарні збори, трафік людей, а також операції через юрисдикції з підвищеним ризиком (у т.ч. «чорний список» FATF);

зовнішня підтримка союзників та обхід санкцій – фінансова, матеріальна й логістична допомога з боку країн-партнерів, а також використання офшорних зон і банківських систем, не охоплених санкціями;

цифрові фінансові інструменти – активне використання криптовалют, DeFi-платформ, міксерів та токенізованих активів для обходу санкцій і прихованого фінансування воєнних дій;

експлуатація окупованих територій – використання природних ресурсів, трудових ресурсів та мобілізація населення для підтримки окупаційної логістики та військових кампаній.

Воєнні злочини та відповідальність держави-агресора

Війна російської федерації проти України супроводжується воєнними злочинами й злочинами проти людяності. Ці дії документуються міжнародними організаціями та розслідуються Міжнародним кримінальним судом, що є підставою для притягнення до відповідальності як окремих осіб, так і самої держави-агресора.

Дії росії, також включають енергетичний тероризм, масові депортації, співпраця з терористичними угрупованнями. російська федерація створює гуманітарні кризи, дестабілізує економіку України.

Використання «тіньового флоту» для обходу санкцій

Російська федерація активно застосовує так званий «тіньовий флот» для транспортування нафти, газу та нафтопродуктів в обхід міжнародних санкцій.

Цей механізм є ключовим елементом фінансової стратегії, що дозволяє зберігати валютні надходження попри обмеження з боку G7, ЄС та США.

Тіньовий флот складається переважно із застарілих суден без страхового покриття західних компаній. За даними розвідки, вони забезпечують до 70% морського експорту російської сирої нафти. Судна систематично змінюють назви, прапори, вимикають систему ідентифікації, перевантажують сировину в офшорних водах та змішують нафту з іншими сортами для ускладнення її ідентифікації.

1.4. Фінансування тероризму та колабораціонізму

Україна продовжує активно вживати заходів із протидії фінансуванню тероризму та колабораціонізму, реагуючи на нові безпекові загрози. На тлі триваючої агресії з боку російської федерації, яка активно використовує фінансові механізми для підтримки диверсійних і терористичних структур, питання фінансової безпеки набуває критичної важливості для захисту національної стабільності.

У 2024 – 2025 роках спостерігається активне використання гібридних схем фінансування тероризму, що поєднують традиційні та цифрові канали. Ключові механізми фінансування: криптовалюта, готівка, банківські інструменти – рахунки на підставних осіб («дропів»), фіктивні компанії, офшори. Також фінансування терористичної діяльності часто маскується під легальну активність: використовуються псевдоблагодійні фонди, волонтерські та гуманітарні проєкти, а також бізнес-структури, які створюють фасад легальності.

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

Використання віртуальних активів. Одним із головних викликів для фінансової безпеки залишається активне використання віртуальних активів, які забезпечують високий рівень анонімності та значно ускладнюють виявлення незаконних фінансових потоків, пов’язаних із тероризмом.

Віртуальні активи стали критично важливим інструментом фінансування терористичної діяльності. Здійснюється прямий збір пожертв у криптоактивах через Telegram-канали та P2P-платформи. Значні обсяги коштів обмінюються через OTC-дески – позабіржові торгові майданчики з мінімальними вимогами до ідентифікації користувачів.

Додатково використовуються криптоміксери та DeFi-платформи — децентралізовані фінансові сервіси, які працюють без банків або бірж. Вони дозволяють фрагментувати потоки, приховувати джерела та одержувачів, обходити фінансові обмеження й нагляд. Стейблкоїни та токенізовані активи сприяють швидкому перетворенню вартості та ускладнюють її відстеження через традиційні канали.

Готівкові кошти. Готівкові кошти залишаються ключовим інструментом фінансування тероризму та колабораціонізму.

Кіберзлочинність. Паралельно посилюється кіберзлочинність – зростає кількість фішингових атак, зламів фінансових організацій та крадіжок персональних даних, які можуть використовуватись для фінансування тероризму та колабораціонізму.

Пропаганда та інформаційні атаки. Російська федерація продовжує фінансування пропаганди та інформаційних атак через підконтрольні медіа й організації, особливо на окупованих територіях, поширюючи фейки, дискредитуючи опонентів і виправдовуючи терористичні дії з метою підриву державності України.

Використання «дропів» для фінансування диверсійних груп. Фінансування диверсійних груп через такі канали, як онлайн-казино та карткові рахунки «дропів» (грошових мулів), є реальною загрозою. Описана схема дозволяє розірвати прямий зв'язок між спонсором (наприклад, спецслужбою агресора) та виконавцем, а також швидко перевести кошти в готівку.

Наприклад, на банківський рахунок соціально вразливої особи надходять кошти з нетипових джерел (казино, P2P), які миттєво транзитом переказуються або повністю знімаються готівкою в географічно аномальному місці. Це є надзвичайно потужним сигналом про можливе фінансування злочинної, в тому числі диверсійної діяльності.

1.5. Російсько-українська кібервійна

Кіберскладова стала ключовим елементом сучасної війни, де кібервійна динамічно розвивається завдяки новітнім технологіям, інструментам і тактикам. Внаслідок цього країни інвестують у розвиток кіберзахисту, формують спеціалізовані підрозділи та налагоджують міжнародну співпрацю для протидії цифровим загрозам.

У відповідь на ці виклики уряди та організації розробляють адаптивні стратегії кібербезпеки, впроваджують штучний інтелект та автоматизовані системи для швидкого виявлення та нейтралізації загроз.

Кібервійна російської федерації проти України характеризується ескалацією та високотехнологічністю. Україна активно протидіє загрозам, розвиваючи свої кіберспроможності та адаптуючи нові стратегії захисту. Масштаб та складність атак з боку росії залишаються серйозною загрозою для національної безпеки України.

CERT-UA

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

Завдяки роботі CERT-UA вдається своєчасно виявляти атаки, мінімізувати їхні наслідки та підвищувати рівень кіберстійкості країни.

Ландшафт кіберзагроз у 2025 році. Від початку 2025 року CERT-UA фіксує в середньому близько 15 кіберінцидентів на день та відстежує понад 150 кластерів кіберзагроз. Основним джерелом кібератак залишається російська федерація. Окрім цього, спостерігається активність з білорусі, Китаю, КНДР та, на жаль, з боку груп, що діють з тимчасово окупованих територій України.

Основні типи хакерської кіберактивності містять:

- ***Шпигунство***. Переважно російське, спрямоване на будь-які сфери, особливо військову, має найбільший вплив на ситуацію на фронті.
- ***Фінансово вмотивовані злочини***. Спрямовані на викрадення коштів.
- ***Саботаж***. Кібертероризм, що впливає на кожного в Україні.
- ***Інші***. Специфічні атаки, наприклад, на нотаріусів.

Кібершпигунство. Шпигунство проти Сил оборони України є одним із пріоритетних напрямів для ворожих спецслужб в Україні.

Фінансово вмотивовані атаки. Ряд хакерських груп використовують цільовий фішинг для отримання віддаленого доступу до комп'ютерів бухгалтерів з метою створення нових або модифікації існуючих платіжних доручень для виведення коштів на свої рахунки.

Кібертероризм

Кіберудари по критичній інфраструктурі вже стали системним явищем.

23 березня 2025 року здійснена кібератака на Укрзалізницю. Деякі з атак здійснюються для підсилення наслідків кінетичних ударів.

Пріоритетними цілями головного управління генерального штабу збройних сил рф, як і раніше, залишалися знищення та виведення з ладу об'єктів енергетичної інфраструктури. Крім того, атакам піддавалися організації оборонно-промислового комплексу, постачальники телекомунікаційних послуг і навіть науково-дослідні установи.

Кібератаки на банківську систему

У 2022 - 2025 роках фінансовий сектор України зазнав суттєвого впливу з боку кібератак, що здебільшого координувалися або походили з території російської федерації. Кібератаки перетворилися з поодиноких інцидентів на систематичну, скоординовану кампанію, що змусило українську банківську систему кардинально перебудувати підходи до безпеки та призвело до еволюції злочинних схем.

Основними векторами атак стали спроби дестабілізувати роботу банків, масове викрадення фінансових даних громадян через фішинг та цілеспрямоване кібершпигунство.

Банківський сектор України став однією з головних цілей російських кібератак, кількість яких з кожним роком зростає. Це стимулювало банки до інвестицій у кібербезпеку. Банківські установи зазначають, що впроваджували:

- ***багатофакторну автентифікацію:*** застосування додаткових чинників для підтвердження особи (біометрія, токени);
- ***системи на основі ШІ та машинного навчання:*** використання ШІ для аналізу великих обсягів даних і виявлення аномалій у транзакціях;
- ***криптографію та блокчейн:*** ці технології використовувалися для захисту конфіденційності та прозорості транзакцій, що ускладнювало зовнішнє втручання;
- ***створення резервних копій:*** банки почали створювати резервні копії критично важливих даних, щоб у разі успішної атаки мати можливість швидко відновити роботу.

Фішингові схеми

Російські кіберзлочинці значно вдосконалили фішингові схеми, роблячи їх більш персоналізованими та цілеспрямованими. Фішингові схеми стали більш витонченими: шахраї активно експлуатували тематику війни, гуманітарної допомоги, державних виплат чи підтримки переселенців.

Через фальшиві сайти, SMS або повідомлення у месенджерах зловмисники виманювали особисту інформацію, банківські реквізити, логіни до онлайн-банкінгу, що надалі використовувалися для викрадення коштів.

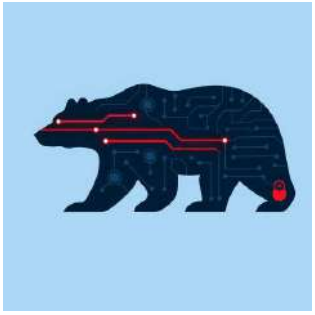
Злочинці використовують соціальну інженерію та фейкові повідомлення, щоб спонукати користувачів до розкриття своїх фінансових даних.

Кібершпигунство та зловживання даними

Російські кіберугруповання, що працюють під прикриттям державних структур, здійснюють кібершпигунство для збору інформації про фінансову систему України.

Метою кібершпигунства є отримання даних для аналізу економічної ситуації, виявлення слабких місць та подальших дестабілізаційних атак.

Водночас виникли випадки цілеспрямованого шпигунства, коли атаки мали на меті не лише фінансову вигоду, а й доступ до стратегічно важливої інформації про внутрішні банківські системи, транзакції, обсяг державної чи міжнародної допомоги, а також персональні дані клієнтів, які могли стати об’єктом подальших атак або шантажу.



За даними Державної служби спеціального зв'язку та захисту інформації України, російські хакери використовують ШІ у кібератаках проти України.

Хакери тепер використовують його не лише для створення фішингових повідомлень, але деякі зразки шкідливого програмного забезпечення мають чіткі ознаки того, що вони були створені за допомогою штучного інтелекту.

Наймасштабніші кібератаки на Україну

2022 рік – Кібератаки на урядові сайти та державні реєстри

Вночі 14 січня 2022 року російські хакери атакували «Дію», сайти Кабміну, МОЗ, Міністерства закордонних справ, ДСНС, Міністерства освіти, Міністерства спорту, Міністерства аграрної політики, Міністерства енергетики, Міноборони, Державної казначейської служби та інших органів. Загалом від хакерської атаки постраждали 70 державних сайтів.

На повне усунення наслідків пішли три доби.

23-24 лютого 2022 року було продовження атаки. Хакери атакували сайти Кабінету Міністрів України, Верховної Ради, Міністерства закордонних справ, Служби безпеки України та інших органів влади. На відновлення їхньої роботи витратили один-два дні.

2022 рік – Кібератака на українські банки

15 лютого 2022 року російські хакери атакували близько 15 банків, у тому числі ПриватБанк та Ощадбанк. Крім того, кібератаці зазнали сайти Міноборони, Міністерства з питань реінтеграції тимчасово окупованих територій.

2023 рік – Кібератака на мобільного оператора «Київстар»

Вранці 12 грудня 2023 року у роботі найбільшого оператора зв'язку «Київстар» по всій країні стався збій: були недоступні послуги мобільного зв'язку та мобільного, домашнього інтернету. У компанії заявили, що сталася хакерська атака.

2024 рік – Кібератака на державні реєстри України

Відбулася наймасштабніша зовнішня кібератака на державні реєстри України. Внаслідок цілеспрямованої атаки тимчасово призупинено роботу Єдиних та Державних реєстрів, які перебувають у компетенції Міністерства юстиції України, у тому числі реєстр актів цивільного стану громадян, реєстри довіреностей та боржників, Єдиний державний реєстр юридичних осіб та ФОП. Крім того, було порушено роботу сервісів у «Дії».

2024 рік – Кібератака на дата-центр «Парковий»

25 січня 2024 року кібератаки зазнав дата-центр «Парковий», внаслідок чого стався збій у роботі сервісів «Нафтогазу», Укрзалізниці, Укрпошти та системи «Шлях».

Найдовше відновлював роботу своїх онлайн-сервісів, сайтів та колцентрів «Нафтогаз» – близько чотирьох днів.

1.6. Гібридні схеми реалізації та легалізації викрадених ресурсів з тимчасово окупованих територій України

Умови триваючої військової агресії російської федерації спричинили систематичне та масштабне незаконне вилучення матеріальних ресурсів на тимчасово окупованих територіях України.

Характеристика гібридних схем. Сформовані окупаційними адміністраціями та пов'язаними кримінально-комерційними групами канали переміщення, збуту та легалізації таких ресурсів набули ознак складних гібридних схем, що поєднують фізичне транспортування вантажів, юридичне маскування їх походження та транскордонні фінансові операції з приховуванням бенефіціарів.

Початковий збут викрадених ресурсів. Викрадені на тимчасово окупованих територіях України ресурси – зерно, лісоматеріали, метали, енергоносії, промислове обладнання та предмети культури – реалізують через багаторівневі гібридні схеми, які поєднують фізичний збут і юридичне маскування: місцеві перекупники й ринки забезпечують первинну реалізацію або конвертацію в готівку й бартер, після чого партії часто передаються пов'язаним або номінальним компаніям, зареєстрованим у суміжних або у «дружніх» юрисдикціях.

Юридичне маскування та маскування під легальний товар. Для створення зовнішньої легітимності товарів використовують підроблені або фальсифіковані інвойси й сертифікати походження, перепакування, перемішування крадених вантажів із легальними партіями, а також тимчасове зберігання на транзитних хабах і багаторазові перевантаження – усе це дає змогу «переписати» походження і приховати фактичний маршрут.

Ключові учасники посередницьких операцій. Значну роль відіграють посередники: логістичні оператори, брокери, адвокати, номінальні директори та афілійовані торгові мережі, які забезпечують створення формальних документів й доступ до портів та складів.

На міжнародних ринках товар може реекспортуватися через третю країну під іншою декларацією або через ланцюжки компаній-посередників, де фінансові операції структурують так, щоб приховати кінцевого бенефіціара – через фіктивні контракти, завищення або заниження цін в інвойсах, бартерні угоди та складні серії переказів між афілійованими фірмами. Частина платежів відбувається готівкою або через позабіржовий ринок чи P2P-перекази, де KYC відсутній; для часткового «конвертування» використовуються операції в криптовалюті, хоча вони рідше стають основним каналом, бо залишають цифровий слід та привертають увагу аналітиків.

Логістичні методи маскування включають ship-to-ship[2] перевантаження, тимчасову зміну прапорів суден, відключення AIS або часті зміни маршрутів і портів, що ускладнює відстеження фізичного переміщення вантажів.

Типові маркери ризику. Типові маркери ризику, які фіксують розслідування – невідповідність між заявленим та реальним походженням у сертифікатах, часті зміни власників або операторів вантажу протягом короткого часу, аномальні цінові розриви в інвойсах, повторні перевантаження та незвичні маршрути через транзитні хаби.

Поєднання традиційних даних та блокчейн-аналітики. Для виявлення й блокування таких схем критично важлива кореляція Off-chain[3] і On-chain[4] даних: поєднання митних декларацій, банківських операцій і торгових реєстрів з AIS/satellite-даними, супутниковими знімками складів і портів, аналізом ланцюгів власності та OSINT-розслідуваннями.

Контрзаходи та міжнародна координація. Ефективні контрзаходи включають посилений KYC та поглиблену належну перевірку клієнта (Enhanced Due Diligence, EDD) для торгових контрагентів і логістичних операторів, лабораторну перевірку партій при підозрі (коли можливо), міжнародну координацію митниць і правоохоронних органів, застосування санкційних та фіскальних інструментів до підозрілих компаній і активів, а також використання розвідувальних потоків даних (intelligence feeds) і журналістських розслідувань для виявлення мереж і проміжних осіб.

Злочинні мережі покладаються на багатошаровість і юридичну неоднозначність, але їхні слабкі місця – документальний та логістичний слід, незвичні фінансові потоки та фізичне переміщення вантажів – дають можливість для виявлення за умови інтегрованого аналізу даних і міжнародного співробітництва.

Наприклад, крадіжка зерна російською федерацією з окупованих територій почалася у 2014 році, коли агресор вперше вторгся в Україну, і продовжилася після повномасштабного вторгнення, розпочатого у лютому 2022 року.

[2] Ship-to-ship (STS) — операція прямого перевантаження вантажу між двома суднами в морі

[3] Off-chain дані – це усі дані, що знаходяться поза блокчейном, але можуть бути співставленні з on-chain активністю.

[4] On-chain дані –це всі дані, які записані безпосередньо в блокчейні.

Злодії зерна: мережа, що стоїть за розграбуванням українського зерна  https://iphronline.org/articles/grain-thieves-report/	Дослідження проведено Міжнародним партнерством з прав людини (IPHR) – незалежною неурядовою організацією, заснованою у Брюсселі у 2008 році. З початку повномасштабного вторгнення в Україну в лютому 2022 року російські війська окупували одні з найродючіших земель світу, захопивши сільськогосподарські угіддя, врожай, обладнання та інфраструктуру в українських фермерів та агробізнесів.

Фермери, яким вдалося зберегти контроль над своїми господарствами, були змушені продавати всю свою продукцію новим російським державним монополіям за встановленими цінами.

За оцінками українського уряду, лише у 2023 році росія відправила приблизно 4 мільйони тон зерна з окупованих територій України на міжнародний ринок, що зробило торгівлю награбованою сільськогосподарською продукцією як джерелом стабільного доходу, так і геополітичним інструментом для росії.

Російська влада створила схему промислового масштабу для розграбування українських зернових та сільськогосподарських ресурсів.

З 2014 року десятки українських державних та приватних шахт були захоплені та включені до окупаційної економіки.

Надалі через занепад вугільних шахт, підтримувана російською федерацією окупаційна влада почала передавати шахти приватним російським фірмам.

Процес передачі називався «інвестиційною» моделлю. За цією схемою компанії орендували шахти на кілька років з правом викупу через три роки. Тим часом шахти мають законних власників в Україні. Схема схожа на перепродаж краденого.

1.7. Використання дітей для вчинення злочину

Правоохоронні органи надалі виявляють випадки вербування підлітків через інтернет російськими спецслужбами з метою залучення їх до протиправної, зокрема диверсійної діяльності.

Посилений фінансовий моніторинг для безпеки дітей в умовах гібридних загроз. Суб'єкти первинного фінансового моніторингу мають відігравати ключову роль у захисті неповнолітніх від злочинних схем.

Підлітки часто стають мішенню як злочинних угруповань, так і країни-агресора, тому фінансові установи повинні уважно відстежувати їхні операції.

До ознак підозрілої діяльності можуть належати великі або регулярні грошові перекази, нетипові витрати чи надходження, а також часті транзакції, що не відповідають віку та соціальному статусу клієнта. Для підвищення ефективності контролю установам рекомендується створювати власні індикатори ризику та скорингові моделі, які допоможуть своєчасно виявляти потенційні загрози, пов'язані з відмиванням коштів, фінансуванням тероризму чи іншими формами фінансової експлуатації неповнолітніх.

Вербування. Спеціальні служби російської федерації системно використовують українських підлітків у гібридній війні, вербуючи їх через соціальні мережі, месенджери та ігрові платформи. Злочинці застосовують шантаж, психологічний тиск і обіцянки «легких» грошей, залучаючи дітей до підпалів, диверсій та збору розвідувальних даних.

Протиправна діяльність. Завербованих підлітків спецслужби російської федерації використовують для вчинення протиправної діяльності, зокрема:

- вчинення підпалів автомобілів військових, держслужбовців, волонтерів;
- закладання вибухових пристроїв;
- повідомлення про псевдомінування;
- встановлення GPS-маячків, стеження за переміщенням військових;
- зйомка та передача фото/відео військових об'єктів, блокпостів, техніки;
- поширення фейків у соцмережах, дискредитація Збройних Сил України;
- участь у збиранні (обслуговуванні) військової техніки чи дронів; примусове навчання чи «тренінги» бойового чи розвідувального характеру;
- вербування через «ігрові квести» чи завдання-вікторини (з відтягуванням до шпигунської діяльності).

Залучення дітей до такої діяльності руйнує життя самих підлітків, які можуть стати фігурантами кримінальних проваджень або навіть зазнати фізичної загрози.

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

Чатбот **t.me/spaly_fsb_bot** створено в телеграмі, оскільки цю мережу ворог використовує для того, щоб залучити громадян України, а особливо молодь та неповнолітніх, до вчинення злочинів.

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

Освітній фронт: як СБУ та поліція навчають молодь протидії ворожим впливам.

Представники Служби безпеки України та Національної поліції проводять зустрічі зі школярами та студентами у навчальних закладах усіх регіонів України. Під час лекцій вони розповідають молоді про методи, які російські спецслужби використовують для вербування у соціальних мережах і месенджерах та надають практичні поради, як не потрапити на гачок до ворога.

Кібербулінг. В умовах повномасштабної війни кібербулінг стає не лише соціальною проблемою, а й інструментом інформаційно-психологічного впливу, який використовують ворожі спецслужби російської федерації. Зокрема, агресор застосовує кібербулінг як один із методів тиску та маніпуляції над підлітками. У такому стані підлітки стають легкою мішенню для вербування, що дозволяє втягувати їх у підривну діяльність на шкоду національній безпеці України.

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

У випадку кібербулінгу деструктивна поведінка набуває форми систематичних образ, принижень чи погроз, що здійснюються через електронні засоби комунікації – інтернет, соціальні мережі, месенджери або мобільні телефони. Такий вид агресії особливо небезпечний, адже він може тривати цілодобово, охоплювати широке коло свідків і завдавати значної психологічної шкоди жертві.

Європол про зростання злочинності

EU-SOCTA 2025. Європол у своєму звіті EU-SOCTA 2025 зазначає, що кримінальне використання молодих злочинців все частіше стає тактикою, яку використовують злочинні угруповання, щоб уникнути виявлення, затримання, судового переслідування та покарання.

Інтернет та зашифровані засоби комунікації дають злочинцям можливість вербувати кілерів, у тому числі молодих, та координувати насильницькі дії. Інтернет-платформи та зашифровані засоби комунікації є основним каталізатором насильства, вербування, комунікації, вимагання або дистанційної координації, оскільки вони полегшують доступ до молодих правопорушників.

Участь молодих злочинців у насильницьких злочинах спостерігається у вуличних пограбуваннях, вимаганні та рекеті, сексуальному насильстві над дітьми й торгівлі людьми, а також стала особливо помітною у сфері незаконного обігу наркотиків.

Звіт EU SOCTA 2025 містить окремий розділ «Кримінальне використання молодих злочинців».

У 2025 році Європол створив нову Оперативну групу (OTF) для боротьби зі зростанням тенденції насильства як послуги та вербування молодих злочинців до тяжких та організованих злочинів.

Ця оперативна група, відома як OTF GRIMM (GRIMM – назва оперативної групи), очолювана Швецією, об’єднує правоохоронні органи Бельгії, Данії, Фінляндії, Франції, Німеччини, Нідерландів та Норвегії, а Європол надає оперативну підтримку, аналіз загроз та координацію.

Експлуатація молодих злочинців для скоєння злочинів стала тактикою, що швидко розвивається, і використовується організованою злочинністю. Ця тенденція також була підкреслена в «Оцінці загрози серйозної та організованої злочинності Європейського Союзу за 2025 рік» (EU-SOCTA), в якій було визначено навмисне використання молодих осіб як спосіб уникнути виявлення та судового переслідування.

Насильство як послуга стосується передачі насильницьких дій на аутсорсинг постачальникам кримінальних послуг, що часто передбачає використання молодих злочинців для здійснення погроз, нападів або вбивств за певну плату.

Розслідування показують, що ці дії часто організовуються дистанційно, коли молодих людей вербують та навчають онлайн. Існує явний попит з боку злочинного світу на молодих людей, готових виконувати насильницькі завдання, а також є вразлива молодь, яку готують або примушують до цього.

Молодих людей навмисно переслідують та вербують для скоєння широкого спектра злочинів – від торгівлі наркотиками та кібератак до онлайн-шахрайства та насильницького вимагання.

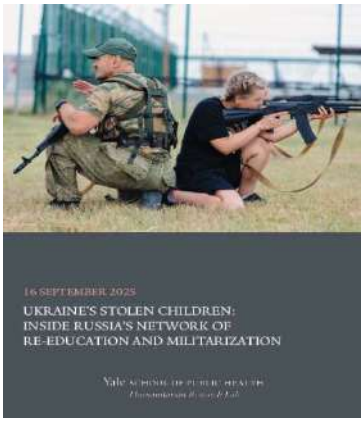
Платформи соціальних мереж та месенджери використовуються для охоплення молоді за допомогою закодованої мови, мемів та ігрових завдань. В обмін на гроші, статус чи відчуття приналежності їх втягують у злочинні схеми, які є як насильницькими, так і транснаціональними.

Використовуючи молодих злочинців, злочинні мережі прагнуть зменшити власний ризик та захистити себе від правоохоронних органів.

OTF GRIMM: координує обмін розвідувальними даними; вивчає методи рекрутингу та стратегії монетизації, що використовуються мережами; виявляє та ліквідує постачальників кримінальних послуг, які сприяють насильству на вимогу; співпрацює з технологічними компаніями з метою виявлення та запобігання вербуванню в соціальних мережах.

Через OTF GRIMM Європол надає платформу для аналізу даних, оперативної координації та спільних розслідувань, забезпечуючи узгодженість дій правоохоронних органів по всій Європі у відстеженні, розслідуванні та зриві діяльності злочинних мереж.

Росія використовує викрадених українських дітей для зборки дронів у таборах «перевиховання»



За даними дослідження Єльської гуманітарної лабораторії, російська федерація використовує викрадених українських дітей у військових цілях.

У таборі на узбережжі Чорного моря неповнолітніх віком 13 - 17 років змушували проходити «навчання» зі збирання безпілотників, мінодетекторів та іншого військового обладнання.

Табір, підпорядкований Міністерству освіти російської федерації та з 2022 року прийняв щонайменше чотири групи українських дітей (близько 300 осіб).

Частину дітей залучали до програми «ЮНТЕХ», організованої молодіжною воєнізованою організацією. Дітям ставили завдання з «виробництва військової техніки», а супутникові знімки засвідчують стройові навчання та підготовку, подібну до бойової.

Дії російської федерації підтверджують системну практику мілітаризації та ідеологічної обробки українських неповнолітніх.

Суб'єкти первинного фінансового моніторингу відзначають, що молодь, через недостатній життєвий досвід, обмежені знання у фінансовій сфері та підвищену вразливість до соціальних і цифрових маніпуляцій, може несвідомо ставати учасниками фінансових операцій з ознаками злочинної діяльності.

Ризик залучення неповнолітніх залишається високим, адже молоді люди не завжди здатні критично мислити, легко піддаються маніпуляції, психологічному впливу, мають потребу у власних коштах, не усвідомлюють наслідків, та складно притягуються до відповідальності.

Типові способи залучення неповнолітніх до схем відмивання коштів:

1. Використання як дропів (грошових мулів).

Неповнолітні надають доступ до своїх банківських рахунків або оформлюють картки на себе, їхні рахунки використовуються для транзиту коштів, отриманих злочинним шляхом.

2. Оформлення ФОПів на молодих осіб.

У деяких випадках ФОПи реєструються на молодих осіб (через підроблені документи або за згодою батьків), щоб уникнути податкового контролю. Такі ФОПи використовуються для фіктивних операцій, переведення коштів у готівку.

3. Криптовалютні транзакції.

Підлітки залучаються до обміну криптовалют, участі у псевдотрейдингу або як виконавці технічних операцій (наприклад, перекази через міксери). Часто вони не усвідомлюють, що беруть участь у схемах ВК.

4. Робота в псевдо-ІТ або фінансових проєктах.

Молодь залучається до «фінансових стартапів», які насправді є оболонками для відмивання коштів. Їм пропонують «роботу» з обробки платежів, ведення баз даних, оформлення договорів.

На основі практичних спостережень опитувані фінансові посередники повідомляють про випадки використання неповнолітніх осіб як «номінальних осіб» у здійснених фінансових операціях. Рахунки «дропів» використовують як «транзитні» для переказу та відмивання незаконних коштів.

РОЗДІЛ ІІ. САНКЦІЇ

Санкції проти російської федерації в умовах війни мають стратегічне значення, проте потребують постійного вдосконалення, адаптації, зміцнення міжнародної коаліції та посилення національної інституційної спроможності.

Санкції є одним із ключових інструментів економічного та політичного тиску на агресора, але на практиці їх реалізація стикається з викликами, які впливають на їх ефективність.

2.1. Виклики застосування санкцій та механізми їх обходу агресором

Застосування санкцій проти російської федерації в умовах повномасштабної війни з Україною супроводжується низкою викликів як на національному, так і на міжнародному рівнях.

Міжнародний рівень. На міжнародному рівні одним із ключових викликів залишається вкрай тривалий і багатоступеневий процес ухвалення та впровадження санкційних рішень**,** що істотно знижує оперативність реагування на загрози, які створює російська федерація.

Процедури узгодження між державами, обов'язковість політичного консенсусу, складність юридичного оформлення та необхідність оцінки потенційних економічних наслідків призводять до того, що санкційні заходи часто вводяться із суттєвою затримкою, дозволяючи російській федерації адаптуватися до них, змінювати логістику, перебудовувати фінансові та торговельні канали, а також напрацьовувати нові схеми обходу обмежень.

Геополітичні та економічні фактори стримування санкцій. Додатковою проблемою є позиція окремих держав**,** які з політичних, економічних або геостратегічних міркувань затягують, пом'якшують або відкрито **блокують** ухвалення рішень, спрямованих на посилення санкційного тиску. У результаті знижується загальна ефективність глобальної санкційної коаліції, а ризики фінансування війни, незаконної торгівлі та переміщення товарів подвійного призначення зростають.

Несинхронність санкційної політики між країнами-партнерами дає російській федерації можливість обходити обмеження через треті країни.

Національний рівень. Однією з ключових проблем є обмежена можливість застосування санкцій щодо комерційних найменувань і торговельних марок, оскільки в низці секторів, зокрема у криптоіндустрії, ускладнено ідентифікацію конкретних юридичних осіб.

Реалізація санкційних рішень ускладнюється також труднощами з ідентифікацією реальних бенефіціарів російських активів через багаторівневі структури власності, офшорні юрисдикції та використання номінальних осіб.

Найпоширеніші внутрішні схеми обходу санкцій включають маскування контролю над активами через їх переоформлення на підставних осіб, створення підконтрольних або офшорних компаній, виведення коштів через довірених осіб, підробку документів та зміну реєстраційних даних, застосування складних внутрішніх платіжних ланцюгів та формальний «розпродаж» майна напередодні запровадження санкцій.

Приклад 2025.2.1.1. Уникнення санкцій шляхом заміни кінцевого бенефіціарного власника

НКЦПФР виявила підсанкційну особу, яка була КБВ юридичної особи та яка переоформила свою частку на підставну особу, що дозволило компанії уникнути застосування до неї санкційних обмежень.

Адаптація політики держави-агресора до санкційного тиску. Динамічна робота російської федерації з трансформації структури компаній, зміни юридичних осіб, переорієнтації комерційної діяльності, а також використання складних схем для приховування реальних власників і контролерів має суттєвий вплив на ефективність санкційних заходів. Особливу складність становить зростання рівня непрозорості російських державних реєстрів, які навмисно не розкривають інформацію.

Російська федерація продовжує переорієнтацію зовнішньої торгівлі на країни Азії, які стали основними каналами постачання товарів, включно з підсанкційною продукцією. Китай зберігає статус головного торговельного партнера росії та ключового джерела високотехнологічних товарів.

Роль криптовалют у схемах обходу санкцій

У 2022–2025 роках криптовалюти стали одним із ключових інструментів обходу санкцій, накладених на російську федерацію з боку ЄС, США та партнерів.

Незважаючи на високий рівень прозорості блокчейн-транзакцій, децентралізована інфраструктура та розгалужена мережа високоризикових сервісів створюють можливості для приховування походження коштів, зняття контролю за транскордонними переказами та уникнення традиційних комплаєнс-процедур.

Наприклад, криптоміксери та P2P-перекази дозволяють маскувати транзакції. Крім того, російська федерація розробила стейблкоїни, прив’язані до рубля, за допомогою яких здійснюються розрахунки на мільярди доларів, при цьому операційна компанія підсанкційної криптобіржі Garantex — Grinex зареєстрована у Киргизстані.

Інформаційно-аналітична фірма TRM Labs на своєму сайті повідомила, що криптовалютна біржа Garantex після санкцій проти неї була ребрендована як Grinex[5].

[5] https://www.trmlabs.com/resources/blog/grinex-emerges-as-likely-garantex-rebrand

Корупційні механізми обходу санкцій. Російська федерація активно шукає шляхи обходу санкцій, спираючись насамперед на корупційні механізми. Представники держави-агресора використовують мережі міжнародних корупційних зв'язків, залучають посередників у третіх країнах та маніпулюють прогалинами в санкційних режимах.

Бартерні схеми розрахунків як інструмент обходу санкцій

Бартерні механізми дедалі частіше застосовуються російською федерацією та пов'язаними комерційними структурами для приховування фактичних фінансових потоків та уникнення контролю з боку санкційних режимів США, ЄС та партнерів. Суть таких схем полягає у заміні грошових транзакцій на прямий обмін товарами чи послугами, що дозволяє уникати банківських перевірок, запобігати блокуванню платежів та маскувати природу комерційних відносин.

Прикладами таких схем є бартерні угоди в зовнішній торгівлі російської федерації, зокрема з КНР:

- обмін російської пшениці та металів (зокрема алюмінію) на китайські автомобілі;
- експорт російського насіння льону в обмін на китайську побутову техніку та будматеріали.

В умовах санкцій і платіжних ризиків бартер може стати одним з основних способів взаєморозрахунків у зовнішній торгівлі росії, зокрема з КНР та країнами Глобального півдня.

Створення альтернативних платіжних систем, зокрема інтеграція національних платіжних систем із країнами «чорного списку» FATF

З точки зору фінансового сектору, найбільш тривожними є перехід до двосторонніх розрахунків, зокрема між російською федерацією та Іраном у місцевих валютах та зусилля обох сторін щодо створення незалежної від західної фінансової системи фінансової інфраструктури. Серед іншого російська платіжна система «Мир» та іранська система «Shetab» були інтегровані у три етапи, що дозволило здійснювати транскордонні розрахунки та використання карток «Мир» та «Shetab» у росії та Ірані.

Росія активно розробляє та залучає інші країни до участі у системі передачі фінансових повідомлень (СПФС — російська альтернатива SWIFT).

Центральний банк російської федерації обмежив оприлюднення переліку операторів, підключених до СПФС, з 19.04.2022 (станом на зазначену дату налічувалося 338 учасників, 52 з яких були іноземними операторами з 12 країн, зокрема білорусі, Республіки Куба, Республіки Казахстан, Республіки Таджикистан, Республіки Вірменія).

Також росія намагається встановлювати прямі кореспондентські відносини із іноземними банками.

Вразливість російської федерації та логістичні ускладнення імпорту підсанкційних товарів

Економіка російської федерації перебуває під зростаючим навантаженням, що свідчить про її системну нестійкість і залежність від зовнішніх джерел.

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

Після запровадження широкомасштабних міжнародних санкцій російська федерація зіткнулася зі значним ускладненням логістики імпорту підсанкційних товарів. Обмеження на використання європейської портової інфраструктури, закриття прямих маршрутів та контроль за високотехнологічними товарами призвели до формування довших, дорожчих і складніших транспортних ланцюгів.

Наприклад, це:

- додаткові транзитні країни;
- перетин сухопутних кордонів замість морської доставки;
- перевантаження товару між різними видами транспорту (морський – залізничний – автотранспорт).

У результаті час доставки та вартість доставки збільшується**,** що суттєво підвищує фінансове навантаження на російську федерацію.

Динаміка та ключові етапи санкцій ЄС щодо російської федерації

Хронологія - Санкції ЄС проти російської федерації Європейська Рада Рада Європейського Союзу https://www.consilium.europa.eu/en/policies/sanctions-against-russia/timeline-sanctions-against-russia/	Огляд санкцій, прийнятих ЄС у відповідь на агресію росії проти України, порушення нею прав людини, гібридні загрози та незаконну анексію Криму, а також Донецької, Луганської, Запорізької та Херсонської областей України.

Наприклад, 19-й пакет санкцій проти росії включає наступні заходи:

- санкції проти ще 69 осіб, включаючи крипто-провайдерів;
- заборона на імпорт російського скрапленого природного газу до ЄС;
- заборона доступу до портів для додаткових 117 суден тіньового флоту рф;
- заборона на операції з п’ятьма додатковими російськими банками та іншими банками з третіх країн;

- заборона на взаємодію операторів ЄС з російською національною системою платіжних карток («Мир») або системою швидших платежів («СБП»);
- зобов’язання російських дипломатів заздалегідь інформувати держави-члени ЄС про поїздки в Шенгенську зону;
- експортні обмеження для 45 нових суб’єктів господарювання, деякі з яких розташовані в третіх країнах, що постачають товари та технології подвійного використання;
- подальші заборони на експорт товарів і послуг;
- Заходи, вжиті проти білорусі, включають:
- санкції проти ще п’яти осіб;
- торговельні заходи, аналогічні тим, що були запроваджені проти росії.

Правові рамки ЄС щодо виявлення та покарання за порушення санкцій

Європейський Парламент та Рада Європейського Союзу 24 квітня 2024 року прийняли Директиву № 2024/1226 про виявлення правопорушень, пов’язаних з порушеннями обмежувальних заходів та санкцій ЄС за такі порушення.

Текст Директиви доступний за посиланням: https://eur-lex.europa.eu/eli/dir/2024/1226/oj/eng

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

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

2.2. Типові схеми обходу санкцій та сучасні підходи до їхнього моніторингу і протидії

Повномасштабна агресія російської федерації проти України спричинила значне ускладнення та зростання схем обходу санкцій, які держава-агресор реалізує через торговельні, фінансові, логістичні та цифрові механізми, у тому числі за участю посередників у третіх країнах.

Типові схеми обходу санкцій, які використовує російська федерація:

Торговельні схеми (реекспорт через треті країни; фіктивне декларування походження товару; зміна країни походження; подвійні інвойси; змішування товарів для маскування російського походження).

Логістичні схеми (ship-to-ship перевантаження; відключення AIS; тимчасова зміна прапорів суден).

Фінансові схеми (розшарування платежів через посередників; залучення банків у юрисдикціях зі слабким AML/CFT-контролем; використання криптовалют і здійснення P2P-переказів, у тому числі через анонімні платформи; бартерні операції).

Товари подвійного призначення та схеми їх незаконного імпорту (ЧІПи, дрони, оптика, мікроелектроніка).

Наприклад, з моменту вторгнення в Україну російська федерація суттєво розширила свій тіньовий флот нафтових танкерів, причому понад 40% нових суден тіньового флоту надходять від продавців з ЄС.

Тіньовий флот постійно зростає, наприклад, у 2022 році 100 суден та у 2025 році понад 340 суден, причому російська федерація додає приблизно сім суден на місяць протягом останніх трьох років.

Попри численні санкційні режими партнерів України, російська федерація продовжує шукати шляхи імпортувати критичні товари, необхідні для підтримання свого оборонно-промислового комплексу та технологічної спроможності.

До ключових категорій товарів належать:

- ***мікроелектроніка, комплектувальні для дронів і високоточні технології.*** Використовуються посередники у третіх країнах для придбання застарілих або модифікованих компонентів. Також застосовують перекласифікацію товарів у митній документації, фрагментацію великих замовлень на дрібні партії і пошук локальних аналогів або контрафакту в

дружніх юрисдикціях. Компоненти масово виявляють у захопленій російській техніці на полі бою;

- ***критичні товари подвійного призначення.*** Наприклад: тепловізори, оптико-електронні системи, генератори та перетворювачі, телекомунікаційне та обладнання систем зв'язку;
- ***нафтопромислове та енергетичне обладнання.*** Наприклад, для модернізації нафтовидобутку, що забезпечує підтримання видобутку нафти й газу на санкційно-критичному рівні;
- ***літакові комплектуючі та авіаційні запчастини.*** Санкції забороняють експорт деталей до літаків, але російська федерація продовжує шукати гальмівні системи, запчастини до двигунів, блоки управління та елементи шасі через треті юрисдикції та «сірі» логістичні маршрути.

Моніторинг та виявлення схем обходу санкцій. Описані вище факти формують потребу в посиленому моніторингу, застосуванні сучасних аналітичних інструментів, міжнародній координації та зміцненні національних механізмів протидії для своєчасного виявлення та блокування таких схем.

Основним методом моніторингу та виявлення фактів обходу санкцій є перевірка всіх залучених сторін під час проведення транзакцій та аналіз предмета самої транзакції (товарів або послуг).

Методи виявлення схем обходу санкцій:

- поглиблена перевірка платежів із залученням ризикових країн, з особливою увагою до держав, які є «дружніми» до російської федерації та сприяють обходу санкцій. Про такі країни постійно з'являються публікації на сайтах державних органів, зокрема розвідувальних та правоохоронних;
- аналіз ланцюгів постачання товарів та перевірка країн призначення / поставки / походження товарів (особлива увага приділяється нафтопродуктам та товарам, що можуть мати подвійне призначення);
- перевірка наявності в структурі власності нерезидентів, які є учасниками платежу, на предмет наявності в них російського сліду;
- якісна та регулярна KYC з метою визначення реальних КБВ.

Моніторинг фінансових операцій. Моніторинг за визначеними сценаріями є ключовим елементом у виявленні підозрілих транзакцій, зокрема тих, що характеризуються складністю, незвично великими сумами, нетиповим способом проведення, відсутністю очевидної економічної мети або невідповідністю заявленому профілю діяльності клієнта.

Інструментарій. Для моніторингу та виявлення фактів обходу санкцій використовуються різні інструменти технічного, аналітичного та правового характеру. Одним із ключових є системи автоматичного скринінгу санкційних списків (OFAC, EU, UN тощо), які перевіряють клієнтів, компанії, судна та інші об'єкти на відповідність обмеженням.

Також активно застосовуються інструменти моніторингу фінансових транзакцій – вони виявляють підозрілі перекази, нетипові схеми розрахунків або транзитні платежі через високоризикові юрисдикції.

Торгові потоки. Важливу роль відіграє аналіз торговельних потоків: дані про експорт-імпорт, митні коди, ціни та обсяги допомагають ідентифікувати аномалії та потенційні спроби обходу санкцій. Наприклад, база даних Comtrade ООН збирає детальну глобальну річну та місячну статистику торгівлі.

Морська логістика. Для морської логістики використовують супутниковий моніторинг, AIS-трекинг суден, дані про зміну прапорів або відключення транспондерів.

КБВ. У сфері бенефіціарної перевірки важливі реєстри власників, комерційні бази даних і процедури посиленого аналізу (EDD/KYC).

Криптовалюта. У криптовалютному середовищі працюють блокчейн-аналітичні платформи, що дозволяють відстежувати рух активів через гаманці. Доповнюють систему OSINT-інструменти, журналістські розслідування, аналітичні звіти спеціалізованих компаній та міжурядові інформаційні обміни.

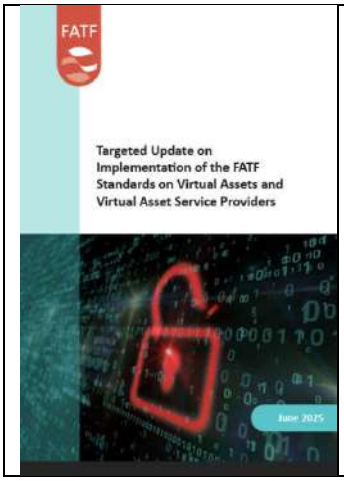
РОЗДІЛ ІІІ. ОГЛЯД АКТУАЛЬНИХ ДОСЛІДЖЕНЬ

3.1. Публікації FATF

FATF регулярно відстежує нові та такі, що розвиваються, способи відмивання коштів і фінансування тероризму, а її типологічні звіти підвищують обізнаність державних органів і приватного сектору про актуальні ризики, допомагаючи своєчасно запроваджувати ефективні заходи з їхнього пом'якшення.

Складні схеми фінансування розповсюдження та обходу санкцій[6].

Звіт FATF висвітлює основні прогалини у глобальній відповіді на фінансування розповсюдження зброї масового знищення та ухилення від санкцій.



Цільове оновлення щодо впровадження стандартів FATF щодо віртуальних активів та постачальників послуг віртуальних активів[7].

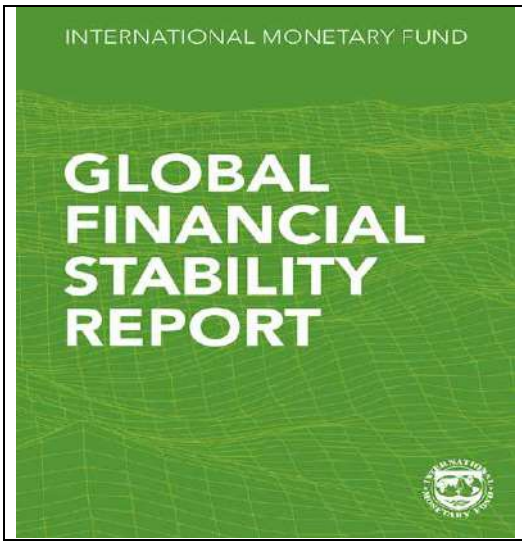
У звіті оцінюється дотримання юрисдикціями Рекомендації FATF 15 та її Пояснювальної записки (R.15/INR.15), яка була оновлена у 2019 році для застосування заходів протидії відмиванню коштів/фінансуванню тероризму до постачальників послуг з віртуальними активами (VASP).

[6] https://www.fatf-gafi.org/en/publications/Financingofproliferation/complex-proliferation-financing-sanction-evasion-schemes.html

[7] https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2025-Targeted-Upate-VA-VASPs.pdf.coredownload.pdf

3.2. Публікації Міжнародного валютного фонду

Міжнародний валютний фонд у своїх дослідженнях і звітах системно аналізує глобальні ризики відмивання коштів та фінансування тероризму, оцінює ефективність наглядових режимів, вплив фінансових технологій на кримінальні потоки, а також вразливості держав до корупції та фінансових злочинів.

	**Звіт про глобальну фінансову стабільність[8].** У Звіті про глобальну фінансову стабільність наведено оцінку світової фінансової системи та ринків, а також розглянуто питання фінансування на ринках, що розвиваються, у глобальному контексті. МВФ аналізує глобальні ризики, пов'язані з фінансовою стабільністю, зокрема, оцінює вплив кіберризиків та геополітичних загроз на фінансовий сектор, що є актуальним для України.

3.3. Публікації Європол

Європол у своїх щорічних звітах та спеціалізованих аналітичних оглядах висвітлює ключові тенденції та загрози, пов'язані з організованою злочинністю, кіберзлочинами та фінансовими злочинами в Європі. Публікації Europol, зокрема IOCTA та оцінки загроз економічній і фінансовій злочинності, містять актуальні дані про методи відмивання коштів, використання криптовалют, мереж дропів, торгово-посередницькі схеми та механізми обходу санкцій.

[8] https://www.imf.org/en/publications/gfsr/issues/2025/10/14/global-financial-stability-report-october-2025?utm_source=chatgpt.com

	**Звіт про оцінку загроз організованої злочинності** (EU Serious and Organised Crime Threat Assessment - SOCTA)[9]. SOCTA – це стратегічний звіт Європолу, який надає комплексну оцінку загроз від злочинності в Європейському Союзі. Документ аналізує ключові кримінальні ринки, транснаціональні злочинні мережі, нові тенденції та прогнози щодо еволюції злочинності.

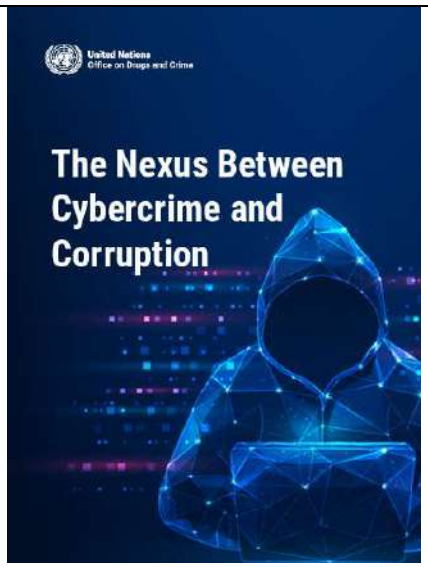
	**Оцінка загроз організованої кіберзлочинності в Інтернеті (IOCTA) 2025** (Internet Organised Crime Threat Assessment (IOCTA) 2025)[10] Звіт IOCTA 2025 – головний аналітичний документ Europol щодо кіберзагроз. У ньому виділено ключові тренди, важливі для типологічних досліджень з відмивання коштів.

[9] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf

[10] https://www.europol.europa.eu/publication-events/main-reports/steal-deal-and-repeat-how-cybercriminals-trade-and-exploit-your-data

3.4. Публікації Організації Об’єднаних Націй

Організація Об’єднаних Націй у своїх профільних публікаціях, зокрема звітах UNODC та аналітичних оглядах щодо транснаціональної організованої злочинності, висвітлює глобальні тенденції у сфері відмивання коштів, незаконних фінансових потоків, торгівлі людьми, корупції, кіберзлочинів та незаконного обігу наркотиків і зброї.



Зв’язок між кіберзлочинністю та корупцією[11].

Дослідження UNODC показує, що в цифрову епоху корупція стала структурним елементом кіберзлочинності, а не просто супутнім явищем. Корупційні зв’язки формують нову «цифрову інфраструктуру безкарності», у якій державні посадовці, банківські та IT-працівники й злочинні кібергрупи діють як єдина екосистема.

Приклади UNODC:

Східна Азія – «scam factories» працюють під прикриттям поліції, чиновників та окремих дипломатів.

Африка – угруповання типу Black Axe конвертують криптовалютні доходи у «політичні інвестиції» (хабарі).

Латинська Америка – хабарі здійснюються через токени, NFT, «цифрові ваучери», що маскують природу платежів.

Кіберкорупція – це нова архітектура злочинності, де корупція забезпечує доступ і прикриття, а цифрові технології забезпечують масштабування, приховування та відмивання незаконних доходів. Така модель створює високоризикові середовища для ВК/ФТ та потребує інтегрованого фінансово-цифрового моніторингу.

[11] https://www.unodc.org/roseap/uploads/documents/Publications/2025/2025.10.21_The_Nexus_Between_Cybercrime_and_Corruption.pdf?utm_source=chatgpt.com

	**Всесвітній звіт про наркотики 2025[12].** Звіт є глобальним довідником з ринків наркотиків, тенденцій та розвитку політики, пропонує безліч даних та аналізу, а у 2025 році містить кілька елементів, адаптованих для різної аудиторії.

«Світовий звіт про наркотики 2025» спрямований не лише на сприяння посиленню міжнародної співпраці для протидії впливу світової проблеми наркотиків на здоров'я, управління та безпеку, але й на допомогу державам-членам у передбаченні та усуненні загроз, що виникають з боку ринків наркотиків, та пом'якшенні їхніх наслідків

3.5. Публікації Egmont Group

Egmont Group (мережа фінансових розвідувальних підрозділів) у своїх публікаціях, зокрема відкритих бюлетенях, аналітичних оглядах та матеріалах конкурсу BECA, узагальнює практичний досвід підрозділів фінансової розвідки з усього світу щодо виявлення схем відмивання коштів і фінансування тероризму.

	**Звіт на тему «Роль підрозділів фінансової розвідки у боротьбі зі зловживанням неприбутковими організаціями для фінансування тероризму»[13].** Сектор неприбуткових організацій є складним для моніторингу через масштаб, специфічну структуру та характер діяльності. З огляду на підвищені ризики та швидке глобальне зростання цього сектору, підрозділи фінансової розвідки відіграють ключову роль у виявленні операцій, пов'язаних із фінансуванням тероризму.

[12] https://www.unodc.org/unodc/data-and-analysis/world-drug-report-2025.html?utm_source=chatgpt.com

[13] https://egmontgroup.org/news/fius-role-in-the-fight-against-the-abuse-of-npos-for-tf-activities-public-summary-report/?utm_source=chatgpt.com

	Міжнародний характер роботи НПО робить критично важливими ефективну співпрацю та своєчасний обмін інформацією між ПФР. Звіт узагальнює, яким чином неприбуткові організації можуть бути використані для фінансування терористичної діяльності.

	**Звіт на тему: «Зловживання віртуальними активами з метою фінансування тероризму»[14].** Звіт висвітлює, як віртуальні активи можуть бути використані для фінансування тероризму, та визначає основні вразливості, пов'язані з новими технологіями.
Документ узагальнює практичний досвід підрозділу фінансової розвідки Великої Британії щодо виявлення й запобігання таким схемам. Особлива увага приділяється складності відстеження руху віртуальних активів, що значно ускладнює роботу компетентних органів у справах, пов'язаних із фінансуванням тероризму.	

[14] https://egmontgroup.org/news/public-summary-on-abuse-of-virtual-assets-for-terrorist-financing-purposes-report/?utm_source=chatgpt.com

3.6. Публікації Світового банку

Світовий банк активно залучений до ПВК/ФТ, оскільки відповідно до свого мандату забезпечує сприяння економічній стабільності та розвитку. Світовий банк у своїх дослідженнях та аналітичних звітах приділяє значну увагу ризикам відмивання коштів, фінансування тероризму та незаконним фінансовим потокам, особливо в країнах з підвищеною вразливістю та під час процесів відбудови.

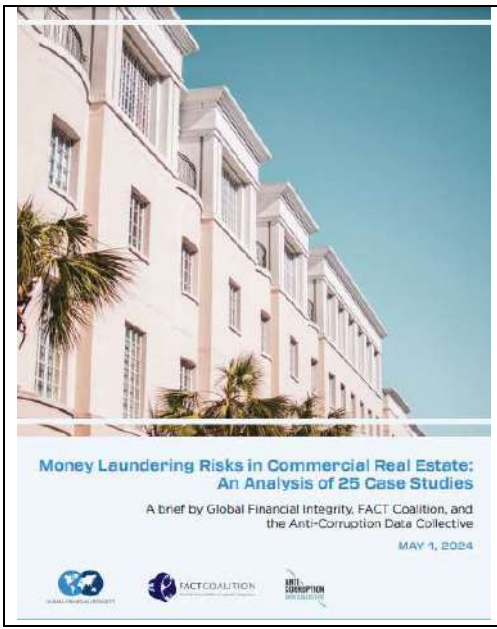
Національна оцінка ризиків протидії відмиванню коштів/фінансуванню тероризму щодо віртуальних активів та постачальників послуг з віртуальних активів[15].

Посібник Світового банку та ЄС – AML/CFT National Risk Assessment on Virtual Assets and Virtual Asset Service Providers (VASP), один із найбільш практичних документів 2024–2025 років для країн, які оновлюють національну оцінку ризиків щодо криптовалют та відповідних сервісів.

[15] https://openknowledge.worldbank.org/entities/publication/bb5a7475-ac52-4697-afdc-5f618a550623?utm_source=chatgpt.com’

3.7. Публікації Global Financial Integrity

Global Financial Integrity (GFI) – це незалежна міжнародна аналітична організація, заснована у Вашингтоні (США), яка спеціалізується на дослідженні незаконних фінансових потоків у світі. У своїх звітах досліджує масштаби та механізми незаконних фінансових потоків, зосереджуючись на тіньовій економіці, корупції, ухиленні від сплати податків, неправомірних торговельних практиках і транснаціональних схемах відмивання коштів.



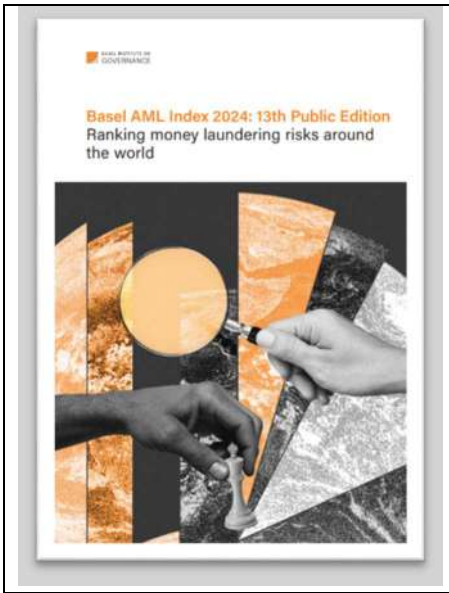
Ризики відмивання грошей у сфері комерційної нерухомості: аналіз 25 прикладів[16]

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

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

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

3.8. Публікації Basel Institute



Базельський індекс AML 2024. Рейтинг ризиків відмивання коштів[17]

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

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

3.9. Національні публікації

Міністерство фінансів України, як орган, що формує державну політику у сфері ПВК/ФТ/ФРЗМЗ, забезпечує підготовку щотижневих Методологічних Бюлетенів[18].

Бюлетені публікуються на офіційному вебсайті Міністерства фінансів України в рубриці «Діяльність-Антилегалізаційна політика (AML) – Методологія – Методологічні бюлетені» та регулярно доповнюються матеріалами.

[17] https://index.baselgovernance.org/api/assets/0789b440-8537-45b4-8bfd-e44ac456c15d.pdf
[18] https://www.mof.gov.ua/uk/methodological_bulletins-875

РОЗДІЛ IV. СПЕЦІАЛЬНА ЧАСТИНА ТИПОЛОГІЇ

У 2025 році, в умовах військової агресії російської федерації, злочинні схеми зазнають суттєвої трансформації та адаптації до функціонування економіки в період воєнного стану, що супроводжується зростанням ризиків зловживань і тіньових фінансових операцій.

Загальні тенденції організованої злочинності

В умовах воєнного стану організована злочинність характеризується високою адаптивністю та застосуванням багатоетапних фінансових схем. Злочинні угруповання використовують фіктивні й підконтрольні суб'єкти господарювання, ланцюги юридичних осіб і ФОПів, а також підставних осіб («дропів») з метою транзиту коштів, легалізації доходів і маскування реальних бенефіціарів. Одночасно зростає роль організованої злочинності у корупційних правопорушеннях.

Чинники активізації діяльності організованої злочинності:

Макроекономічні та соціальні фактори

Війна руйнує економічні зв'язки, стимулює тіньову економіку, нелегальний обіг товарів і зброї, а також ускладнює контроль за переміщенням осіб. Економічна нестабільність, масова міграція та зростання соціальної вразливості населення створюють умови для активізації організованої злочинності.

Інституційні та правові чинники

Постійне перевантаження правоохоронних органів і корупція знижують ефективність розслідувань та сприяють безкарності, а відмінності між юрисдикціями використовуються злочинцями для ускладнення притягнення до відповідальності.

Технологічні чинники

Розвиток цифрових фінансів, зокрема криптоактивів, фінтех-рішень та електронних грошей, розширює можливості для приховування та швидкого переміщення незаконних коштів. Використання інструментів анонімізації, онлайн-ринків і штучного інтелекту (deepfake, соціальна інженерія) суттєво ускладнює ідентифікацію учасників та виявлення злочинних схем.

Геополітичні та безпекові чинники

Гібридна війна передбачає використання організованої злочинності як інструменту дестабілізації та впливу на внутрішню безпеку держави. Санкційний тиск і ослаблення контролю на окремих ділянках кордону стимулюють розвиток транскордонної злочинної діяльності.

Основні напрями діяльності організованої злочинності

Фінансово-економічна злочинність

Фінансово-економічна злочинність є одним із ключових напрямів діяльності організованих злочинних груп та охоплює відмивання доходів, податкові злочини й шахрайські схеми з ПДВ.

Транскордонна злочинність

Транскордонна злочинність охоплює контрабанду підакцизних товарів, палива, медикаментів, а також незаконний обіг культурних цінностей через використання міжнародних маршрутів і вразливостей кордонного контролю. Окремим напрямом є організація нелегальної міграції, що посилюються в умовах воєнного стану.

Незаконний обіг зброї та військових товарів

Незаконний обіг зброї та військових товарів охоплює торгівлю зброєю, боєприпасами, вибухівкою й товарами подвійного призначення з використанням воєнних ризиків і прогалин контролю. Окрему загрозу становить перепродаж військового майна та гуманітарної допомоги з метою незаконного збагачення.

Наркозлочинність

Наркозлочинність зосереджується на виробництві та логістиці синтетичних наркотиків із активним використанням даркнет-майданчиків і цифрових каналів збуту.

Кіберзлочинність

Кіберзлочинність включає шахрайські електронні повідомлення, фінансові афери та атаки із вимаганням викупу, а також викрадення персональних і фінансових даних. Окремим напрямом є онлайн-шахрайство під виглядом інвестиційних проєктів або благодійних зборів, що особливо поширене в умовах війни.

Корупційно-злочинні зв'язки

Корупційно-злочинні зв'язки проявляються через проникнення організованої злочинності у державні закупівлі, логістичні процеси, митні та ліцензійні процедури. Через вплив на посадових осіб злочинні угруповання отримують можливість маніпулювати управлінськими рішеннями та забезпечувати власну безкарність.

Використання легального бізнесу

Використання легального бізнесу для прикриття незаконної діяльності й легалізації доходів.

Основні напрями злочинної діяльності

У межах зазначених тенденцій фіксуються такі основні прояви злочинної діяльності:

1. Національний рівень.

В сучасних умовах фіксується приховування зв'язків із агресором шляхом зміни структури власності, використання номінальних власників і реєстрації нових юридичних осіб.

Традиційні схеми. Паралельно продовжують застосовуватися традиційні злочинні схеми — «конвертаційні центри», P2P-мережі, «дропи», фіктивні ЗЕД-операції. Юридичні особи продовжують застосовувати дроблення бізнесу, використовуючи ФОПів для ухилення від сплати податків.

Використання неповнолітніх осіб. Фіксується залучення неповнолітніх осіб до незаконної діяльності, що зумовлено їхньою вразливістю та використовується злочинцями для виконання окремих шахрайських або допоміжних операцій.

Шахрайство. Поширюються шахрайські дії, зокрема несанкціоноване списання коштів із рахунків юридичних та фізичних осіб.

Розкрадання бюджетних коштів та корупційні правопорушення. Фіксуються схеми розкрадання бюджетних коштів, зокрема спрямованих на оборонні та гуманітарні потреби, а також корупційні правопорушення, що створюють підвищені ризики відмивання доходів у період воєнного стану.

В умовах збройної агресії російської федерації фіксується зростання злочинних схем, пов'язаних із коштами державних підприємств оборонного сектору, введенням в обіг товарів без встановленого походження та залученням фіктивних суб'єктів господарювання і багаторівневих ланцюгів ФОПів для транзиту коштів, підміни номенклатури, ухилення від оподаткування й розкрадання бюджетних коштів, зокрема у сфері відновлення інфраструктури.

2. Міжнародний рівень.

На міжнародному рівні спостерігається активний обхід санкцій російською федерацією через юрисдикції третіх країн, компанії-прокладки, логістичні ланцюги та «тіньовий флот», що створює перетин ризиків ВК/ФТ із ризиками фінансування розповсюдження зброї та підтримки воєнної машини агресора.

Експлуатація фінансових інститутів у третіх країнах. Злочинці використовують банки та фінансові установи в країнах зі слабким фінансовим моніторингом, щоб обходити санкції та здійснювати транскордонні перекази.

Транскордонні канали незаконного обігу ресурсів. Незаконно вилучені природні, промислові чи культурні ресурси вивозяться за межі країни та переправляються на міжнародні ринки через транскордонні нелегальні канали, що сприяє фінансуванню агресора та підриває глобальні режими санкційного контролю.

У контексті зазначених тенденцій дедалі більшої актуальності набуває вплив новітніх технологій на трансформацію фінансових злочинів. Одночасно з технологічними загрозами зростає ризик зловживань у неприбутковому секторі, який залишається чутливим до фінансових маніпуляцій та схем легалізації.

Технологічна та цифрова еволюція злочинних фінансових схем

У 2025 році фіксується зростання цифрових і кіберзагроз, пов'язаних із використанням віртуальних активів, крипто-міксерів, DeFi-інструментів, викрадених цифрових ідентичностей та ШІ-генерованого шахрайства. Криптовалюти активно застосовуються для анонімізації, швидкого транскордонного переміщення коштів, обходу санкцій, фінансування тероризму та відмивання доходів.

Готівкові операції дедалі частіше замінюються цифровими активами, а фінансові потоки, що проходять через треті країни та децентралізовані платформи, суттєво ускладнюють їх відстеження.

Традиційні схеми із залученням підставних осіб («дропів») еволюціонують шляхом використання викрадених облікових записів, deepfake-документів, фішингових атак, шахрайських кол-центрів та інших форм кіберзлочинності.

Неприбутковий сектор.

Окремим чутливим блоком залишаються операції неприбуткових організацій та волонтерських структур, де доброчесна діяльність поєднується з випадками зловживань, фіктивних зборів та транскордонних схем.

Поширюється маскування злочинної діяльності під гуманітарну, волонтерську чи релігійну активність з подальшим відмиванням коштів через криптобіржі або готівкові операції.

Маскування під благодійність та волонтерство є однією з найпоширеніших тенденцій. Зловмисники створюють фейкові благодійні фонди, збираючи кошти нібито на допомогу ЗСУ або постраждалим, а насправді легалізують їх, змішуючи з легальними пожертвами.

Виклики та інструменти обходу системи ПВК/ФТ

Ураховуючи масштаби та динаміку сучасних загроз, особливого значення набувають виклики у сфері ПВК/ФТ та інструменти, які використовують злочинці для обходу фінансового моніторингу.

Виклики ПВК/ФТ. Усе це формує складне та динамічне середовище, у якому протидія ВК/ФТ потребує одночасного посилення аналітики, автоматизації, OSINT-моніторингу, міжнародної співпраці та постійного оновлення індикаторів підозрілості.

Злочинці все частіше застосовують складні фінансові потоки для маскування своєї діяльності. Зростає технологічна складність злочинних схем, що проявляється у широкому використанні штучного інтелекту, ботоферм, фішингових атак, фейкових онлайн-платформ та мереж «дропів».

Інструменти обходу. Злочинці продовжують шукати слабкі зони у системі фінансового моніторингу та прогалини законодавства для проведення незаконних фінансових операцій.

Аналіз підозрілих фінансових операцій свідчить про зростання використання злочинцями міжнародних професійних мереж, що включають групи фіктивних суб'єктів господарювання та численні рахунки в різних юрисдикціях і банках.

Зберігається активне використання підставних осіб («дропів»), зокрема із соціально вразливих груп, у тому числі із застосуванням цифрових та транскордонних інструментів. «Дропи» використовуються для розшарування та маскування незаконних доходів, що суттєво ускладнює їх відстеження.

Віртуальні валюти залишаються одним із ключових трендів у сфері фінансових злочинів. Недостатній рівень регулювання та контролю в цій сфері дає змогу злочинцям здійснювати анонімні транзакції, приховувати джерела походження коштів і розшаровувати фінансові потоки.

З урахуванням характеру виявлених схем, джерел незаконних доходів та механізмів їх легалізації, у межах цього дослідження типології ВК/ФТ умовно згруповано за такими ключовими напрямами:

1. ФТ та ВК як частина фінансування війни.
2. Обхід санкцій та фінансових обмежень.
3. Корупційні злочини та схеми відмивання злочинних доходів.
4. Використання НПО у незаконній діяльності та незаконне заволодіння і привласнення благодійної допомоги.
5. Транскордонне ВК.
6. Податкові злочини та схеми ухилення від оподаткування.
7. Відмивання доходів, отриманих від шахрайських дій та кіберзлочинів.
8. Відмивання злочинних доходів із використанням віртуальних активів.
9. Використання віртуальних активів та нелегального грального бізнесу для ВК/ФТ.
10. Торгівля зброєю, людьми та наркотичними засобами.
11. Використання страхового ринку та небанківських фінансових установ у схемах відмивання доходів, одержаних злочинним шляхом.

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

У 2022–2025 роках російська федерація активно застосовує фінансування тероризму та відмивання коштів як ключові інструменти ведення війни. Водночас ці практики не є новими – вони системно використовувались ще з 2014 року, після початку агресії проти України.

Фінансування тероризму у сучасному світі є не лише кримінальним явищем, а й важливим елементом демонстрування підтримки воєнних дій. Сьогодні фінансові ресурси виступають такою ж зброєю, як і танки чи ракети. Саме через грошові потоки терористичні режими утримують армію, закуповують боєприпаси та військову техніку, забезпечують логістичні маршрути та здійснюють пропагандистську діяльність.

Фінансування війни в Україні, яку веде росія, залишається пріоритетним для агресора при формуванні федерального бюджету.

Відповідно до інформації, опублікованої Службою зовнішньої розвідки України, федеральний бюджет країни-агресора на 2025-2027 роки містить рекордні витрати на статті, пов’язані з російсько-українською війною, – 41% від усіх видатків.

Зазначається, що на статтю «національна оборона» російська госдума виділила 133,6 млрд дол США, що на 25% більше порівняно з 2024 роком, а на статтю «національна безпека та правоохоронна діяльність» – 3,18 млрд дол США, що перевищує на 3% порівняно з 2024 роком. Також було зростання витрат на «патріотичне виховання» у контексті мобілізаційних заходів.

Ескалація війни та пошук фінансових ресурсів в умовах санкційної ізоляції. На тлі затяжної агресивної війни проти України, країна-агресор змушена шукати нові джерела надходжень через обмежений доступ до міжнародних фінансових ринків та технологій. Військові витрати залишаються рекордно високими – включаючи виплати військовим, логістику, озброєння, пропаганду та розвідку.

Енергетичні схеми обходу санкцій та тіньові прибутки агресора. Ключовим джерелом доходів залишається експорт енергоносіїв. Щоб обійти санкції, російська федерація активно використовує «тіньовий флот», торгівлю через треті країни, а також юридичне маскування походження нафти. Такі схеми дозволяють агресору отримувати великі прибутки, незважаючи на обмеження.

Активізація підривної діяльності рф через фінансування агентурної мережі. Посилюються заходи російських спецслужб для фінансування розвідувально-підривної діяльності на території України із залученням представників маргінальних верств населення та свідомих колаборантів.

Інформаційно-психологічна війна. російська пропаганда активізує спроби дискредитувати гарантії безпеки для України, прагне підірвати довіру українців та жителів Заходу до міжнародної підтримки, зокрема до роботи «коаліції охочих». Усі ці заходи потребують колосальних фінансових вливань і кремль шукає різні способи забезпечити максимальне фінансування.

Ресурсне забезпечення тероризму. Готівка різної валюти, грошові кошти на рахунках в банках, матеріальні ресурси залишаються як і раніше незмінними видами ресурсів, які використовуються для фінансування російського терористичного режиму. Проте сьогодні з'являються і нові типи ресурсів, такі як криптовалюта.

Запобігання тероризму. Протидія фінансуванню тероризму та відмиванню коштів є важливим питанням для забезпечення національної безпеки. Активне відстеження та блокування нелегальних фінансових потоків, які використовуються терористичними угрупуванням, в тому числі росією, – одне з пріоритетних завдань для підтримки фінансової стабільності та зміцненню національної та міжнародної безпеки.

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

Приклад 2025.4.1.1. Використання віртуальних активів та соціальних мереж для фінансування тероризму

Держфінмоніторингом виявлено схему використання спецслужбами російської федерації криптогаманця (USDT у мережі «Tron») для фінансування підготовки терористичних актів та інших злочинів, спрямованих проти основ національної безпеки України.

Встановлено, що мультивалютний криптогаманець W застосовувався як інструмент для приховування походження активів, у тому числі злочинних. Така можливість забезпечувалася механізмами внутрішньої взаємодії гаманців на платформі, зокрема змішуванням коштів, що значно ускладнювало їх подальше відстеження.

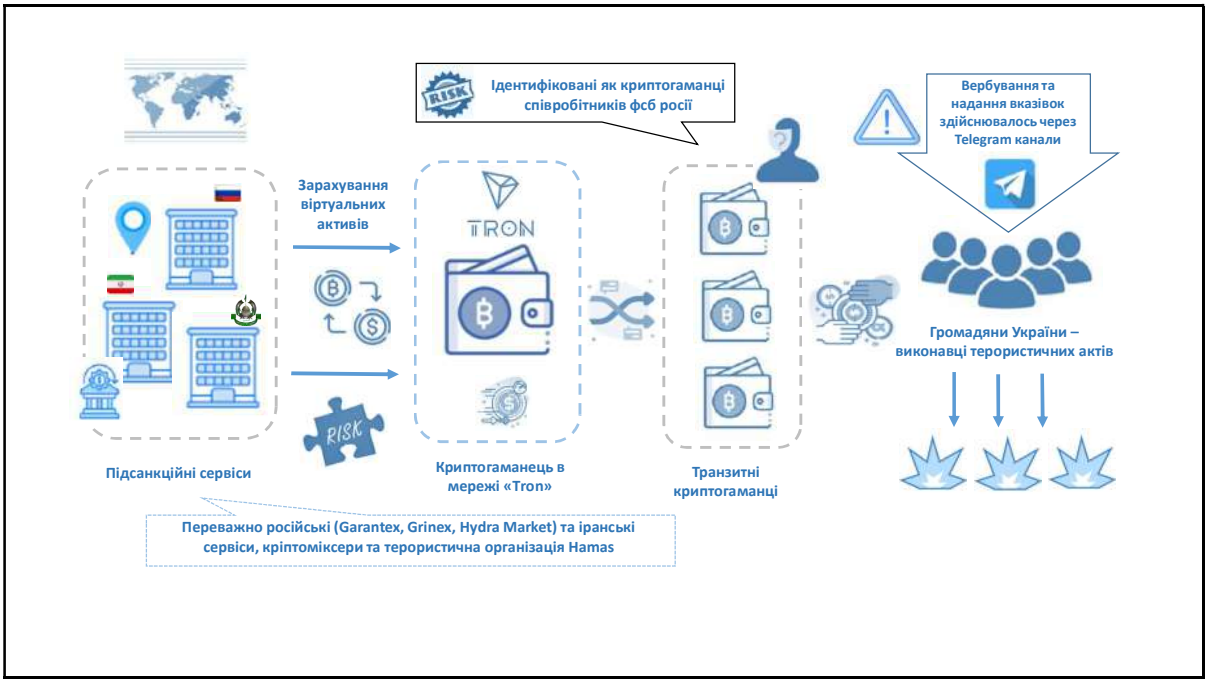
Протягом останніх семи років на криптогаманець W надходили значні обсяги віртуальних активів від переважно російських (Garantex, Grinex, Hydra) та іранських підсанкційних сервісів, криптоміксерів, а також терористичної організації Хамас.

Під час аналізу Держфінмоніторингом виявлено ланцюг криптотранзакцій, за яким активи з криптогаманця W перераховувалися на транзитні криптогаманці, власниками яких ідентифіковано співробітників ФСБ російської федерації.

Надалі кошти з кінцевих акаунтів на біржах Binance і WhiteBIT за допомогою P2P-платформ конвертувалися з USDT у гривню та надходили на карткові рахунки громадян України, яких було завербовано для вчинення терористичних актів та інших злочинів на території України.

Також встановлено, що вербування громадян України та передача їм інструкцій здійснювалися співробітниками ФСБ через Telegram-канали.

Правоохоронними органами розпочато досудове розслідування.



Приклад 2025.4.1.2. Схема використання рахунків фізичної особи для фінансування організації терористичних та диверсійних актів на території України

Держфінмоніторингом, з урахуванням інформації правоохоронного органу, виявлено схему використання рахунків фізичної особи для фінансування організації вчинення терористичних та диверсійних актів на території України.

Встановлено, що на рахунки **Фізичної особи** були перераховані кошти від **Групи фізичних осіб А** (як встановлених осіб, так і невстановлених), безготівковим та готівковим шляхом.

Надалі **Фізичною особою** було здійснено перерахування коштів для поповнення мобільних рахунків, оплати товарів і послуг, переказів між власними рахунками та зняття готівки, а також перераховано кошти іншій **Групі фізичних осіб Б**.

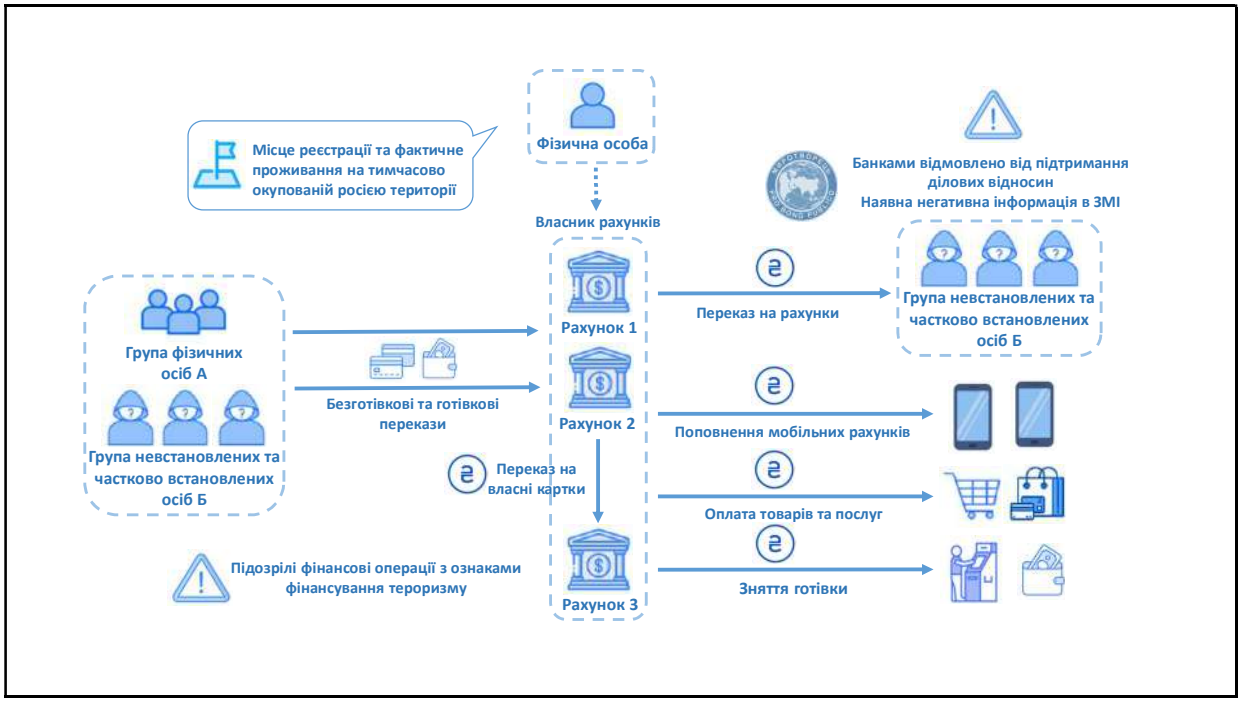
У зв’язку з підозрами у здійсненні незаконних операцій ряду осіб із **Групи фізичних осіб Б**, банками було відмовлено у підтриманні ділових відносин з ними на підставі встановлення клієнту неприйнятно високого ризику.

Встановлено, що **Фізична особа** зареєстрована та фактично перебуває на тимчасово окупованій росією території та, за інформацією правоохоронного органу, залучена до організації терористичних і диверсійних актів в Україні.

Крім того, встановлено, що один із контрагентів фізичної особи внесений до бази даних «Миротворець» як посібник російських окупантів, який добровільно обійняв посаду в незаконних органах влади на тимчасово окупованій території.

Таким чином, є підстави вважати фінансові операції, здійснені по рахунках **Фізичної особи**, спрямовані на фінансування тероризму та організацію незаконних дій на території України.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2025.4.1.3. Отримання доходів фізичною особою від забороненої соціальної мережі

Держфінмоніторингом виявлено підозрілі фінансові потоки за рахунками **Фізичної особи**, здійснені готівковим і безготівковим шляхом, у тому числі за участі третіх осіб.

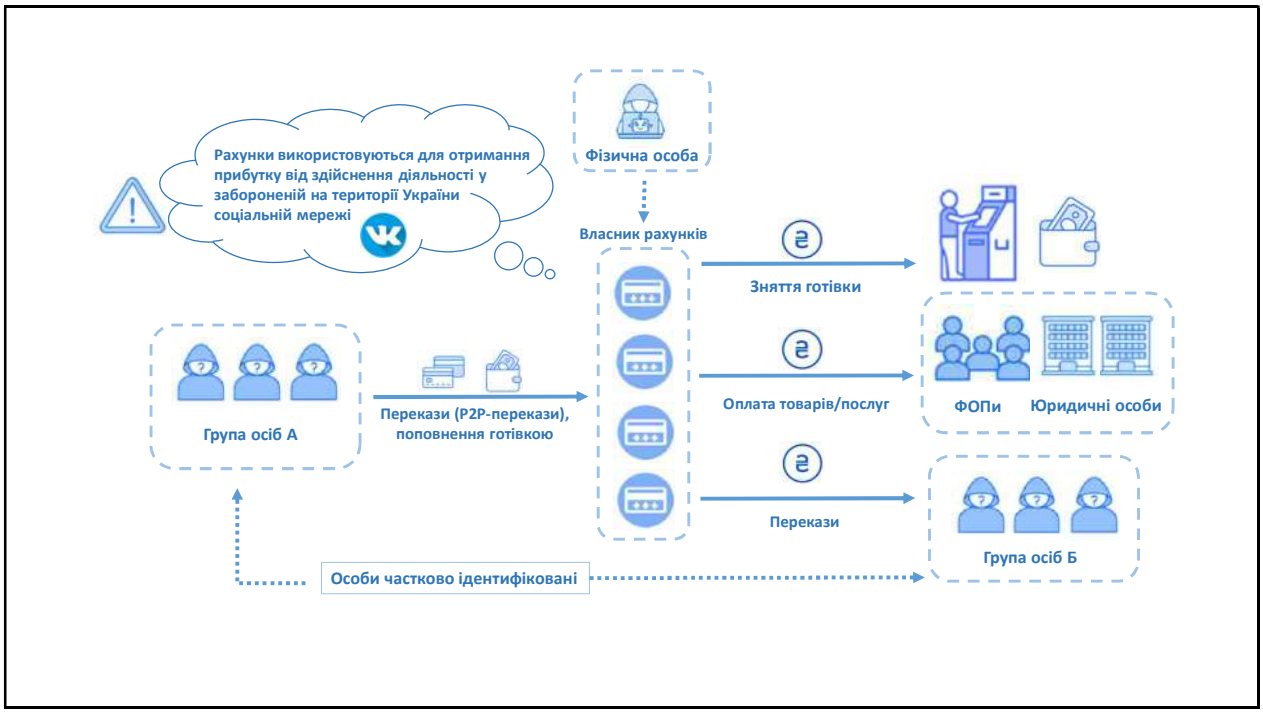
Встановлено, що на рахунки **Фізичної особи** надходили кошти від **Групи осіб А** (невстановлених та частково встановлених) шляхом зарахування P2P-переказів та поповнення готівкою.

Надалі кошти фізичною особою частково знімалися готівкою, частково перераховувалися іншій **Групі осіб Б** (невстановлених та частково встановлених), а також на користь ФОПів та юридичних осіб у якості оплати товарів і послуг. При цьому **Фізична особа** офіційно не працевлаштована та отримує доходи як самозайнята особа.

Встановлено, що **Фізична особа** використовувала рахунки для отримання прибутків з країни, яка здійснює збройну агресію проти України, від здійснення сумнівної діяльності у забороненій на території України соціальній мережі. Також є підозра щодо проведення **Фізичною особою** фінансових операцій на значні суми для здійснення прихованої комерційної діяльності, у тому числі на сайтах, пов'язаних з організацією проведення нелегальних азартних ігор.

Таким чином, є підстави вважати, що фінансові операції, пов'язані із зарахуванням коштів на рахунки **Фізичної особи**, можуть бути пов'язані з колабораційною діяльністю та ухиленням від сплати податків.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2025.4.1.4. Шахрайська діяльність в IT-сфері, яка спрямована на фінансування тероризму

Держфінмоніторингом, з урахуванням інформації, отриманої від державного органу, ПФР іноземної держави та суб'єктів первинного фінансового моніторингу, виявлено фінансові операції ряду **Фізичних осіб**, які потенційно можуть бути причетні до діяльності урядових організацій країни, що знаходиться у списку держав-терористів та допомагає російській федерації у війні проти України.

Окремим державним органом України надано інформацію щодо систематичного використання урядовими організаціями Північної Кореї українських IT-працівників у шахрайській діяльності, доходи від якої використовуються для фінансування діючого режиму підсанкційної та терористичної держави.

Щодо ряду цих **Фізичних осіб** наявні повідомлення СПФМ про підозрілу діяльність, переважно пов'язану з несанкціонованим доступом до

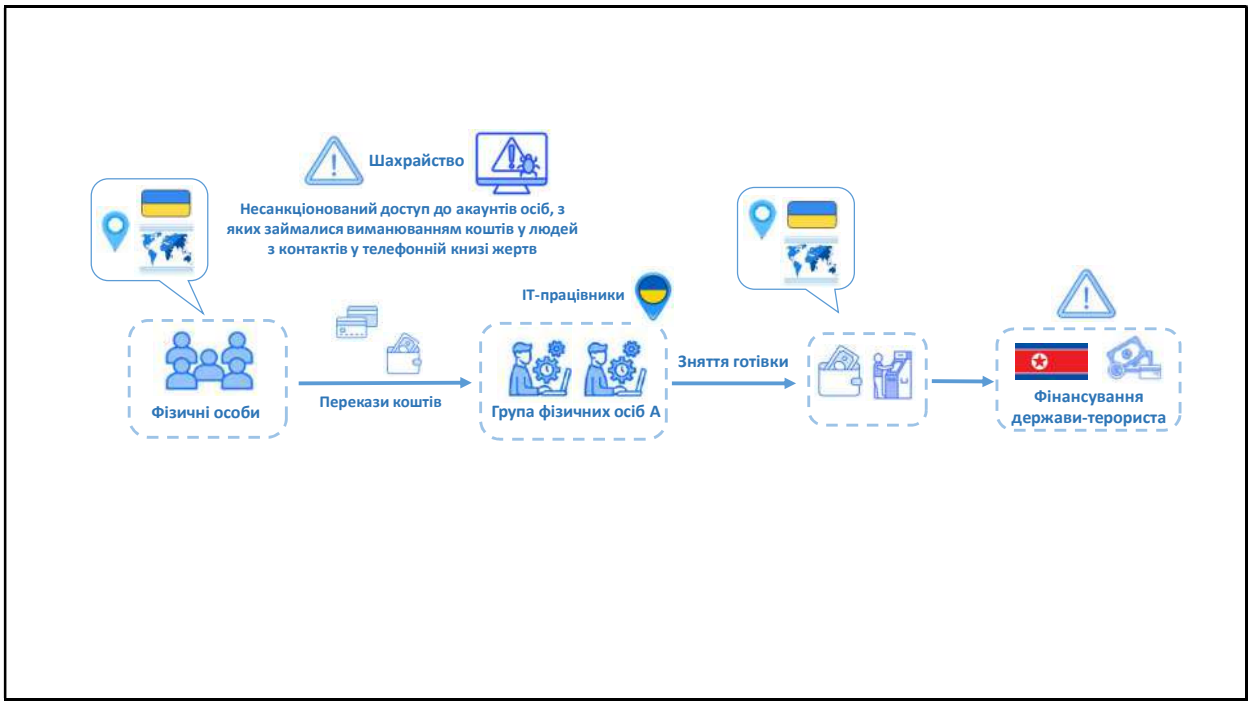
акаунтів осіб, виманюванням коштів у людей із контактів у телефонній книзі жертв, транзитом коштів із подальшим зняттям готівки.

Крім того, наявна негативна інформація від ПФР іноземної держави щодо ряду громадян України, які здійснювали операції, що вважалися підозрілими у контексті потенційного сприяння діяльності Північної Кореї, спрямованої на отримання доходів у кіберпросторі.

Встановлено, що на рахунки **Групи фізичних осіб А**, які є українськими ІТ-працівниками, надходили перекази коштів з картки на картку та готівкові перекази від різних фізичних осіб з українських та іноземних банківських рахунків. Надалі **Групою фізичних осіб А** знімалася готівка як на території України, так і за кордоном. Суми здійснених операцій не відповідають офіційно задекларованим доходам фізичних осіб, більшість із яких є офіційно безробітними.

Враховуючи викладене, є підстави вважати, що кошти, використані **Групою фізичних осіб А**, можуть мати незаконне походження внаслідок шахрайства та співпраці з урядовими підприємствами підсанкційної та терористичної держави.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2025.4.1.5. Надання громадянином України криптовалюти для фінансування збройних формувань агресора

Держфінмоніторингом, з урахуванням інформації правоохоронного органу та СПФМ, виявлено схему, пов’язану з добровільним фінансуванням громадянином України збройних сил рф, які ведуть агресивну війну проти України.

Правоохоронним органом надано інформацію, що **Фізична особа А**, яка є громадянином України, на криптовалютній біржі «Binance» перерахувала криптовалюту згідно з реквізитами криптогаманців, розміщеними у російських та проросійських Telegram-каналах, які здійснюють збір коштів для закупівлі збройними формуваннями рф безпілотних летальних апаратів, обладнання, техніки тощо.

Виявлено підозрілі фінансові операції по рахунках **Фізичної особи А**, відкритих у банківських установах, значна частина яких стосувалася проведення численних зарахувань та переказів з карток та на картки невстановлених осіб, операцій з готівкою (у тому числі за межами України), розрахунків за товари (у тому числі в російських рублях).

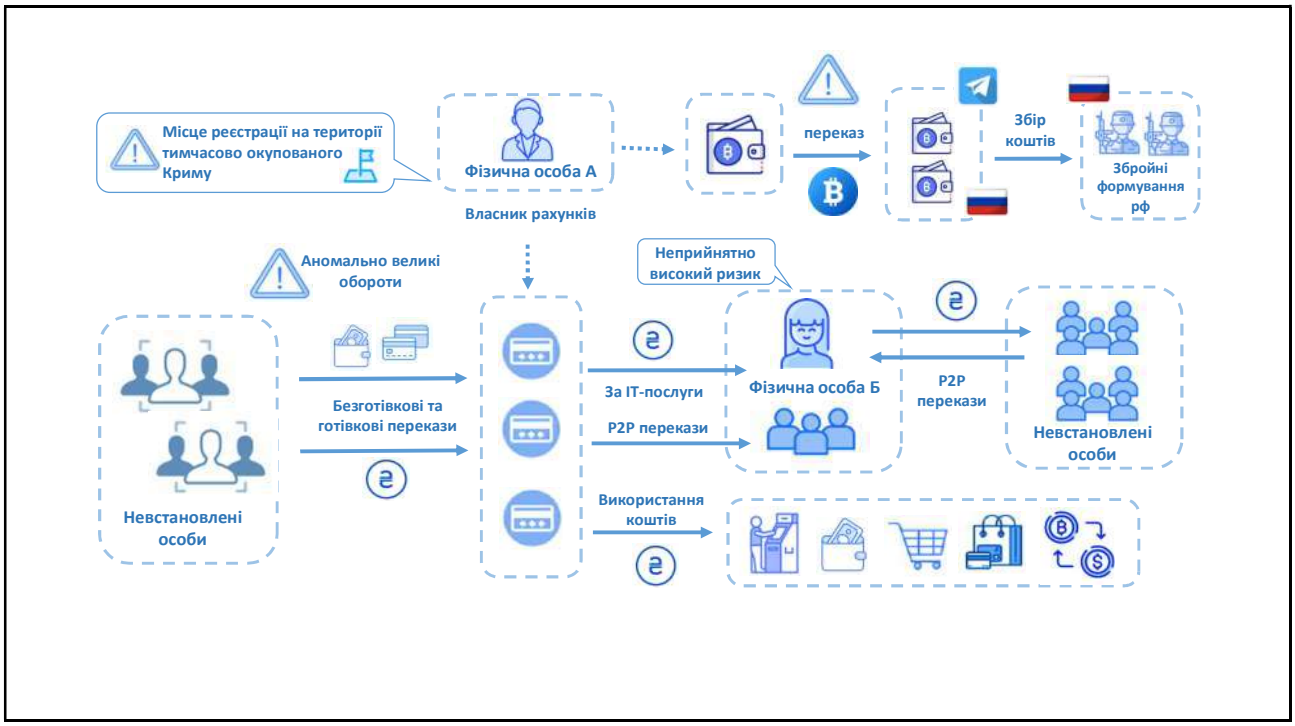
Встановлено здійснення переказів коштів на користь групи осіб, у тому числі на користь **Фізичної особи Б**, зареєстрованої в прифронтовій зоні, стосовно якої банківською установою було встановлено неприйнятно високий ризик та розірвано ділові відносини.

По рахунках **Фізичної особи Б**, яка на той час була новоствореним підприємцем, виявлено транзитне переміщення коштів, отриманих як поповнення рахунку та оплата ІТ-послуг, з подальшим перерахуванням на користь великої кількості фізичних осіб.

Відомо, що адресою реєстрації **Фізичної особи А** є тимчасово окупована територія АР Крим, а адресою тимчасового перебування – Київська область.

Враховуючи викладене, встановлено, що фінансові операції зазначених фізичних осіб спрямовані проти основ національної безпеки України та на надання допомоги збройним формуванням рф у веденні агресивної війни проти України.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2025.4.1.6. Схема фінансування терористично-диверсійної діяльності з тимчасово окупованих територій України

Держфінмоніторингом, з урахуванням інформації, отриманої від СПФМ та правоохоронного органу, виявлено підозрілі фінансові операції на рахунках групи фізичних осіб, які підозрюються в участі у терористично-диверсійній діяльності на території України в інтересах країни-агресора.

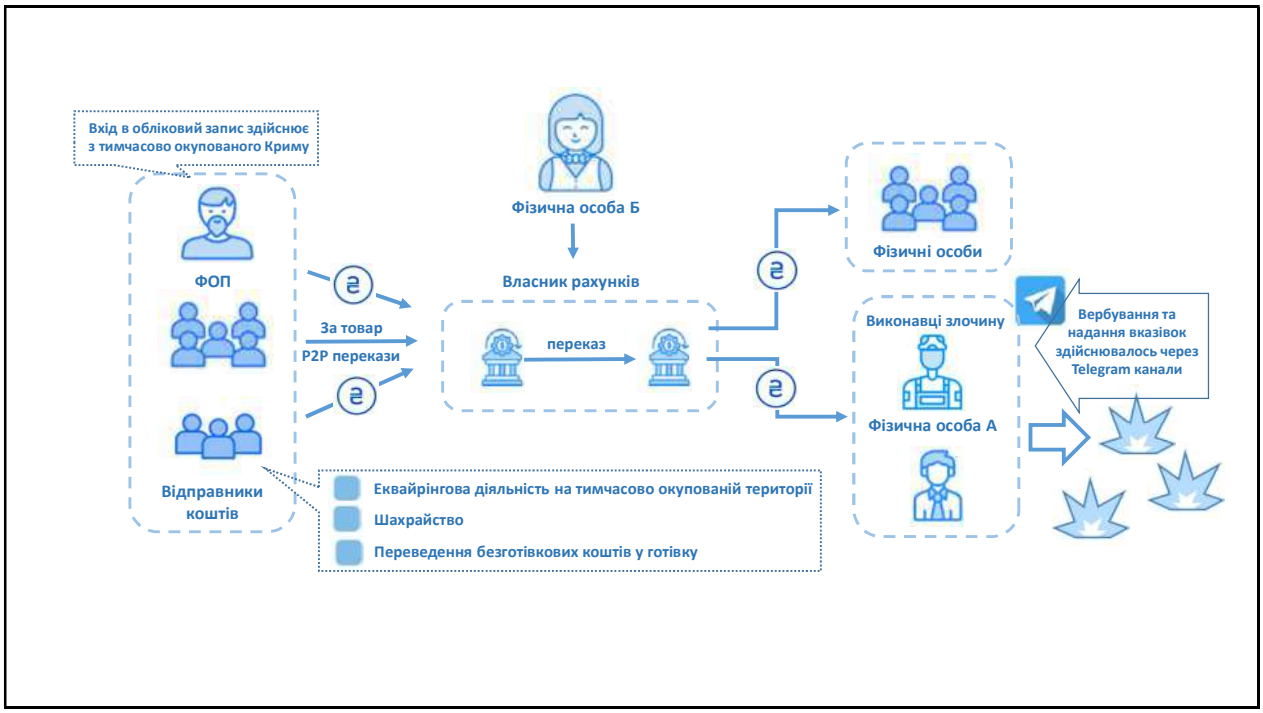
Правоохоронним органом надано інформацію, що представниками спецслужб рф через Telegram-канал на тематичних сайтах з пошуку роботи розміщувалися оголошення щодо легкого заробітку великих коштів за вчинення різноманітних диверсійних дій на території України.

Відомо, що до такої діяльності було залучено двох громадян України, зокрема **Фізичну особу А**, які за вказівками організаторів здійснили підпал об'єкта, що має важливе господарське та оборонне значення. Крім того, відомо, що для придбання засобів для вчинення підпалу **Фізична особа А** отримала кошти з особового рахунку **Фізичної особи Б**.

Встановлено, що на ім'я **Фізичної особи Б** відкрито рахунки як фізичної особи-підприємця (ФОП), так і як фізичної особи. На рахунки ФОП надходили безготівкові платежі за товари, закупівлю яких вона не могла підтвердити, до того ж обсяги надходжень перевищували суми очікуваних/запланованих доходів. У подальшому зараховані кошти здебільшого перераховувалися на власні рахунки, відкриті вже як фізичній особі, і одразу перенаправлялися на користь різних осіб без зазначення мети, у тому числі – на користь **Фізичної особи А**.

Крім того, серед зарахувань на рахунок **Фізичної особи Б** виявлено переказ від **ФОП**, стосовно якого встановлено, що його контрагентами по рахунку є мешканці тимчасово окупованої території (Херсонська область), а входи в його обліковий запис здійснюються з території тимчасово окупованого Криму. Стосовно деяких інших контрагентів **Фізичної особи Б** банківськими установами повідомлено про підозрілу діяльність, пов'язану з еквайринговою діяльністю на тимчасово окупованих територіях України, конвертацією безготівкових коштів у готівку та фіктивним підприємництвом.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2025.4.1.7. Фінансування розвідувально-підривної діяльності з використанням суб'єктів господарської діяльності

Держфінмоніторингом, з урахуванням інформації правоохоронного органу, виявлено схему використання реквізитів суб'єктів господарської діяльності, підконтрольних представникам країни-агресора, для фінансування розвідувально-підривної діяльності на території України.

Правоохоронним органом поінформовано про те, що спецслужби рф залучають громадян України – переважно осіб літнього віку, які, виконуючи завдання спецслужб, через каси банківських установ перераховують грошові кошти на рахунки суб'єктів господарської діяльності, підконтрольних представникам країни-агресора.

При цьому передача готівкових коштів особам літнього віку здійснюється через агентів (кур'єрів) спецслужб рф.

Держфінмоніторингом виявлено фінансові потоки, пов'язані із зарахуванням на користь трьох **Компаній А, Б, В** – значної суми коштів від великої кількості фізичних осіб як оплати за товари та/або послуги з використанням банківських установ та платіжних систем.

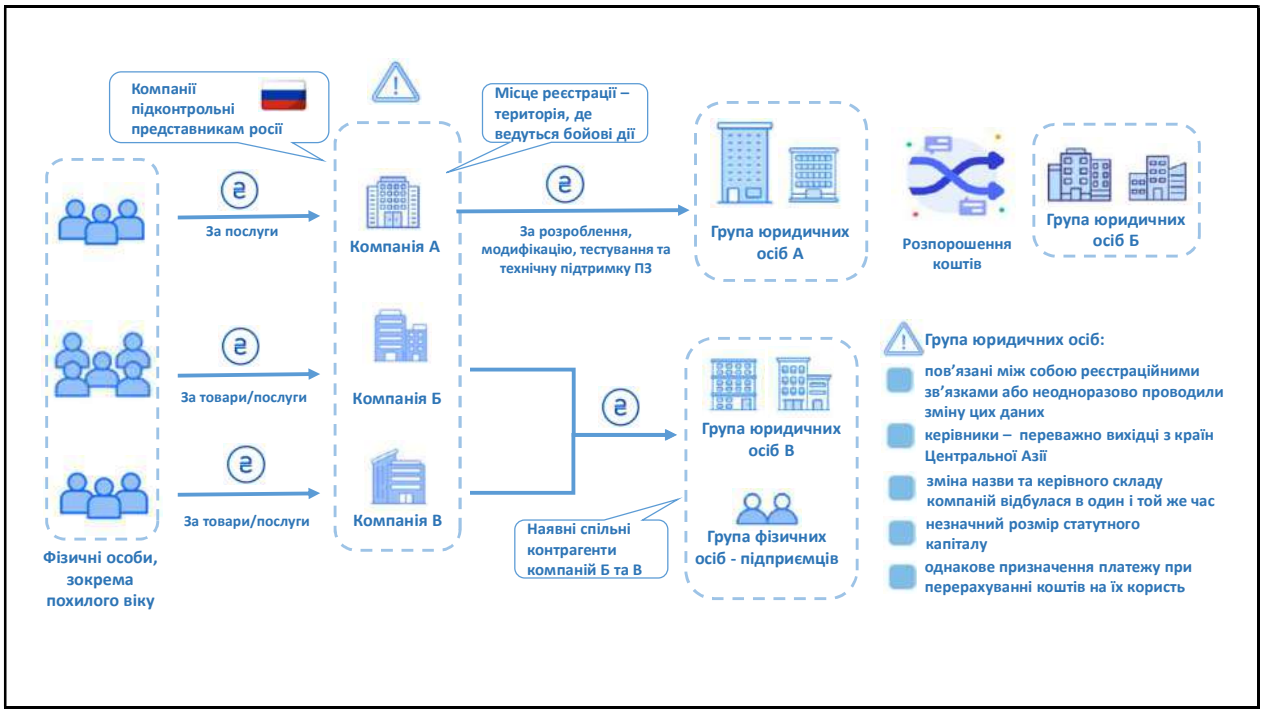
У подальшому отримані кошти **Компанією А** були перераховані на користь **Групи юридичних осіб А** як оплата за розроблення, модифікацію, тестування та технічну підтримку програмного забезпечення, які згодом були розподілені між **Групою юридичних осіб Б** як оплата за різноманітні товари та послуги.

Компаніями Б та В отримані кошти також були перераховані на користь **Групи юридичних осіб** та **фізичних осіб** –підприємців, у тому числі на користь спільних контрагентів.

Юридичні особи, що входять до **Групи**, мають ознаки фіктивності та характеризуються таким: пов'язані між собою реєстраційними зв'язками або неодноразово змінювали ці дані; мають однаковий основний вид діяльності; зміна назви та керівного складу компаній відбулася одночасно; керівники — переважно вихідці з країн Центральної Азії; незначний розмір статутного капіталу; при перерахуванні коштів на їхню користь зазначено однакове призначення платежу.

Таким чином, існує ймовірність використання рахунків юридичних та фізичних осіб для вчинення дій, спрямованих на отримання доходу від злочинної діяльності та подальшого його використання для фінансування тероризму.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2025.4.1.8. Залучення неповнолітніх до підпалу автомобілів[19]

Служба безпеки та Національна поліція затримали підпалювачів, які на замовлення російських спецслужб діяли на Одещині. Фігурантами виявилися шестеро учнів віком від 13 до 15 років, які шукали «легкі заробітки» у Телеграм-каналах.

За вказівкою окупантів їхні поплічники палили автомобілі українських військових. Коли неповнолітні намагалися «згорнути співпрацю» з окупантами, тоді представники російських спецслужб переходили до погроз та шантажу школярів.

За матеріалами справи, фігуранти діяли порізно. Спочатку шукали потенційні цілі, а потім «погоджували» їх зі своїми російськими кураторами та підпалювали за допомогою легкозаймистих сумішей.

[19] https://ssu.gov.ua/novyny/sbu-ta-natspolitsiia-zatrymaly-6kh-nepovnolitnikh-yaki-na-zamovlennia-rf-palyly-avto-zsu

Під час обшуків у затриманих вилучено мобільні телефони із доказами їхньої підривної діяльності на користь російської федерації.

За всіма викритими фактами затриманим повідомлено про підозру відповідно до вчинених злочинів за двома статтями КК України: ч. 1 ст. 114-1 (перешкоджання законній діяльності ЗСУ та інших військових формувань в особливий період);ч. 2 ст. 194 (умисне пошкодження майна шляхом підпалу).

Зловмисникам загрожує до 10 років позбавлення волі.

Приклад 2025.4.1.9. Залучення неповнолітніх до закладання вибухового пристрою[20]

Контррозвідка Служби безпеки України на випередження викрито двох неповнолітніх, які на замовлення російської федерації намагалися підірвати таунхаус, де проживав воїн Сил оборони.

Для вчинення злочину фігуранти залишили біля входу в будинок саморобний вибуховий пристрій (СВП), який заховали в горщику для квітів. Щоб російські спецслужбісти могли дистанційно активувати вибухівку у момент наближення військового до помешкання, агенти додатково встановили на «локації» телефонну камеру з віддаленим доступом для куратора з рф.

Співробітники Служби безпеки України затримали виконавців «на гарячому», коли вони заклали СВП на вході до таунхаусу.

За матеріалами справи, фігурантами виявилося двоє мешканців Львова віком 14 та 15 років, яких ворог завербував на Телеграм-каналах з пошуку «легких заробітків».

Після інструктажу від окупантів юнаки отримали координати, за якими забрали зі схрону вибухівку, а потім заклали її на місці запланованого теракту. Під час викриття у фігурантів вилучили споряджену вибухівку та смартфони із доказами контактів з куратором.

Слідчі СБУ повідомили їм про підозру за ч. 2 ст. 15, ч. 2 ст. 258 Кримінального кодексу України (закінчений замах на вчинення терористичного акту за попередньою змовою групою осіб). Їм загрожує до 12 років позбавлення волі з конфіскацією майна.

[20] https://ssu.gov.ua/novyny/sbu-zapobihla-shche-odnomu-teraktu-u-lvovi-dlia-vstanovlennia-vybukhivky-rf-zaverbuvala-dvokh-nepovnolitnikh-video

Приклад 2025.4.1.10. Втягнення неповнолітніх осіб у злочинну діяльність під виглядом «квест-ігор»[21]

Служба безпеки України та Національна поліція викрили втягнення російськими спецслужбами неповнолітніх українців у злочинну діяльність під виглядом «квест-ігор».

У результаті багатоетапної спецоперації в Харкові правоохоронці затримали дві агентурні групи ФСБ, які складалися винятково з дітей віком 15 і 16 років. Неповнолітні виконували ворожі завдання з проведення розвідки, коригування ударів та підпалів. Для маскування підривної діяльності обидва ворожі осередки діяли окремо один від одного.

За «правилами квест-гри» діти отримували від ФСБ геолокації, після чого їхнім завданням було дістатися до визначеної точки, зробити фото та відео об'єкта, а також надати короткий опис місцевості. Отримані у такий спосіб розвідувальні дані кожна з агентурних груп надсилала своєму куратору з ФСБ через анонімні чати.

Надалі окупанти використовували ці відомості для здійснення повітряних ударів по Харкову. Співробітники СБУ затримали всіх учасників ворожих груп під час фотографування об'єктів української ППО, яка захищає місто.

Під час розслідування також було виявлено ще одне завдання російських агентів – підпали трансформаторів, що забезпечують рух ешелонів Збройних Сил України у напрямку східного фронту.

Також встановлено особу «зв'язкового» агентурних груп ФСБ – ним виявився співробітник поліції Краснодарського краю російської федерації, який співпрацює з російською спецслужбою.

Організаторам повідомили про підозру за ч. 2 ст. 113 КК України (диверсія, вчинена в умовах воєнного стану). Фігурантів взято під варту та їм загрожує довічне ув'язнення.

[21] https://ssu.gov.ua/novyny/sbu-ta-natspolitsiia-zatrymaly-u-kharkovi-nepovnolitnikh-yaki-shpyhuvaly-dlia-fsb-pid-vyhliadom-kvesthry

РОЗДІЛ 4.2. ОБХІД САНКЦІЙ ТА ФІНАНСОВИХ ОБМЕЖЕНЬ

Цивілізований світ продовжує посилювати санкційний тиск на російську федерацію, позбавляючи її економічної основи для ведення війни.

Під тиском обмежень російська федерація змушена все більше шукати обхідні фінансові шляхи: серед них – обхід через віртуальні активи, «сірий» імпорт, торгівлю через компанії-прокладки та треті країни, а також постачання технологій та компонентів через мережі посередників.

Попри зусилля міжнародної спільноти, «тіньові» потоки та механізми обходу санкцій залишаються актуальними, що підкреслює необхідність постійного міжнародного моніторингу, координації та жорсткіших заходів для перекриття каналів фінансування агресії.

Санкції, спрямовані на послаблення економіки росії, обмеження її доступу до фінансів, технологій та світових ринків, виступають сигналом міжнародної підтримки України та єдності світової спільноти проти тероризму. Головна мета запроваджених обмежень – нанесення відчутного удару по енергетичному, банківському та військовому секторах росії.

У липні 2025 року Рада ЄС ухвалила 18-й пакет санкцій проти 14 осіб і 41 організацію, зокрема, проти постачальників російської оборонної промисловості, які відповідальні за дії, що підривають або загрожують територіальній цілісності, суверенітету та незалежності України.

Загалом кількість осіб у санкційних списках перевищила 2500. Також ЄС знизив цінову стелю на нафту з 60 до 47,6 доларів США за барель, запровадив автоматичний динамічний механізм її перегляду та посилив санкції проти так званого «тіньового флоту» агресора, який допомагає обходити санкції.

У жовтні 2025 року США запроваджено санкції проти російських нафтових компаній «Лукойл», «Роснафта» та їхніх «дочок». До списку потрапило понад 30 підрозділів – від нафтових родовищ до газових і нафтопереробних заводів по всій росії. На компанії «Роснафта» й «Лукойл» припадає близько половини добового видобутку нафти в рф. Зокрема, «Роснафта» забезпечує приблизно 17% доходів російського бюджету.

Як показує практика фінансових розслідувань, ключовими шляхами обходу є: використання посередників та компаній з країн, які не приєдналися до санкцій; створення схем із заниженою вартістю товарів для уникнення податків; а також розвиток власного виробництва або імпорту товарів з Азії. Крім того, деякі підсанкційні компанії використовують криптовалюти для проведення платежів, що ускладнює відстеження транзакцій.

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

Приклад 2025.4.2.1. Обхід санкцій РНБО України[22]

Компанія-резидент – виробник промислових товарів (насосів), що входить до складу російського бізнес-холдингу та має кінцевого бенефіціара – **Громадянина рф**, щодо якого запроваджено санкції РНБО України, до 24.02.2022 здійснювала основне постачання продукції російським контрагентам.

Після початку повномасштабної агресії рф **Компанія-виробник**, згідно з відкритими джерелами та матеріалами кримінального провадження, продовжила виконання контрактів із російськими підприємствами, використовуючи механізми обходу санкційних обмежень.

За результатами аналізу встановлено, що **Компанія-виробник** відвантажувала продукцію **Компанії-резиденту** (експортеру) за операціями, які мають ознаки фіктивності**:**

- розрахунки проводилися шляхом зарахування зустрічних однорідних вимог;
- наявність таких вимог (боргу) не підтверджена документально;
- економічна доцільність механізму розрахунків відсутня.

Надалі **Компанія-експортер** постачала продукцію**:**

- компаніям-посередникам нерезидентам (Казахстан);
- компанії-нерезиденту (Туреччина), яку, згідно з матеріалами кримінального провадження, визнано посередником, що постачав продукцію до рф.

На додаткові запити контролюючих органів щодо підтвердження кінцевого споживача продукції компанія-експортер не надала інформації та документів, що свідчить про умисне приховування кінцевого ланцюга постачання.

Приклад 2025.4.2.2. Спроба проведення платежу на компанію, що приховує реальних власників – резидентів/громадян рф, з обходом санкційних обмежень[23]

Компанія-клієнт Банку виявила намір здійснити міжнародний платіж на користь Компанії-контрагента, зареєстрованої в Німеччині.

Компанія-контрагент була створена у 2022 році та декларує діяльність у сфері логістики, імпорту та експорту різноманітних товарів, у тому числі матеріалів для потреб в сфері хімії, промислового обладнання та мастильних матеріалів.

Кінцевим бенефіціарним власником **Компанії-контрагента** зазначена **Громадянка та Резидент Австрії** (далі – КБВ-1). Продаж компанії цій особі відбувся у жовтні 2022 року.

Водночас встановлено низку факторів ризику:

- попередній власник Компанії-контрагента – Громадянка рф;

[22] За даними НБУ
[23] За даними НБУ

- угоду про продаж частки підписували: попередній директор – Громадянин рф, родич попередньої власниці (одне прізвище), та новий директор – резидент Німеччини, народжений у Казахстані.

У відкритих джерелах виявлено профілі **КБВ-1** у соціальних мережах, у яких немає жодної згадки про **Компанію-контрагента**, а досвід та навички не відповідають її сфері діяльності.

Банк звернувся до Клієнта з вимогою надати докази, що підтверджують реальність КБВ. Проте отримана відповідь не спростувала підозр, оскільки складалася лише з формальних витягів із реєстрів, які Банк уже аналізував.

За результатами аналізу документів, наданих Клієнтом, та інформації з відкритих джерел Банк встановив ознаки приховування реального кінцевого бенефіціара **Компанії-контрагента**.

Наявні наступні ознаки ризику:

- відсутність документів, що підтверджують реальний вирішальний вплив КБВ-1 на діяльність компанії;
- наявність ознак номінального продажу з метою приховування реальних КБВ, пов'язаних із рф;
- дані, що свідчать про можливість того, що фактичним КБВ компанії є громадянин рф.

Приклад 2025.4.2.3. Схема «паралельного імпорту» для обходу санкцій[24]

Банком виявлено схему «паралельного імпорту», яка застосовувалася з метою обходу санкційних обмежень та заборон, установлених постановою Правління Національного банку України від 24.02.2022 № 18 «Про роботу банківської системи в період запровадження воєнного стану» (зі змінами), що забороняє здійснення будь-яких валютних операцій за участю юридичних або фізичних осіб, пов'язаних з рф чи рб.

Компанія-нерезидент, яка зареєстрована в юрисдикції з лояльним до країни-агресора режимом та вигідним логістичним розташуванням, замовила будівельну техніку у **Компанії-резидента України**, яка є офіційним представником **нерезидента-Виробника**. У документах нерезидент декларував, що техніка буде використовуватися та реалізовуватися виключно в межах своєї країни реєстрації.

Під час аналізу зовнішньоекономічної діяльності **Компанії-нерезидента** встановлено, що вона активно здійснює експорт продукції до рф, у тому числі аналогічної до тієї, що закуповується у резидента України. Експортні операції здійснювались в супереч заявленій меті закупівлі.

На додаткові запити Банку щодо підтвердження фактичного використання та місця реалізації продукції **Компанія-нерезидент** надала суперечливу інформацію, яка не дозволяла підтвердити задекларовану мету імпорту.

[24] За даними НБУ

Приклад 2025.4.2.4. Використання стейблкоїна A7A5 та біржі Garantex для обходу міжнародних санкцій[25]

A7A5 – це стейблкоїн, підкріплений рублем, пов'язаний зі схемою ухилення від санкцій, створеною компанією, що належить російському державному банку, та молдавським втікачем, на якого поширюються санкції за втручання у вибори від імені російської федерації.

Загальний обсяг обміну A7A5 перевищив 8,5 мільярда доларів, при цьому емітент A7A5 влив понад 1,3 мільярда доларів ліквідності USDT у власну децентралізовану біржу за останні дні.

Зростаюча доступність та ліквідність A7A5 створює проблеми для міжнародних санкційних зусиль, оскільки вона надає російським організаціям ще один інструмент для здійснення транскордонних переказів поза банківською системою.

Невдовзі після запуску A7A5 було виставлено на торгівлю на санкціонованій російській криптовалютній біржі Garantex. Стейблкоїн Tether, долар США USDT, був найбільшим активом, яким на той час торгували на Garantex, російські користувачі віддавали перевагу його ціновій стабільності порівняно з волатильним рублем, широкій платіжній корисності та ролі в обході санкцій після того, як вітчизняні банки були відключені від SWIFT.

Однак централізований контроль USDT, включаючи його здатність заморожувати гаманці, став проблемою, коли Garantex був змушений відключитися від мережі Секретною службою США у березні 2025 року.

Garantex застосував складне маскування гаманців, щоб спробувати запобігти блокуванню своїх транзакцій іншими біржами, що дотримуються санкцій, та уникнути арешту активів, але Elliptic надала Секретній службі США розвідувальні дані про структуру гаманця Garantex, що дозволило заморозити 26 мільйонів USDT.

Приклад 2025.4.2.5. Схема постачання західної продукції до росії в обхід санкційних обмежень за участю нерезидентів-посередників

Держфінмоніторингом, з урахуванням інформації, отриманої від ПФР іноземної держави, виявлено підозрілу діяльність компаній-нерезидентів, спрямовану на сприяння країні-агресору у війні проти України шляхом підтримки військово-промислового комплексу російської федерації (ВПК рф), ухилення від міжнародних санкцій та обходу експортного контролю.

ПФР іноземної держави надано інформацію щодо підозрілої діяльності **Компанії-нерезидента А**, зареєстрованої в одній з азійських країн, та **Групи підставних компаній**, які вона контролює. Діяльність цієї структури містить ознаки порушень, за які передбачено санкції за підтримку ВПК рф.

[25] https://www.elliptic.co/blog/the-rise-of-a7a5-the-ruble-stablecoin-now-transfers-1-billion-per-day?utm_source=chatgpt.com

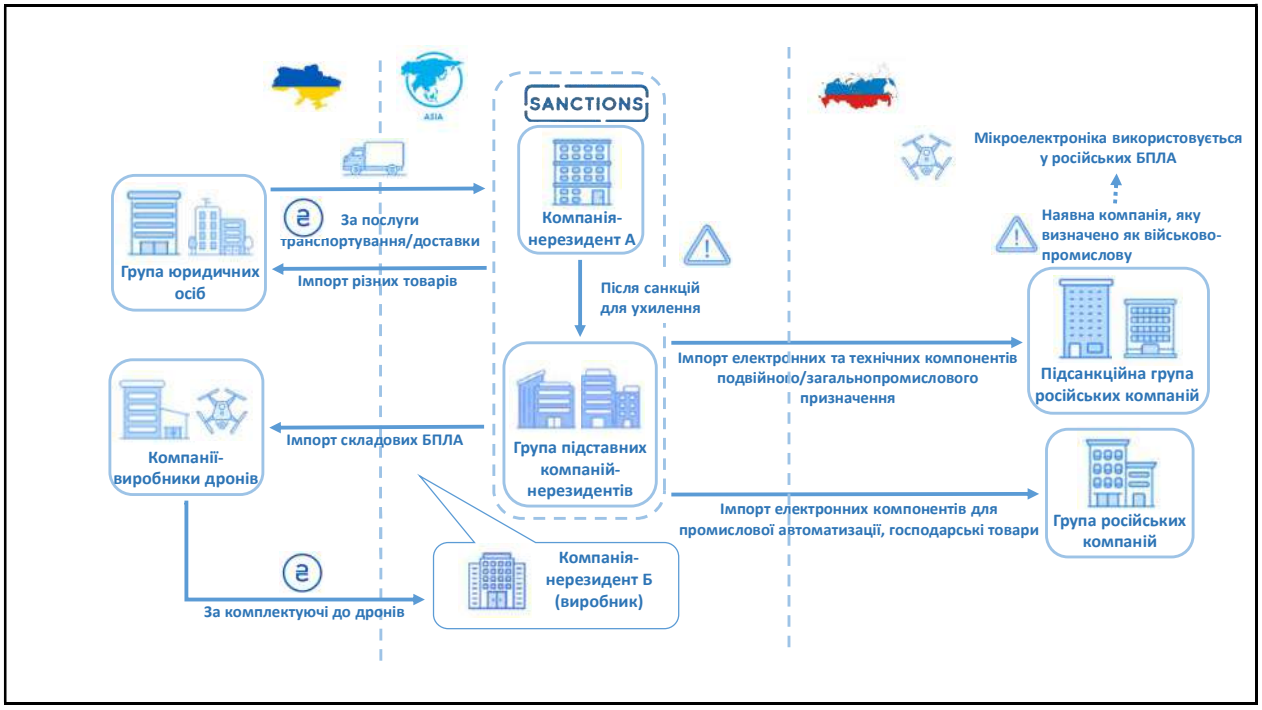
Встановлено, що **Компанія-нерезидент А**, включена до санкційного списку OFAC, постачала електронні компоненти, у тому числі мікроелектроніку подвійного призначення, до групи російських компаній, які входять до складу ВПК рф. Зазначена продукція використовується у виробництві російських БПЛА, що застосовуються під час атак на територію України.

Після запровадження санкцій **Компанія-нерезидент А** продовжила діяльність через мережу підставних компаній-нерезидентів, зареєстрованих у тій самій азійській країні, з метою приховування своєї участі та подальшого обходу експортних обмежень.

Встановлено, що певна українська група юридичних осіб у період до запровадження санкцій здійснювала перерахування коштів на користь **Компанії-нерезидента А** за імпорт товарів та послуги з транспортування/доставки. Після введення санкцій ця українська група продовжила співпрацю вже з підставними компаніями-нерезидентами, що фактично представляли інтереси санкційної компанії.

Відомо, що **одна з підставних компаній-нерезидентів** постачає комплектуючі до БПЛА від імені фактичного виробника цих компонентів на користь українських виробників дронів, які здійснюють прямі розрахунки з виробником. Це може свідчити про використання підставної компанії для маскування ланцюгів постачання та мінімізації ризику викриття санкційних порушень.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2025.4.2.6. Незаконний імпорт продукції, виробником якого є підприємства країни-агресора

Держфінмоніторингом, з урахуванням інформації, наданої правоохоронним органом, виявлено фінансові операції, спрямовані на свідоме ухилення від законодавчих обмежень щодо імпорту товарів та провадження господарської діяльності у взаємодії з представниками держави-агресора.

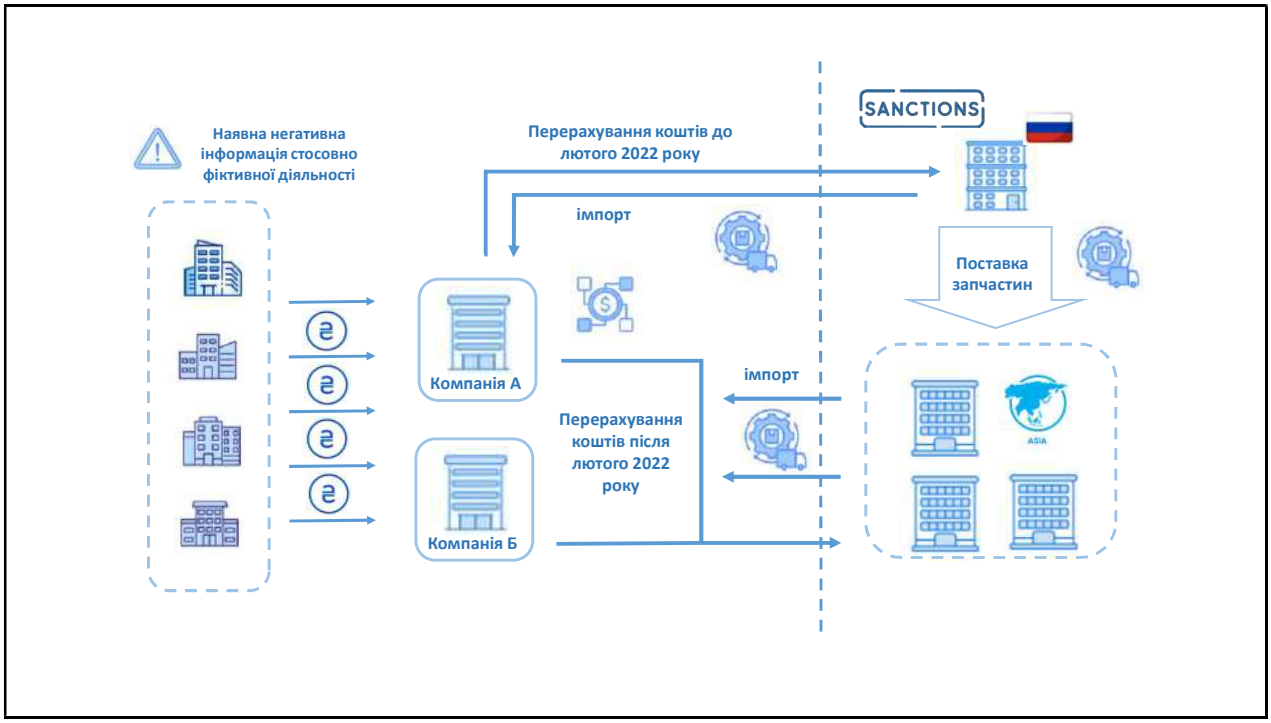
Відомо, що два пов'язані між собою українські підприємства – **Підприємства А** та **Б** – з моменту повномасштабного вторгнення здійснюють імпорт та реалізацію автомобільних запчастин, виробниками яких є суб'єкти з підсанкційних країн (росія, білорусь), використовуючи фірми-«прокладки» з третіх країн для обходу заборони на прямий імпорт з рф.

Встановлено, що до початку повномасштабної агресії **Підприємство А** напряму імпортувало запчастини з території росії та здійснювало розрахунки з російськими постачальниками. Проте після лютого 2022 року підприємство почало перераховувати кошти на користь компаній-нерезидентів, зареєстрованих у країні, яка активно співпрацює з рф.

Крім того, встановлено, що деякі контрагенти **Підприємств А** та **Б** раніше підтримували прямі або опосередковані господарські відносини з підприємствами рф. Також щодо основних контрагентів наявна негативна інформація, зокрема підозри у здійсненні фіктивного підприємництва та транзитної діяльності.

Враховуючи викладене, є підстави вважати, що діяльність **Підприємств А** та **Б**, пов'язана з перерахуванням коштів за запчастини російського походження на користь компаній-«прокладок», має ознаки пособництва державі-агресору та умисного ухилення від дії законодавчих обмежень.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2025.4.2.7. Незаконне постачання українських товарів на користь підсанкційної компанії країни-агресора

Держфінмоніторингом, з урахуванням інформації правоохоронного органу та ПФР іноземної держави, виявлено схему незаконного постачання українських товарів на користь підсанкційної компанії, зареєстрованої на території країни-агресора.

Встановлено, що напередодні повномасштабного вторгнення українське **Підприємство А** уклало договір на поставку обладнання з російською **Компанією Б**, з якою мало тривалі бізнес-відносини.

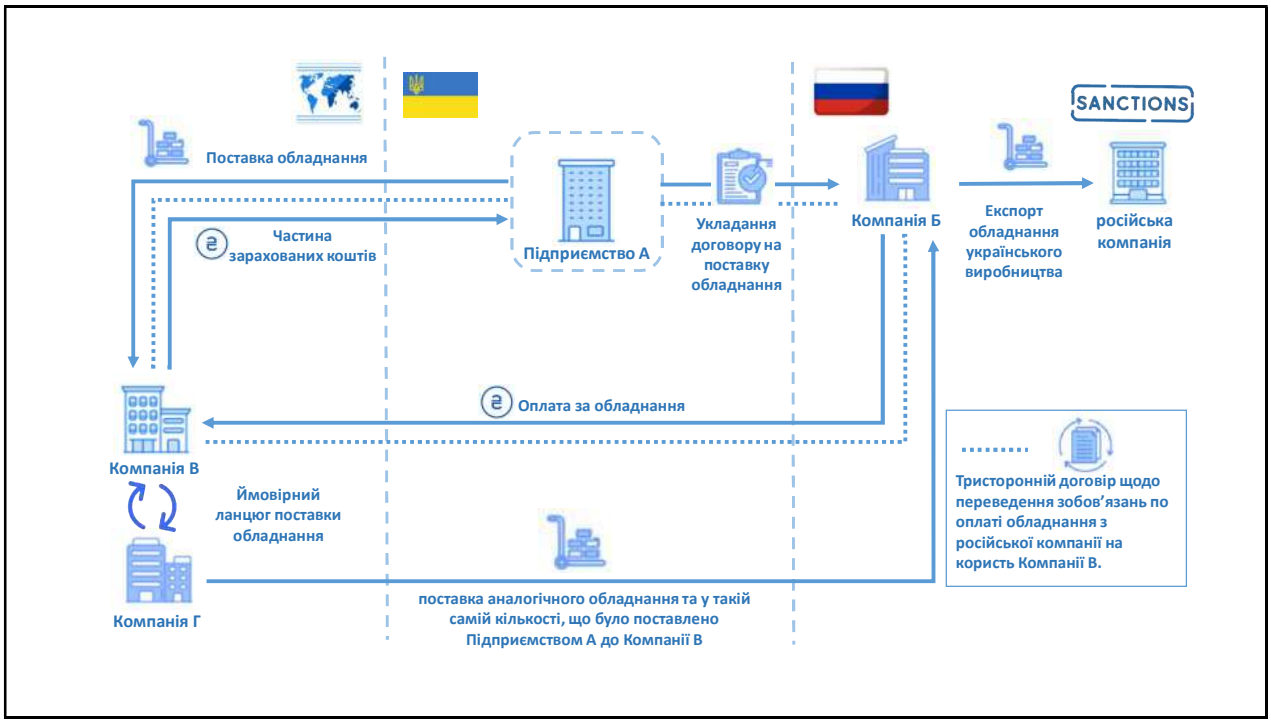
Через невеликий проміжок часу після початку повномасштабного вторгнення між **Підприємством А**, російською **Компанією-нерезидентом Б** та **Компанією В**, зареєстрованою на території іншої країни, було укладено тристоронній договір про переведення боргу – щодо передачі зобов'язань з оплати обладнання від російської компанії на користь **Компанії В**.

Надалі на рахунок **Компанії В** було зараховано кошти від російської компанії як оплату за обладнання, частину з яких переказано на користь українського **Підприємства А**.

Відомо, що **Підприємство А** здійснило поставку обладнання на користь **Компанії-нерезидента В**. Водночас у відкритих джерелах встановлено, що в той самий період інша **Компанія-нерезидент Г** здійснила постачання обладнання з ідентичним найменуванням та у такій самій кількості на користь російської **Компанії Б**. За інформацією правоохоронного органу, **Компанія Б** постачає обладнання іншій російській компанії, щодо якої в Україні запроваджено санкції.

Таким чином, існують обґрунтовані підозри, що, незважаючи на повномасштабну війну, **Підприємство А** не припинило підтримання ділових відносин із представниками російського бізнесу, а обладнання українського виробництва могло бути поставлено через ланцюг компаній-нерезидентів на користь підсанкційної компанії країни-агресора.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2025.4.2.8. Схема легалізації коштів підприємством, підконтрольним особі, стосовно якої застосовано санкції

Держфінмоніторингом, з урахуванням інформації, отриманої від суб'єктів первинного фінансового моніторингу та правоохоронного органу, виявлено фінансову операцію, спрямовану на виведення та легалізацію коштів з підприємства, підконтрольного особі, стосовно якої застосовано санкції.

Встановлено, що **Компанія А**, підконтрольна фізичній особі, щодо якої застосовано обмежувальні заходи (санкції) за співпрацю з країною-агресором, отримала кошти від **Компанії Б** за договором позики, які не були повернуті у встановлений строк. Через короткий проміжок часу **Компанія Б** передала право вимоги за договором позики **Компанії В**, яка, у свою чергу, переуступила це право **Компанії Д**.

Щодо **Компанії Д** відкрито провадження у справі про банкрутство за позовом кредиторів, у межах якого **Компанія Д** звернулася до суду з вимогою про стягнення коштів з **Компанії А** за договором переведення боргу. Суд задовольнив цю вимогу.

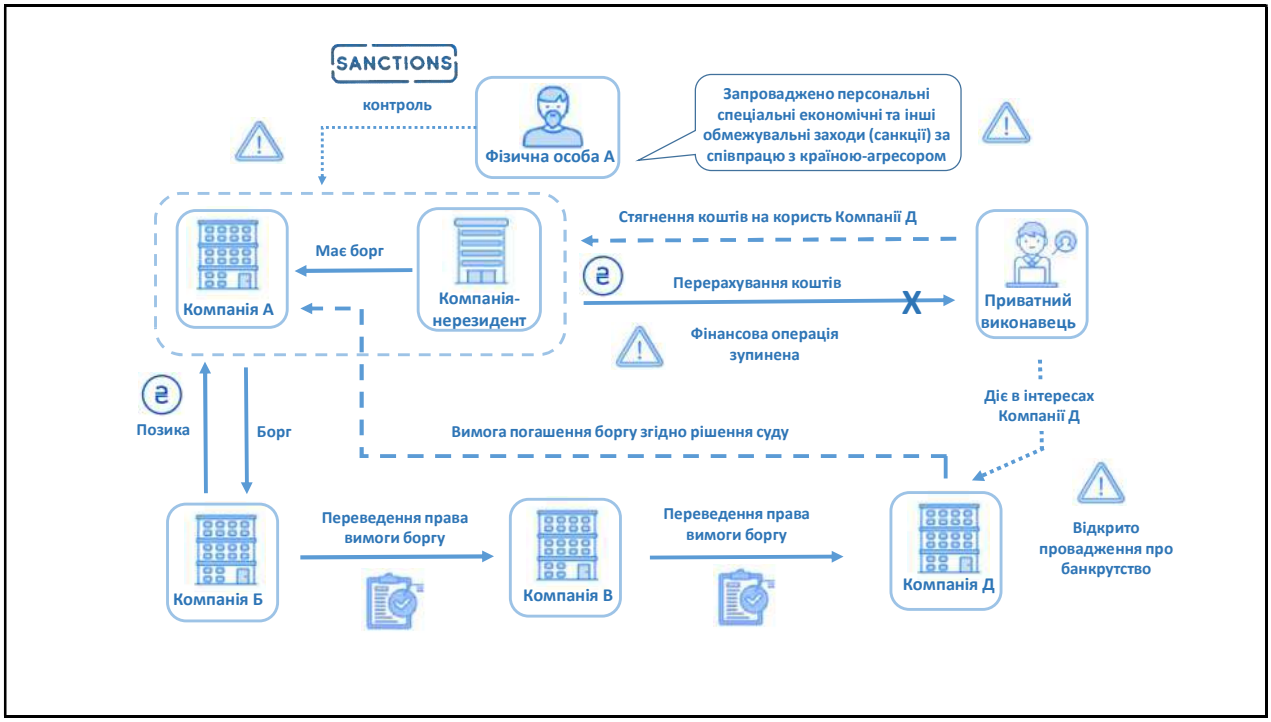
У подальшому приватний виконавець, який діє в інтересах **Компанії Д**, виніс постанову про відкриття виконавчого провадження стосовно **Компанії А**, оскільки боржник не виконує рішення суду, на рахунках бракує коштів, а майном він не володіє. Надалі суд ухвалив рішення про звернення стягнення на рахунок **Компанії-нерезидента**, яка має заборгованість перед **Компанією А**, з метою задоволення вимог **Компанії Д**.

Відомо, що **Компанія-нерезидент** також підконтрольна фізичній особі, щодо якої застосовано обмежувальні заходи (санкції) за співпрацю з країною-агресором.

Враховуючи вищевикладене, банком було прийнято рішення про зупинення фінансової операції зі списання коштів з рахунку **Компанії-нерезидента** на користь приватного виконавця.

Таким чином, є підстави вважати, що описана схема була організована з метою легалізації коштів компанією, підконтрольною підсанкційній особі, із використанням удаваних договорів позики та переуступок прав вимоги.

Правоохоронним органом накладено арешт на рахунок, розслідування триває.



Приклад 2025.4.2.9. Обхід санкційних обмежень, запроваджених стосовно фізичної особи

Держфінмоніторингом, з урахуванням інформації, отриманої від суб'єктів первинного фінансового моніторингу та правоохоронного органу, виявлено фінансові операції, спрямовані на обхід санкційних обмежень, накладених на фізичну особу.

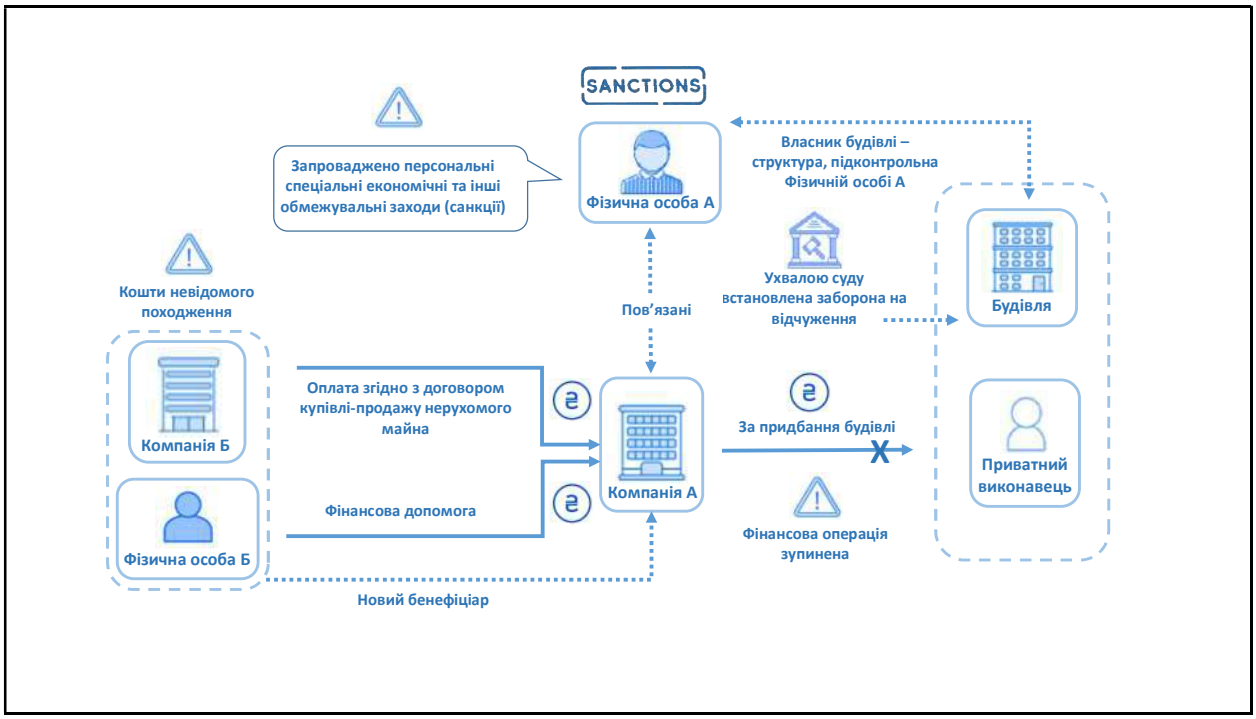
Встановлено, що з рахунку **Компанії А** було здійснено спробу перерахування коштів на користь **Приватного виконавця** з призначенням платежу «кошти за придбання лоту». Предметом торгів виступає об'єкт нерухомості, який є пам'яткою архітектури.

Відомо, що власником цієї нерухомості є структура, підконтрольна **Фізичній особі А**, стосовно якої запроваджено персональні спеціальні економічні та інші обмежувальні заходи (санкції). Крім того, ухвалою суду встановлено заборону на відчуження зазначеного майна. У зв'язку з цим банком було зупинено відповідну фінансову операцію.

Джерелом походження коштів на рахунку **Компанії А**, використаних для проведення зазначеної фінансової операції, були кошти невідомого походження, що були зараховані від **Компанії Б** як оплата за договором купівлі-продажу нерухомого майна, а також кошти від **Фізичної особи Б**, яка є новим бенефіціаром **Компанії А**, у вигляді фінансової допомоги.

Наявна інформація свідчить про можливу афілійованість **Компанії А** з **Фізичною особою А**. Зазначена фінансова операція, ймовірно, була здійснена з метою збереження контролю над об'єктом нерухомості всупереч запровадженим санкціям та з уникненням конфіскації в рамках відкритих кримінальних проваджень.

Правоохоронним органом здійснюється досудове розслідування.



РОЗДІЛ 4.3. КОРУПЦІЙНІ ЗЛОЧИНИ ТА СХЕМИ ВІДМИВАННЯ ЗЛОЧИННИХ ДОХОДІВ

У 2025 році корупція в Україні залишається однією з головних загроз, особливо в умовах військової агресії російської федерації.

Значне збільшення фінансування на нагальні рішення та великі оборонні закупівлі створює сприятливе середовище для корупційних зловживань.

Актуальність боротьби з корупцією в умовах війни. Корупція залишається однією з найсерйозніших загроз для стабільності, безпеки та розвитку держави. Війна, розпочата рф, загострила в суспільстві відчуття справедливості.

За даними дослідження Transparency International Ukraine за 2024 рік, Україна посідає 105 місце серед 180 країн за Індексом сприйняття корупції — 35 балів зі 100 можливих, що на 1 бал менше порівняно з 2023 роком.

Корупційні прояви можуть набувати різних форм – від хабарництва та зловживання владою до привласнення бюджетних коштів і відмивання незаконних доходів.

Відповідно до Єдиного державного реєстру осіб, які вчинили корупційні або пов’язані з корупцією правопорушення, станом на жовтень 2025 року наявно 36 725 записів про фізичних та юридичних осіб, які вчинили такі діяння, з них 18 679 – кримінальні правопорушення, 15 156 – адміністративні, решта – дисциплінарні та без зазначення категорії справи.

Ефективна протидія корупційним злочинам є ключовим завданням державної політики України. Проведені фінансові розслідування дозволяють виявити невідповідності між доходами та витратами посадових осіб; сприяти блокуванню виведення за кордон активів, які можуть бути пов’язані з відмиванням коштів; простежувати фінансові зв’язки у корупційних схемах; виявляти схеми, спрямовані на ухилення від сплати податків тощо.

Спільна робота правоохоронних органів та Держфінмоніторингу дозволяє виявити невідповідності між доходами та витратами посадових осіб, простежувати фінансові зв’язки у корупційних схемах, сприяти блокуванню виведенню активів за кордон тощо.

Один із найбільш небезпечних проявів корупції є розкрадання бюджетних коштів.

Розкрадання бюджетних коштів. Сучасні умови вимагають прозорості використання бюджетних коштів, оскільки це є ключовим чинником довіри громадськості до державних інституцій та основою для сталого розвитку держави. Проблема розкрадання та нецільового використання бюджетних коштів є досі актуальною для України, а під час повномасштабної війни набула особливого значення. Такі дії не лише зменшують ефективність бюджетної політики, а й підривають соціальну справедливість, адже громадяни фактично втрачають ресурси, призначені для суспільного блага.

Розкрадання бюджетних коштів – це не лише кримінальна, а й соціально-економічна проблема, що перешкоджає розвитку держави. Як показують нещодавні гучні корупційні справи, які сколихнули не тільки українське, а й міжнародне суспільство, – ефективний фінансовий моніторинг бюджетних коштів в Україні є фундаментальною вимогою для побудови довіри громадян до влади та залучення міжнародної фінансової допомоги.

За практикою фінансових розслідувань, типовим для схем нецільового використання бюджетних коштів є зловживання під час державних закупівель; збільшення вартості продукції з використанням посередників; невиконання державних контрактів або поставка товару не в повному обсязі та невідповідної якості; фіктивні договори; залучення підконтрольних компаній-нерезидентів; виведення коштів через фіктивні компанії або компанії-оболонки тощо.

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

Приклад 2025.4.3.1. Підозрілі операції за участю політично значущої особи (PEP)[26]

Клієнт Банку (PEP), обслуговується як фізична особа та зареєстрований як фізична особа-підприємець (ФОП) з основним видом діяльності за КВЕД 69.10 «Діяльність у сфері права».

На рахунок ФОП було перераховано значну суму коштів як «чистий дохід». Згідно з наданими документами, ці кошти попередньо надійшли від адвокатського об’єднання в оплату юридичних послуг.

Встановлено, що адвокатським об’єднанням укладено договір з державною установою на надання юридичних послуг за ціною, що суттєво перевищує ринкову.

Під час аналізу виявлено, що **Клієнт Банку** (PEP) та його дружина раніше володіли частками у статутному капіталі цього адвокатського об’єднання.

Згідно з угодою купівлі-продажу частки, вартість відчуження становила символічну суму. Водночас у річній фінансовій звітності об’єднання обліковувалася значна дебіторська заборгованість, що свідчить про наявність активів і потенційної вартості, яка мала би впливати на ринкову ціну частки.

[26] За даними НБУ

Приклад 2025.4.3.2. Підозрілі фінансові операції політично значущої особи з ознаками корупційного зловживання[27]

Клієнт обіймає посаду **Керівника департаменту** у структурі державної служби, що відносить його до категорії політично значущих осіб.

Відразу після відкриття рахунку Клієнта на нього надійшли значні кошти як оплата за нібито надані консультаційні послуги у сфері розвитку муніципальних систем управління надзвичайними ситуаціями та ризиків стихійних лих в Україні.

Джерелом надходження є зовнішньоекономічний контракт, що є нетиповим для новоствореного ФОПа.

Надалі отримані кошти були перераховані на рахунок ФОП дружини Клієнта, після чого використані для:

- придбання високовартісних елітних товарів,
- часткового зняття готівки.

Під час вивчення діяльності Клієнта виникли обґрунтовані підозри, що фактичне надання заявлених послуг може бути відсутнім або штучно створеним.

Клієнт відмовляється надавати достатню інформацію для проведення належної перевірки або надає дані, що є неповними, суперечливими чи складними для підтвердження.

Приклад 2025.4.3.3. Привласнення бюджетних коштів за участю компаній-нерезидентів

Держфінмоніторингом, з урахуванням інформації, отриманої від суб'єктів первинного фінансового моніторингу та ПФР іноземної держави, виявлено схему привласнення бюджетних коштів за участю компаній-нерезидентів з метою їх подальшої легалізації.

Встановлено, що **Державне підприємство** отримало бюджетні кошти для потреб оборонного комплексу країни, які в повному обсязі було перераховано на користь пов'язаного посередника - **Компанії-нерезидента А**- за постачання товарів військового призначення. **Компанія-нерезидент А**, у свою чергу, спрямовувала отримані кошти не лише на користь справжніх виробників військової продукції, а й на користь пов'язаної групи фізичних та юридичних осіб, які підозрюються у відмиванні коштів, а також на інші власні рахунки. При цьому поставка товару на користь **Державного підприємства** була здійснена не в повному обсязі.

[27] За даними НБУ

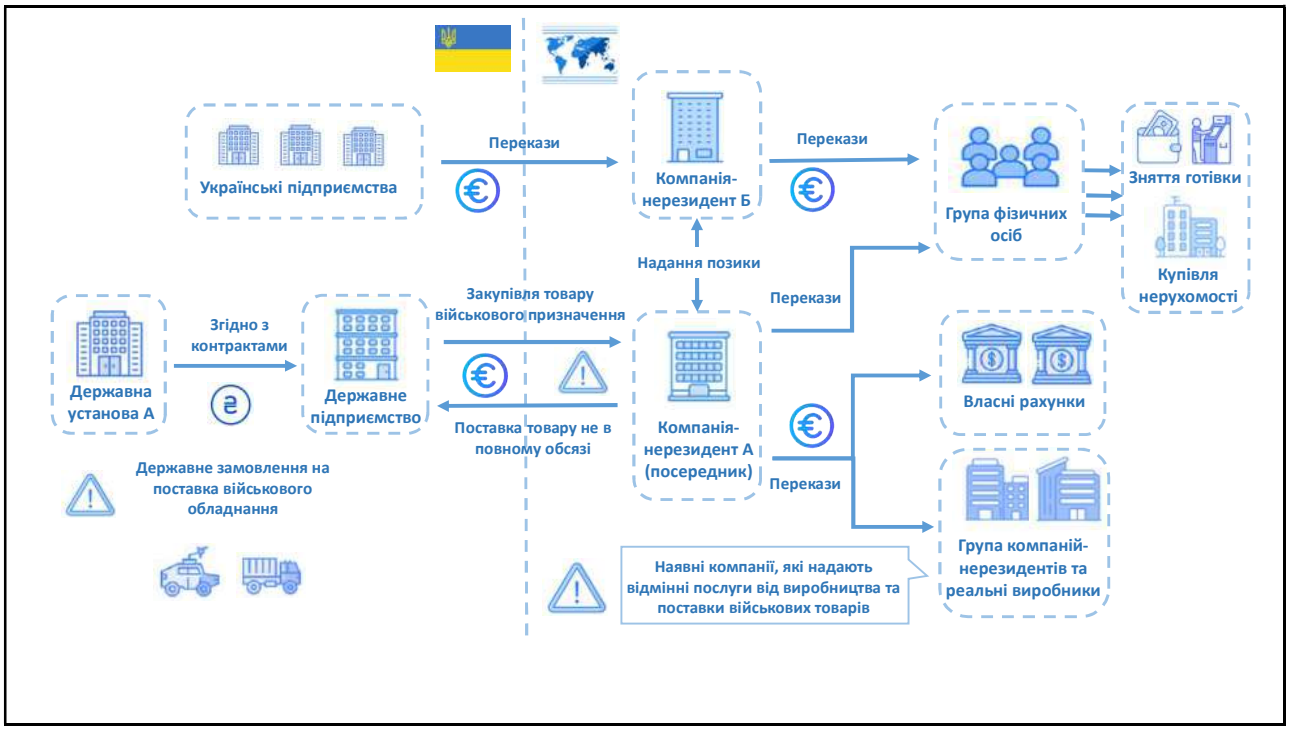
Також встановлено, що отримані від **Державного підприємства** кошти неодноразово переказувалися між рахунками **Компанії-нерезидента А** та **Компанії-нерезидента Б** із використанням ризикових інструментів (надання позики, кредиту), що могло бути спрямоване на ускладнення відслідковування грошових потоків і уникнення фінансового моніторингу. Крім того, **Компанія-нерезидент Б** отримувала кошти й від інших українських підприємств.

У подальшому основна частина коштів була перерахована на користь **Групи компаній-нерезидентів, реальних виробників**, **Групи фізичних осіб**, а також на **власні рахунки**. Серед компаній-нерезидентів, які отримували кошти, були й ті, що надають послуги, не пов'язані з виробництвом або постачанням військової продукції, зокрема: продаж автомобілів, будівельних матеріалів, роздрібна торгівля, просування нерухомості тощо.

Встановлено, що значну частину отриманих коштів **Група фізичних осіб** знімала готівкою або переказувала для придбання об'єктів нерухомості.

Враховуючи вищенаведене, є підстави вважати, що зазначені компанії та фізичні особи є учасниками схеми привласнення державних коштів з подальшою легалізацією (відмиванням) доходів, одержаних злочинним шляхом, за межами України, у тому числі через інвестування в нерухомість.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2025.4.3.4. Привласнення бюджетних коштів з використанням підроблених документів

Держфінмоніторингом, з урахуванням інформації правоохоронного органу, виявлено схему, спрямовану на привласнення бюджетних коштів, за участю пов'язаних юридичних і фізичних осіб, серед яких - колишній народний депутат України.

Встановлено, що **Підприємство А** отримало кошти, зокрема бюджетні, від **Державного підприємства** та **Компанії А** як оплату за комплекти порохових зарядів. У подальшому **Підприємство А** здійснило переказ коштів на користь **Групи юридичних осіб**, **Групи ФОПів**, **Компанії В**, а також на користь **Фізичної особи** – у вигляді оплати частки у статутному капіталі **Компанії В** з метою подальшого використання сировини, що належить цій компанії.

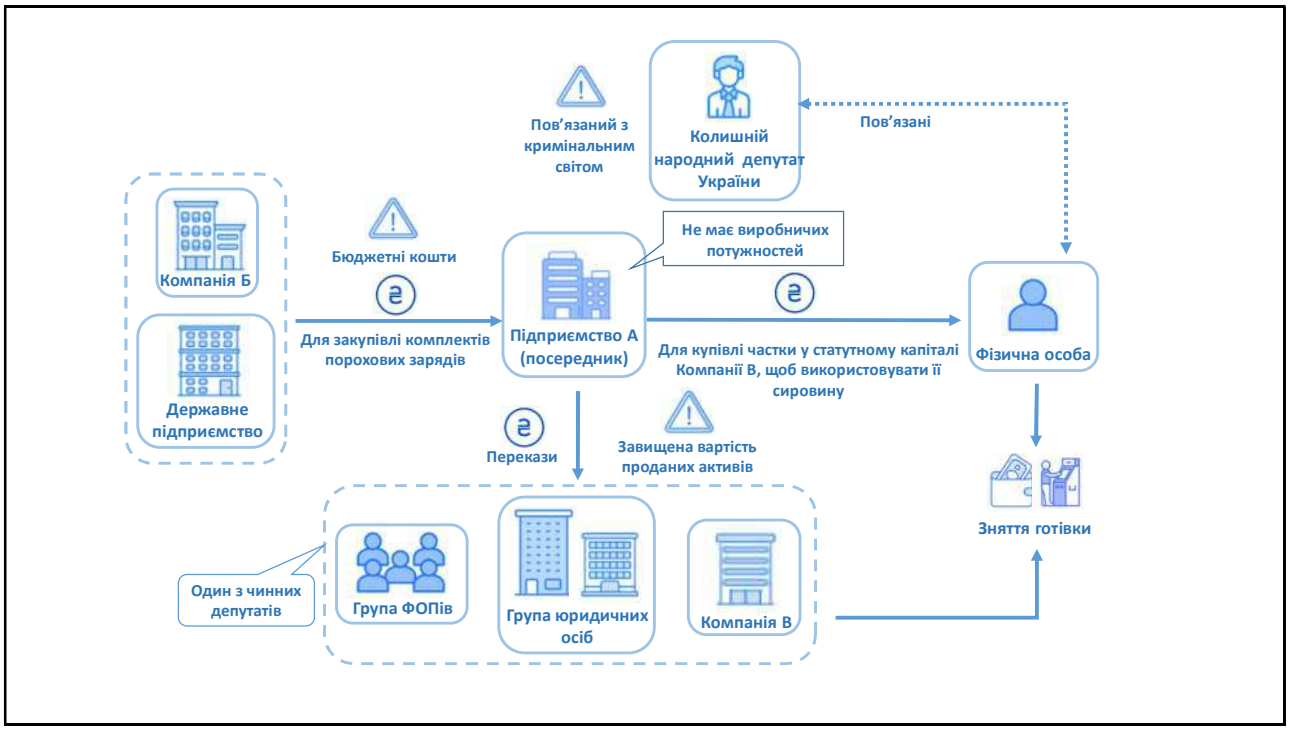
Водночас встановлено, що на балансі **Компанії В** не обліковувалися порохові заряди на відповідну оплачену суму. Це може свідчити про штучне завищення вартості переданих активів, а також про те, що документи, які підтверджують наявність порохових зарядів, мають ознаки удаваності.

У подальшому кошти з рахунків **Фізичної особи**, **Групи юридичних осіб**, **Групи ФОПів** та **Компанії В** у підсумку знімалися готівкою.

Виявлено, що група осіб, задіяних у зазначеній схемі, може бути афілійована з колишнім народним депутатом України, зокрема через **Фізичну особу**, з якою його ймовірно пов'язують родинні зв'язки. Крім того, один із ФОПів, залучених до схеми, є чинним депутатом місцевої ради.

Враховуючи вищевикладене, є підстави вважати, що групою осіб, пов'язаних з колишнім депутатом, була налагоджена схема привласнення бюджетних коштів шляхом використання удаваних документів, штучного завищення вартості активів і подальшої легалізації (відмивання) одержаних злочинним шляхом коштів.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2025.4.3.5. Привласнення бюджетних коштів територіальної громади, виділених для забезпечення ВПО

Держфінмоніторингом, з урахуванням інформації правоохоронного органу, виявлено схему фінансових операцій, спрямовану на привласнення бюджетних коштів територіальної громади, виділених для забезпечення тимчасового проживання та обслуговування внутрішньо переміщених осіб (ВПО).

Встановлено, що **Компанія А** отримала від **Державної установи** бюджетні кошти в якості оплати за будівлю відповідно до цільової програми. У подальшому основна частина цих коштів була використана не за цільовим призначенням: їх було внесено на депозитний рахунок з метою отримання неправомірного доходу у вигляді відсотків, а також перераховано на користь контрагентів - **Компанії Б** за цінні папери, **Компанії В** за нерухоме майно, що їй належить, та на користь **Групи юридичних осіб**, які переважно займаються оптово-роздрібною торгівлею і можуть оперувати необлікованою готівкою.

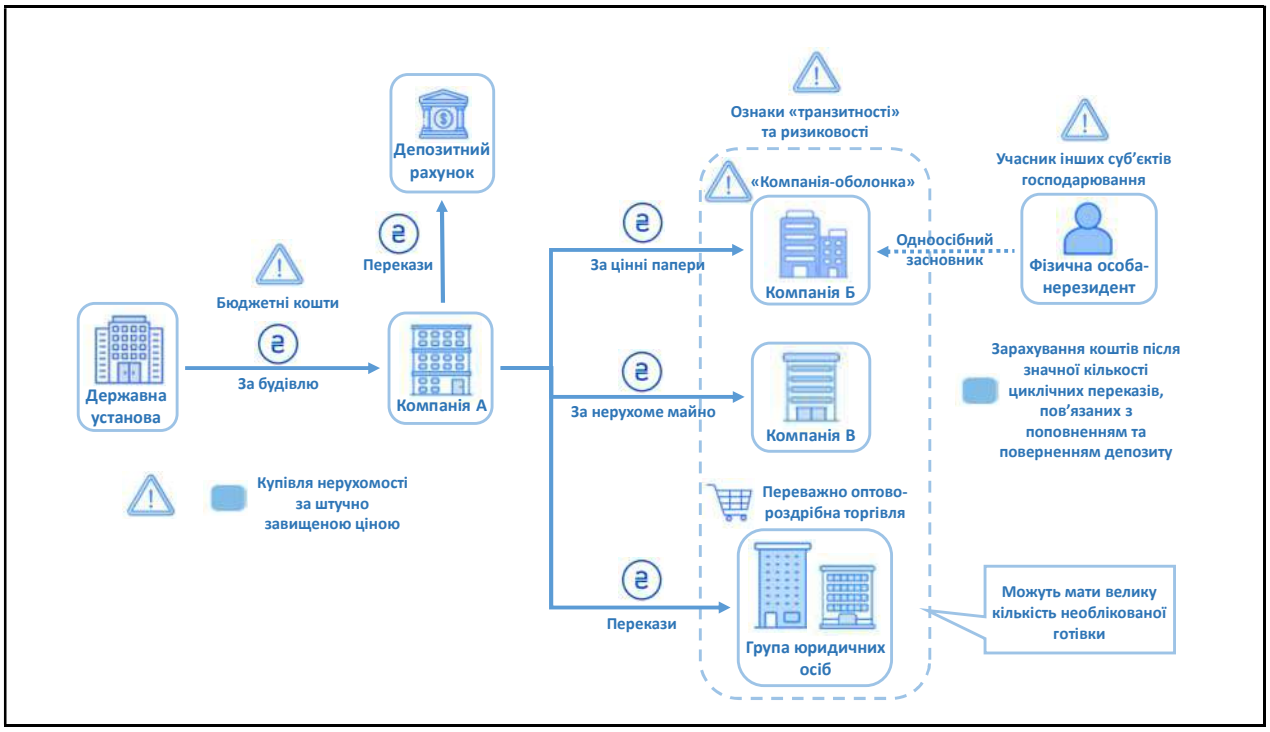
Основна частина бюджетних коштів була акумульована саме на рахунках **Компанії Б** та **Компанії В** після численних циклічних переказів, пов'язаних із поповненням і поверненням депозиту.

Загалом отримувачі бюджетних коштів - **Компанія Б**, **Компанія В** та **Група юридичних осіб** - є суб'єктами господарювання з ознаками фіктивності та ризиковості, а їхні фінансові операції мають характеристики транзитності. Серед отримувачів також є фігуранти кримінальних проваджень і боржники, що ставить під сумнів їхню спроможність виконувати зобов'язання перед державою.

Крім того, єдиним засновником **Компанії Б** є **Фізична особа** - громадянин однієї з країн Центральної Азії, який також є учасником значної кількості інших суб'єктів господарювання.

Згідно з отриманою інформацією, **Державна установа** здійснила купівлю нерухомого майна для потреб ВПО за завищеною вартістю, що може свідчити про існування корупційної схеми за участі посадових осіб цього державного органу.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2025.4.3.6. Нецільове використання бюджетних коштів з подальшою легалізацією

Держфінмоніторингом, з урахуванням інформації, отриманої від суб'єктів первинного фінансового моніторингу та правоохоронного органу, виявлено схему привласнення бюджетних коштів в особливо великих розмірах службовими особами комерційних структур з подальшою їх легалізацією (відмиванням).

Встановлено, що **Державні організації** спільно з **Групою юридичних осіб А** здійснили перерахування бюджетних коштів на користь **Компанії А** як оплату за автозапчастини для військової техніки.

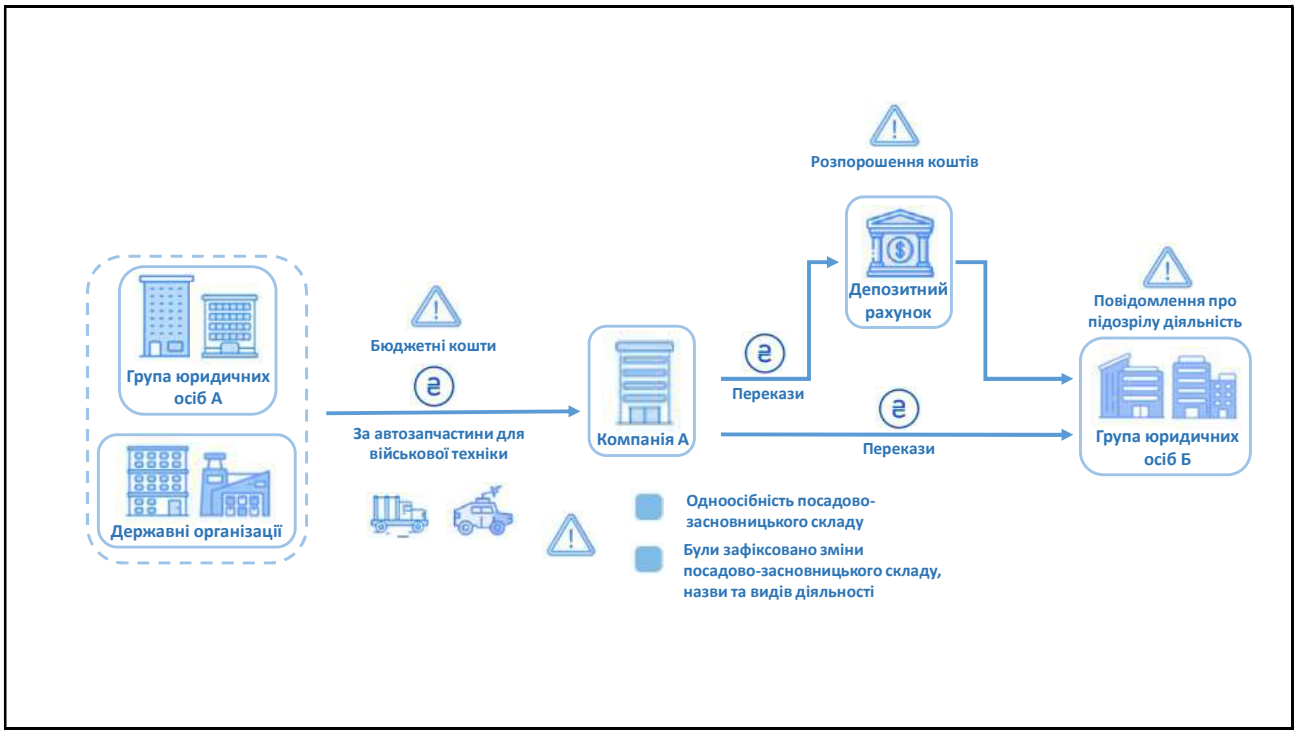
У подальшому отримані кошти, пройшовши транзитом через власний депозитний рахунок або одразу безпосередньо, були перераховані **Компанією А** на рахунки **Групи юридичних осіб Б**. Щодо цих компаній банківськими установами надано повідомлення про підозрілу діяльність і здійснення фінансових операцій, що мають транзитний характер та ознаки схемності.

Значна частина фінансових операцій **Компанії А** має циклічний характер і проводилася із залученням ризикових фінансових інструментів, зокрема шляхом перерахування отриманих коштів на власний депозитний рахунок.

Також встановлено, що **Компанія А** має одноосібний посадово-засновницький склад, який неодноразово змінювався, як і назви компанії та заявлені види діяльності.

Враховуючи вищевикладене, існують обґрунтовані підозри щодо нецільового використання бюджетних коштів **Компанією А** з метою їх подальшої легалізації (відмивання).

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2025.4.3.7. Схема нецільового використання бюджетних коштів групою юридичних осіб

Держфінмоніторингом, з урахуванням інформації правоохоронного органу, виявлено схему, яка, ймовірно, має приховану корупційну складову та пов’язана з підозрами у нецільовому використанні частини бюджетних коштів групою юридичних осіб.

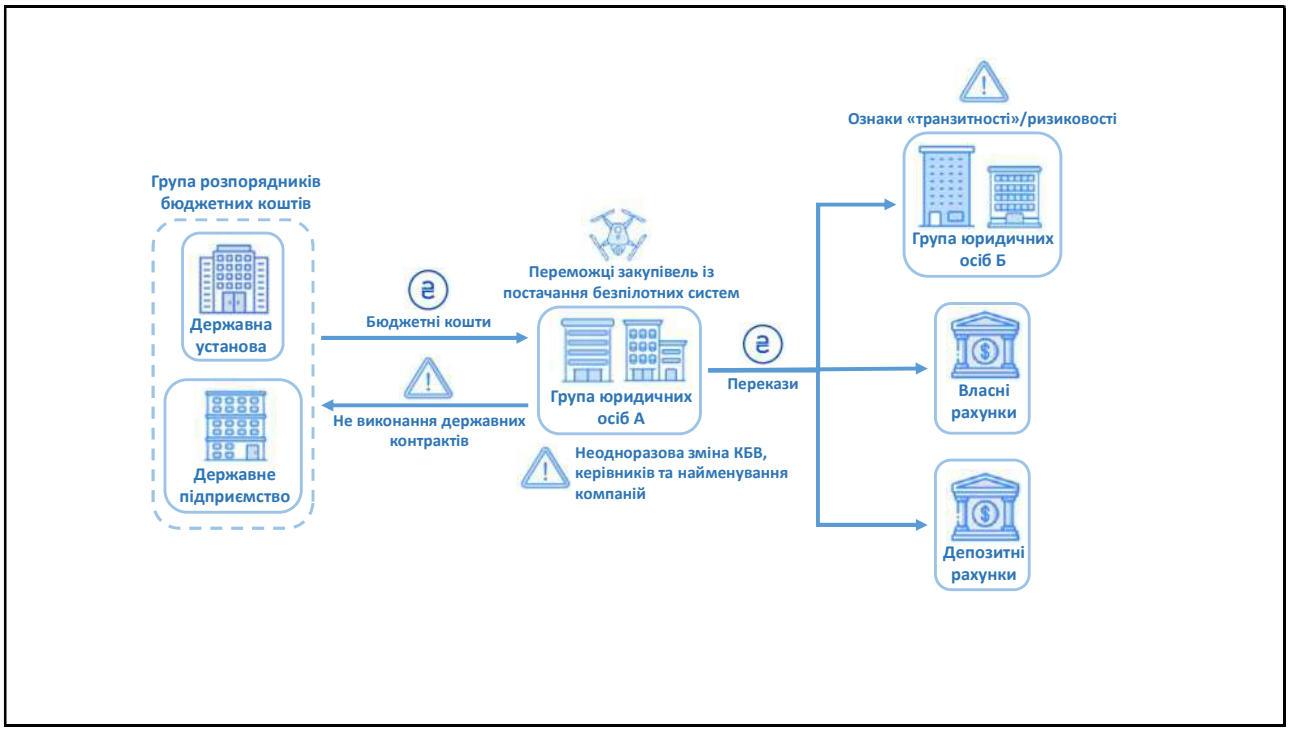
Встановлено, що переможцем закупівель на постачання безпілотних систем виступила **Група юридичних осіб А**, яка після отримання передплати від групи розпорядників бюджетних коштів використовувала ці кошти не за цільовим призначенням. Зокрема, частина коштів перераховувалася на власні рахунки, депозитні рахунки, а також на користь **Групи юридичних осіб Б**, яка має ознаки «транзитності» та ризиковості.

Щодо **Групи юридичних осіб Б** у суб’єктів первинного фінансового моніторингу наявні підозри, що їхня діяльність має ознаки фіктивного підприємництва, а здійснювані фінансові операції - ознаки схемності, відсутності реального економічного змісту, спрямованості на мінімізацію оподаткування, нецільове використання бюджетних коштів або одержання неправомірних економічних переваг третіми особами.

Відомо, що підприємства, що входять до **Групи юридичних осіб А**, отримували прибуток, водночас не виконуючи умови державних контрактів. Зафіксовано неодноразову зміну кінцевих бенефіціарних власників, керівників та найменувань підприємств, що входять до цієї групи.

Враховуючи вищевикладене, є підстави вважати, що фінансові операції, пов'язані із зарахуванням бюджетних коштів на користь **Групи юридичних осіб А**, можуть бути спрямовані на їх привласнення шляхом нецільового використання бюджетних ресурсів.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2025.4.3.8. Нецільове використання та привласнення бюджетних коштів українською компанією за участі компанії-нерезидента

Держфінмоніторингом, з урахуванням інформації, отриманої від правоохоронного органу та ПФР іноземної держави, виявлено схему нецільового використання та привласнення бюджетних коштів, перерахованих для виконання державного замовлення.

Встановлено, що на рахунок української **Компанії А** було зараховано кошти від **Державної установи** як оплату за нове будівництво об'єкта інфраструктури. У подальшому кошти з валютних рахунків **Компанії А** були перераховані на користь **Компанії-нерезидента** для закупівлі продукції згідно з укладеним контрактом.

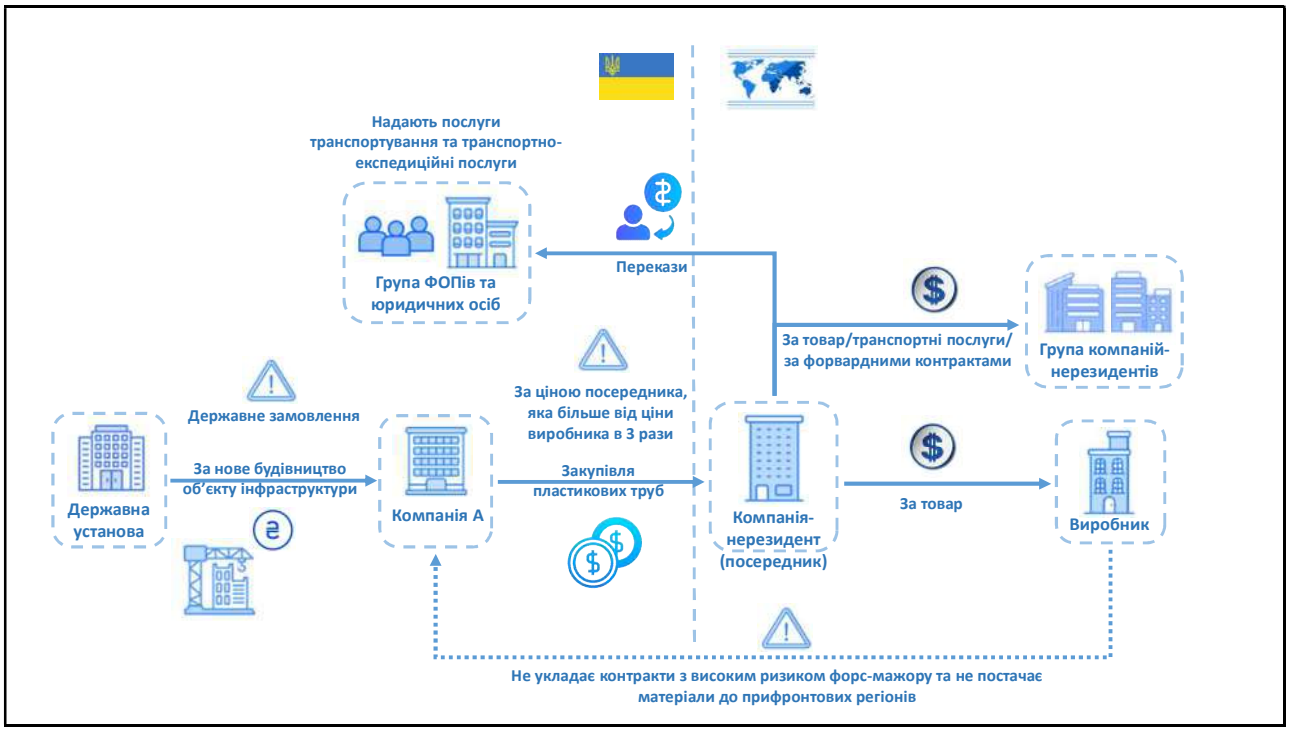
Відомо, що ринкова вартість продукції безпосередньо від **Виробника** втричі нижча за ціну, зазначену в контракті між **Компанією А** та **Компанією-нерезидентом**. Підвищення вартості **Компанія-нерезидент** обґрунтувала тим, що у зв'язку з повномасштабною російською агресією виробник не укладає контракти, що передбачають постачання товарів у регіони з високим ризиком виникнення форс-мажорних обставин, і відмовляється здійснювати постачання до областей, наближених до лінії зіткнення.

У зв'язку з цим **Компанія А** уклала контракт із представником виробника, який погодився взяти на себе всі ризики, пов'язані з постачанням продукції.

Встановлено, що частину коштів, отриманих на виконання контракту, **Компанія-нерезидент** перераховувала як оплату транспортно-експедиційних послуг групі фізичних осіб-підприємців та юридичних осіб, рахунки яких відкриті в українських банківських установах. Крім того, **Компанія-нерезидент** здійснювала перекази коштів на користь **Групи компаній-нерезидентів** як оплату за товари, транспортні послуги та за форвардними контрактами.

Враховуючи вищевикладене, є підстави вважати, що діяльність **Компанії А** та **Компанії-нерезидента** була спрямована на привласнення бюджетних коштів шляхом укладення умисно невигідних контрактів із метою подальшої легалізації незаконно отриманих доходів.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2025.4.3.9. Незаконне привласнення бюджетних коштів за участю пов’язаних юридичних осіб та фізичних осіб-підприємців

Держфінмоніторингом, з урахуванням інформації, отриманої від правоохоронного органу, встановлено факт незаконного привласнення бюджетних коштів за участю групи пов’язаних юридичних осіб та фізичних осіб-підприємців.

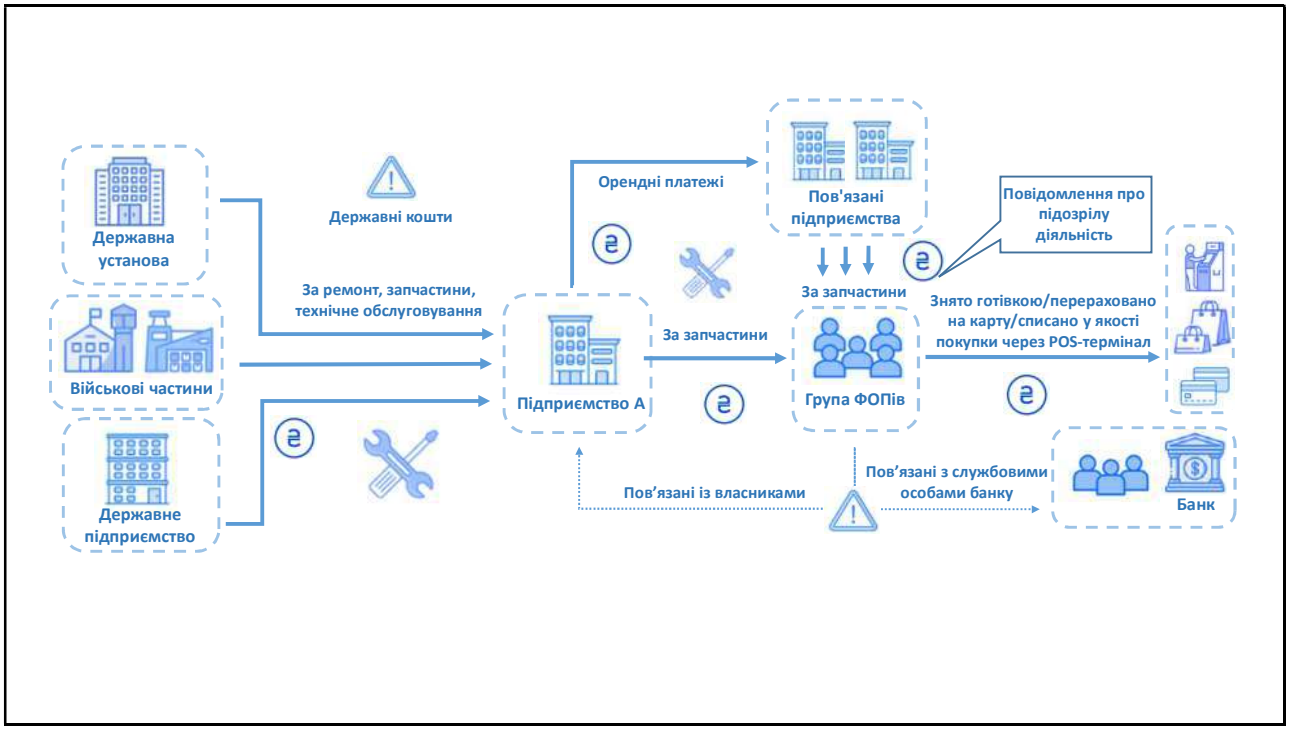
Встановлено, що на рахунки українського **Підприємства**, яке здійснює діяльність у сфері оборони, було зараховано кошти від низки суб’єктів господарювання, зокрема від **Державної установи**, **Державного підприємства** та **військових частин** як оплата за ремонт, постачання запчастин і технічне обслуговування. У подальшому частина цих коштів була перерахована як оплата за запчастини на рахунки **Групи фізичних осіб-підприємців**, пов’язаних із власниками **Підприємства** та зі службовими особами одного з банків.

Іншу частину державних коштів **Підприємство** перерахувало на користь **Пов’язаних підприємств** як орендні платежі, які згодом також були переказані на рахунки **Групи ФОПів** у вигляді оплати за запчастини.

У подальшому отримані кошти з рахунків **Групи ФОПів** знімалися готівкою, переказувалися на особисті карткові рахунки або витрачалися на покупки товарів і послуг через POS-термінали.

Враховуючи вищевикладене, є підстави вважати, що діяльність **Підприємства** була спрямована на привласнення бюджетних коштів із залученням підконтрольних фізичних осіб-підприємців.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2025.4.3.10. Привласнення фізичною особою-підприємцем коштів бюджетної установи, виділених на виконання капітальних ремонтних робіт

Держфінмоніторингом, з урахуванням інформації, отриманої від суб'єктів первинного фінансового моніторингу, виявлено схему, спрямовану на привласнення коштів бюджетної установи, виділених на виконання капітальних ремонтних робіт.

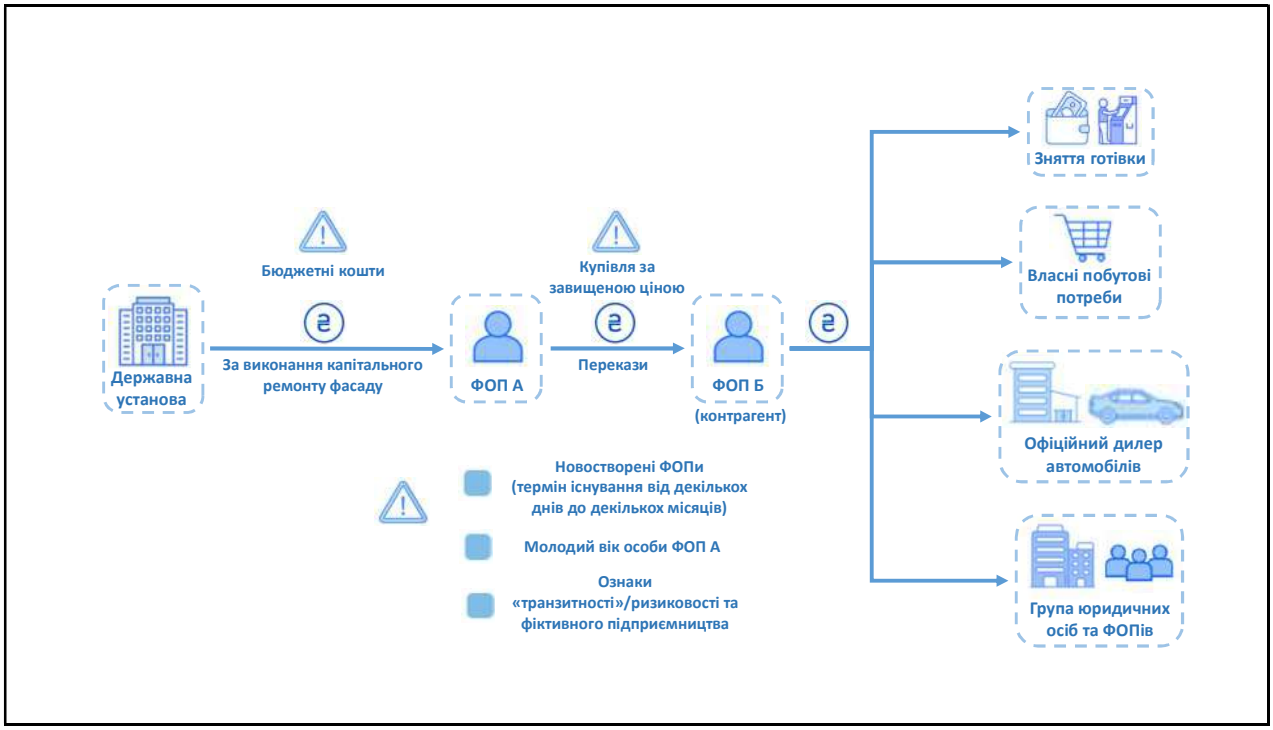
Встановлено, що **Державна установа** перерахувала бюджетні кошти на рахунок **ФОП А** як оплату за проведення капітального ремонту фасаду. Аналіз руху коштів між **ФОП А** та його контрагентом **ФОП Б** свідчить про те, що частина отриманих коштів була обготівкована, спрямована на оплату побутових витрат, придбання автомобіля через офіційного дилера, а також переказана на користь **Групи юридичних осіб** та **ФОПів**, які мають ознаки «транзитності», ризиковості та фіктивності.

Привертає увагу той факт, що на момент укладення договору з **Державною установою**, **ФОП А** існував лише кілька місяців, а **ФОП Б** -лише кілька днів. Крім того, особа, на яку було зареєстровано **ФОП А**, є особою молодого віку.

Відомо, що банківською установою щодо **ФОП А** визначено «високий ризик» та прийнято рішення про відмову у підтриманні ділових відносин.

Враховуючи вищевикладене, є підстави вважати, що отримані бюджетні кошти **ФОП А** були використані не за цільовим призначенням, зокрема шляхом штучного завищення вартості товарів або послуг. Вказані кошти, ймовірно, були отримані за рахунок різниці між завищеною контрактною ціною та фактичною собівартістю.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2025.4.3.11. Розкрадення бюджетних коштів шляхом завищення ціни проданого товару

Держфінмоніторингом, з урахуванням інформації, отриманої від суб'єктів первинного фінансового моніторингу, виявлено схему, спрямовану на розкрадання бюджетних коштів шляхом їх нецільового використання під час закупівлі запчастин для техніки спеціального призначення.

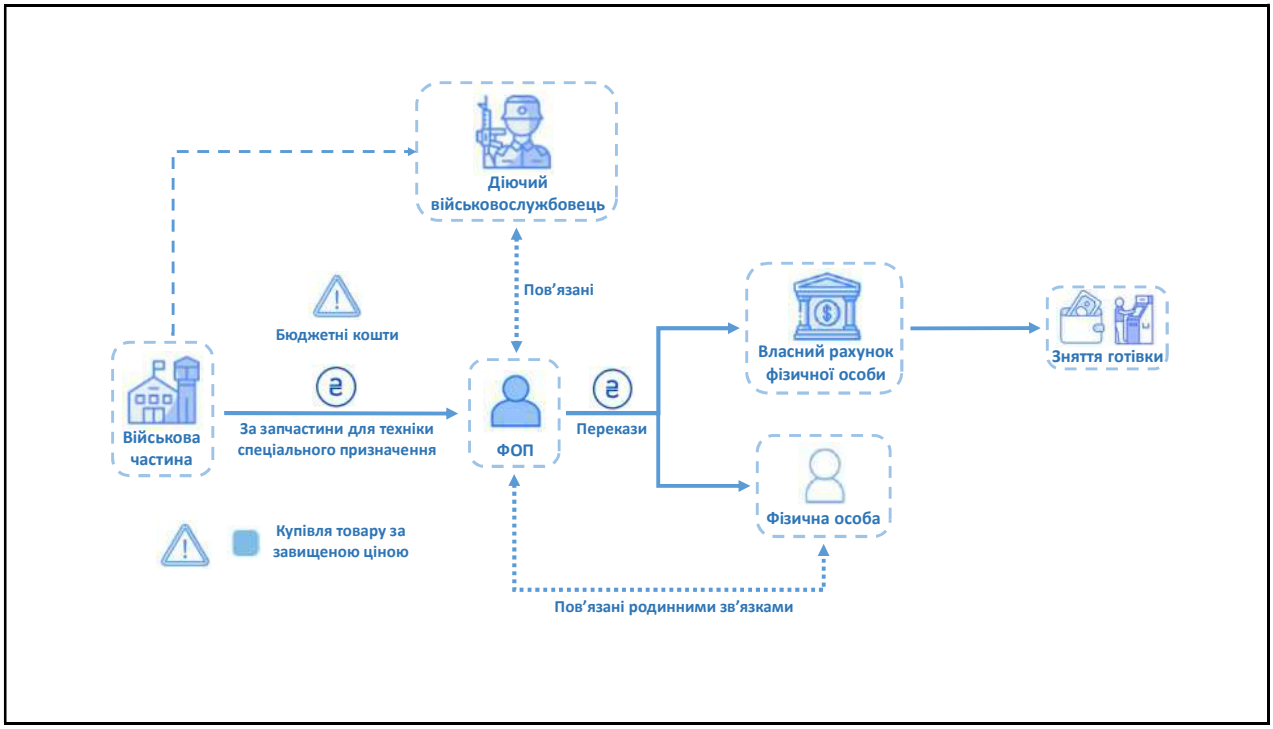
Встановлено, що на рахунок **Фізичної особи-підприємця**, яка, ймовірно, пов'язана з чинним **Військовослужбовцем**, надійшли кошти від **Військової частини** як оплата за запчастини для техніки спеціального призначення. У подальшому значна частина отриманих бюджетних коштів була обготівкована через особистий рахунок цієї **Фізичної особи**, а також перерахована на рахунок іншої фізичної особи, яка, ймовірно, має з ним родинні зв'язки.

Таким чином, бюджетні кошти були використані не за цільовим призначенням, зокрема шляхом завищення вартості товару, що постачався.

Банківською установою щодо зазначеного **ФОПа** визначено високий рівень ризику та прийнято рішення про розірвання ділових відносин.

Враховуючи вищевикладене, існують обґрунтовані підозри щодо ймовірного розкрадання бюджетних коштів **ФОПом** шляхом їх нецільового використання із залученням афілійованих осіб з метою переведення безготівкових коштів у готівку та подальшого використання для оплати товарів і послуг у власних інтересах.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2025.4.3.12. Легалізація (відмивання) незаконних доходів народним депутатом, отриманих внаслідок привласнення коштів фізичних осіб-інвесторів

Держфінмоніторингом виявлено схему легалізації (відмивання) незаконних доходів народним депутатом України, отриманих внаслідок привласнення коштів фізичних осіб-інвесторів.

Встановлено, що **Народний депутат** заснував **Компанію А**, статутний капітал якої був сформований за рахунок його особистого майна - земельної ділянки та житлового будинку.

Згодом, відповідно до договору купівлі-продажу частки у статутному капіталі, **Компанія А** передала **Компанії Б** у власність 100% корпоративних прав. У цей же період на рахунок **Народного депутата** від **Компанії Б** надійшли кошти як оплата за придбані корпоративні права **Компанії А**.
Водночас передача права власності на активи **Компанії А** на користь **Компанії Б** не здійснювалася.

Встановлено, що грошові кошти на рахунок **Компанії Б** надійшли від **Компанії В** у вигляді кредитів та оплати за цінні папери. У свою чергу, кошти на рахунок **Компанії В** були перераховані з рахунків **Компанії Г** як оплата кредитної заборгованості та з іншими цільовими призначеннями, а також частково - від банківської установи як надання кредиту.

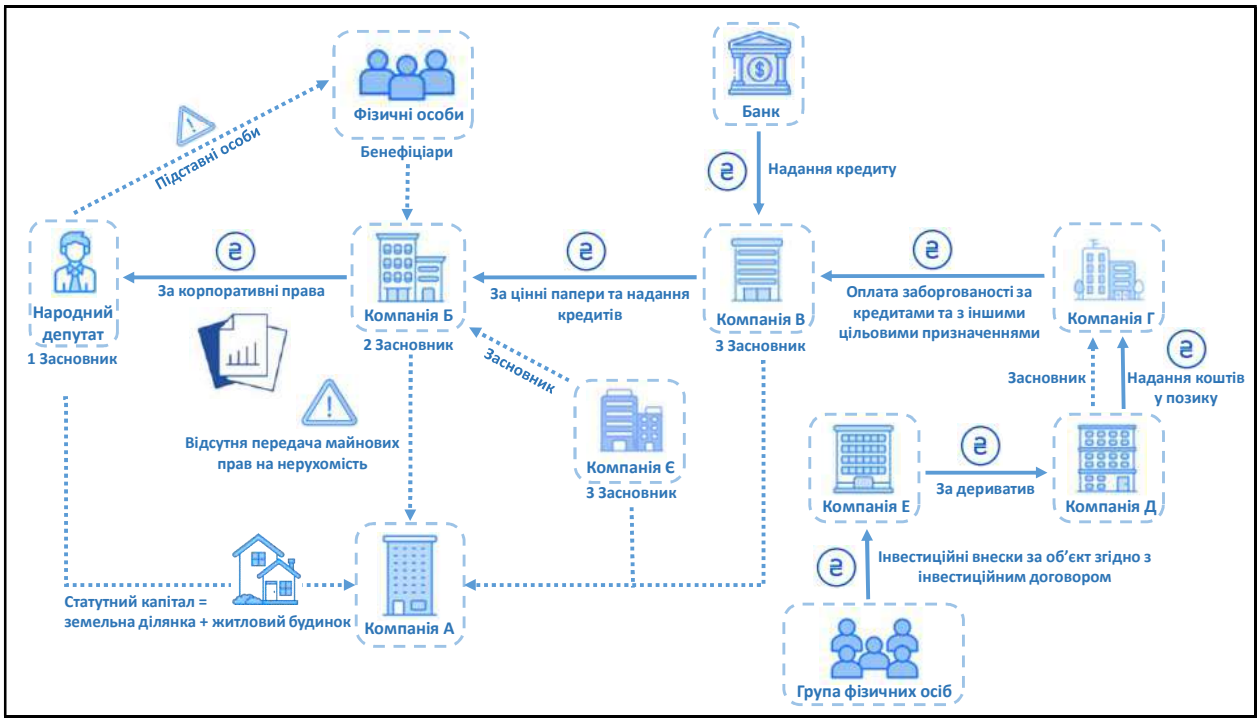
Джерелом коштів на рахунках **Компанії Г** були перекази від **Компанії Д** у вигляді позики. Кошти на рахунок **Компанії Д** надійшли від **Компанії Є** як оплата за деривати.

Водночас **Компанія Є** отримала кошти від **Групи фізичних осіб** як інвестиційні внески згідно з укладеним інвестиційним договором на фінансування об’єктів.

Встановлено, що основні учасники схеми пов’язані між собою через засновників, керівників та бенефіціарних власників, більшість з яких є підставними особами. Крім того, окремі учасники схеми в різні періоди виступали засновниками або співзасновниками **Компанії А**.

Таким чином, є підстави вважати, що зазначена схема була організована з метою легалізації (відмивання) незаконно привласнених інвестиційних коштів фізичних осіб.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2025.4.3.13. Легалізація доходів отриманих у якості неправомірної вигоди використовуючи службове становище

Держфінмоніторингом, з урахуванням інформації, отриманої від правоохоронного органу встановлено, що **посадова особа Військово-медичного закладу, заступник Голови військово-лікарської комісії** з метою особистого незаконного збагачення, отримував незаконні доходи, за які в подальшому придбавав рухоме та нерухоме майно, яке оформляв на **членів сім'ї**, а також акумулював кошти у готівці в іноземній валюті.

Так, з 2022 року **посадова особа Військово-медичного закладу** придбала 2 земельні ділянки та маєток у Київській області, 2 квартири у м. Києві, апартаменти на березі моря у м. Одеса, а також чотири автомобілі преміум-класу останніх моделей.

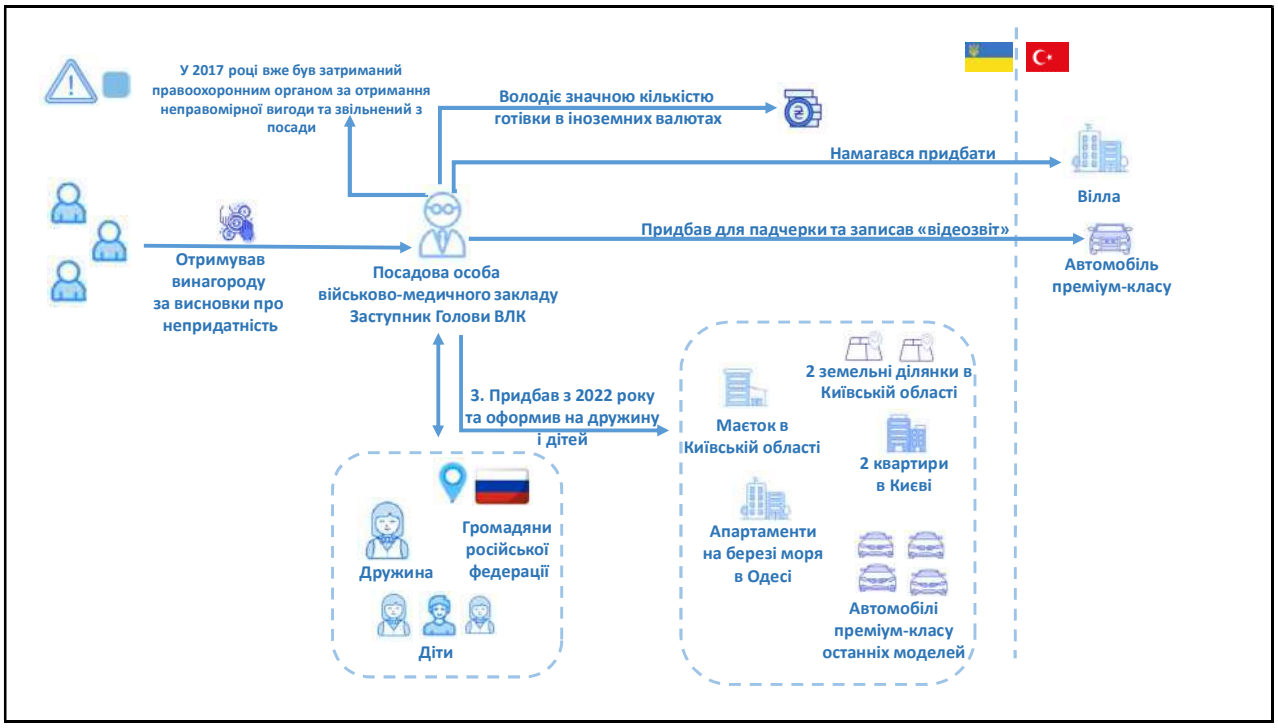
Крім того, відомо що **посадова особа Військово-медичного закладу** володіє значною кількістю готівки в доларах США та євро.

Також відомо, що у 2024 році **посадова особа Військово-медичного закладу** двічі виїжджав до Туреччини, де активно спілкувався з ріелтором щодо придбання елітної вілли, та придбав новий автомобіль преміум-класу для падчерки, про що зняв відповідне відео на телефон.

Привертає увагу, що **члени сім'ї** є громадянами російської федерації.

Крім того, у 2017 році **посадова особа Військово-медичного закладу,** також затримувалась правоохоронним органом за отримання неправомірної вигоди та була звільнена з відповідної посади, яку на той час обіймала.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2025.4.3.14. Схема легалізації (відмивання) доходів одержаних злочинним шляхом

Держфінмоніторингом, з урахуванням інформації правоохоронного органу виявлено схему легалізації коштів отриманих з невстановлених джерел шляхом придбання та набуття у власність високоліквідних активів.

Відомо, що **РЕР (Колишній народний депутат України, депутат міської ради)** організовано схему легалізації доходів через своїх родичів, зокрема через **матір**, **дружину** та **сестру дружини**.

Так, у власності **матері РЕР** перебуває квартира в елітному житловому комплексі м. Києва.

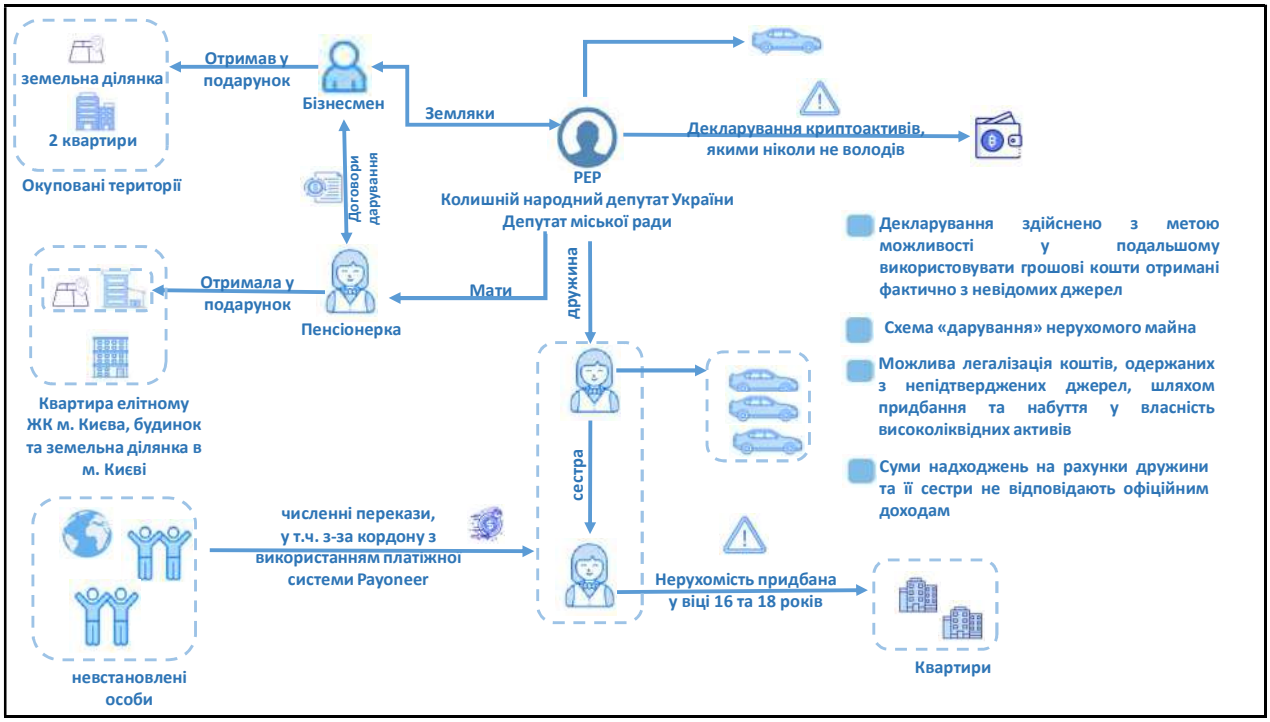
Крім того, **мати РЕР** отримала у подарунок від **фізичної особи - бізнесмена** земельну ділянку та будинок в одному з елітних районів міста Києва та подарувала йому земельну ділянку і дві квартири, що розташовані на окупованій території України та дістались матері у спадок.

Таким чином, фактично за допомогою схеми «дарування» майна, **РЕР** легалізував право власності на елітне нерухоме майно у матері. Слід зазначити, що **Фізична особа** та **РЕР** родом з одного регіону.

Також встановлено, що на рахунки **дружини** та **сестри дружини** надходять численні перекази, що не відповідають розміру їх офіційним доходам. Натомість, відомо, що у власності **дружини** перебуває три автомобіля, а **сестра дружини** придбала дві квартири у м. Ірпінь у віці коли їй було 16 та 18 років, що ставить під сумнів можливість придбання нею нерухомості за власні кошти.

Крім того, встановлено, що **РЕР** задекларовано криптовалюту на значну суму, якою він фактично ніколи не володів, та здійснив їх декларування виключно з метою подальшого використання коштів одержаних з невідомих джерел у протиправних схемах легалізації доходів.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2025.4.3.15. Схема легалізації незаконно отриманих доходів за участю політично значущої особи

Держфінмоніторингом, з урахуванням інформації, отриманої від правоохоронного органу, виявлено схему штучного формування прибутків юридичної особи для створення законності виплати дивідендів **Фізичній особі** та легалізації готівкових коштів, шляхом придбання у «**Політично значущої особи**» корпоративних прав компанії.

Так, **Фізична особа** (колишній заступник голови міської адміністрації) внесла на власний рахунок значні суми готівкових коштів, водночас зняття готівки у співставних обсягах не здійснювалося, що свідчить про можливе незаконне походження таких коштів. Крім того, зазначена **Фізична особа** отримала дивіденди від **ТОВ А**.

Отримані кошти стали джерелом подальших фінансових операцій, у межах яких **Фізична особа** перераховувала їх на користь «**Політично значущої особи**» як оплату за корпоративні права **Компанії К**, зареєстрованої на території однієї з країн Європейського Союзу.

Водночас аналіз операцій **ТОВ А** свідчить, що зазначені фінансові операції є складовими різних, але взаємопов'язаних напрямків коштів, реалізованих у межах єдиної злочинної схеми.

Джерело 1. Перший ланцюг коштів пов'язаний з діяльністю **ТОВ А**, джерелом походження коштів якого є забезпечувальні авансові платежі

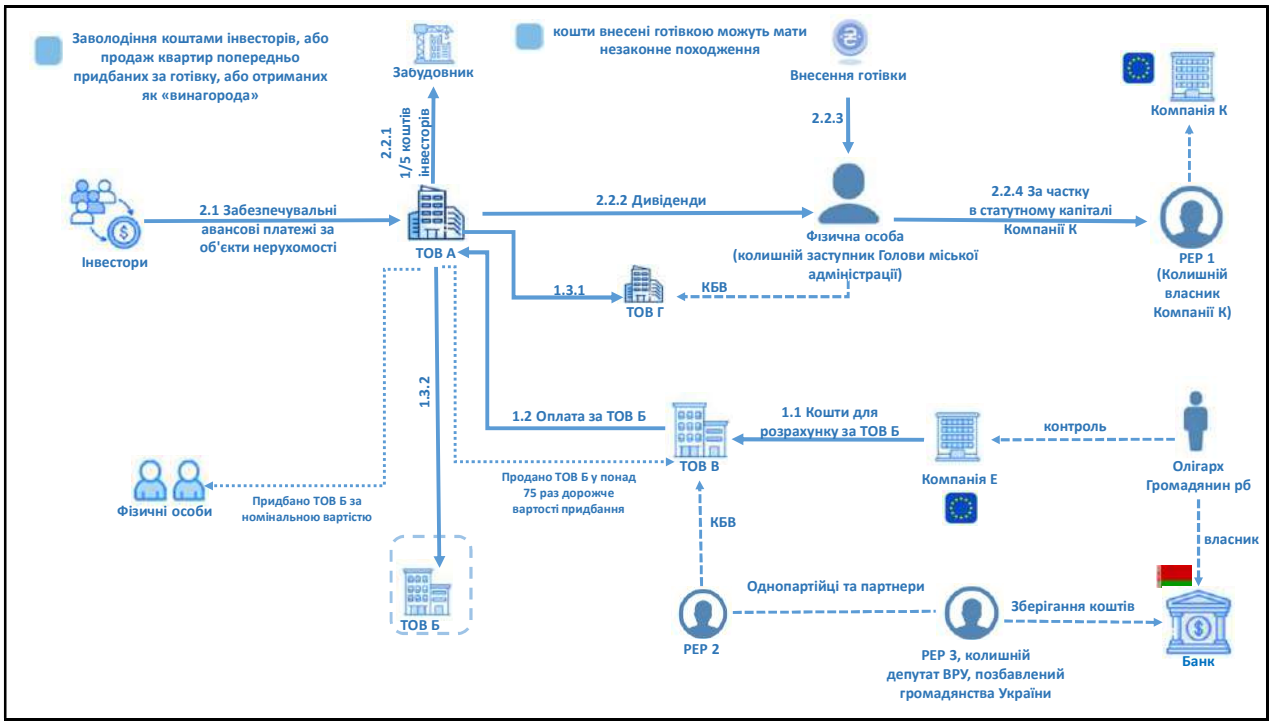
Інвесторів за об’єкти нерухомості, з яких лише 1/5 частина була перерахована забудовнику, що може свідчити про заволодіння коштами інвесторів, продаж квартир, попередньо придбаних за готівку, або отриманих як неправомірна «винагорода».

Джерело 2. Другий ланцюг коштів пов’язаний зі штучним формуванням прибутку **ТОВ А**, який став підставою для виплати дивідендів на користь фізичної особи, зокрема шляхом придбання **ТОВ А** у **двох фізичних осіб** корпоративних прав **ТОВ Б** за номінальною вартістю та їх подальшого продажу на користь **ТОВ В** за ціною, що перевищує вартість придбання більш ніж у 75 разів.

Списання коштів. Отримані кошти **ТОВ А** перерахувало на користь безпосередньо **ТОВ Б** (об’єкт перепродажу корпоративних прав), а також **ТОВ Г** (КБВ якої є Фізична особа – отримувач дивідендів).

Окремо встановлено, що кінцевий бенефіціарний власник **ТОВ В** (покупець корпоративних прав ТОВ Б у межах штучного формування прибутку ТОВ А) є **«Політично значуща особа 2»** – однопартієць та діловий партнер **«Політично значущої особи 3»**, який був позбавлений громадянства України. При цьому джерелом походження коштів для придбання зазначених корпоративних прав були кошти **Компанії Е**, контроль за діяльністю якої здійснює олігарх з республіки білорусь – власник банківської установи, в якій зберігалися кошти **«Політично значущої особи 3»**.

Правоохоронним органом здійснюється досудове розслідування.



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

Неприбуткові організації (НПО), через специфіку своєї діяльності та масштаб гуманітарної підтримки під час війни, залишаються вразливими до зловживань, зокрема до фінансування тероризму або відмивання коштів.

Роль НПО в умовах кризи та регуляторні підходи. У 2025 році в умовах повномасштабної агресії та масових гуманітарних викликів, НПО – як українські, так і міжнародні – залишаються ключовими у наданні допомоги постраждалим, відбудові інфраструктури, документуванні злочинів та підтримці громадянського суспільства.

З одного боку, країни повинні впроваджувати стандарти FATF, оцінювати ризики НПО та застосовувати пропорційні заходи контролю, забезпечуючи прозорість і підзвітність неприбуткових організацій, але водночас важливо не перешкоджати їхній законній гуманітарній діяльності.

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

Приклад 1. Після закінченню Другої світової війни виникла величезна гуманітарна криза. Міжнародна спільнота почала активно організовувати гуманітарну підтримку, але й тут мали місце корупція, зловживання та нерівномірний розподіл ресурсів[28].

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

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

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

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

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

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

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

Корупція у гуманітарній допомозі в умовах конфліктів[29]

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

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

Корупція в гуманітарній сфері – це виклик, притаманний усім конфліктам (війнам), але ефективність протидії залежить від політики та спроможності конкретної країни.

В Україні боротьба з корупцією посилюється завдяки активному громадянському суспільству, яке забезпечує контроль, прозорість розподілу допомоги та взаємодію з донорами.

Оцінка загроз

Ризики зловживання ресурсами. Існують значні загрози зловживання ресурсами, особливо в умовах, коли залучаються великі обсяги коштів, збільшується швидкість ухвалення рішень, а діяльність охоплює широкий спектр напрямів. У таких умовах зростає ймовірність того, що частина

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

ресурсів може бути направлена на незаконні цілі – через непрозору діяльність, відсутність ефективного звітування або слабкий контроль.

Вразливість неприбуткових організацій. Неприбуткові організації користуються високою довірою, мають доступ до складно контрольованих джерел фінансування та можуть працювати з готівкою, що разом із гнучкістю їхньої діяльності робить їх привабливими для терористичних структур і вразливими до зловживань.

Форми зловживань

Зловживання неприбутковими організаціями. Неприбуткові організації можуть бути використані для фінансування тероризму, відмивання злочинних коштів, обходу санкцій, а також для поширення сепаратистських ідей та інформаційного впливу – зокрема через пропаганду наративів «руського миру».

НПО як прикриття для незаконної діяльності. Неприбуткові організації можуть слугувати прикриттям для вчинення фінансових злочинів, зокрема відмивання коштів і фінансування тероризму.

Відмивання коштів. Злочинці використовують неприбуткові організації для ВК, щоб надати незаконним грошам вигляд законних пожертвувань. Часто створюються фіктивні благодійні організації, які не здійснюють реальної діяльності. Кошти перераховуються на їхні рахунки, а потім виводяться під виглядом фінансування легальних проєктів, але насправді йдуть у кишені зловмисників.

Фінансування тероризму. Загальна тенденція використання неприбуткові організації для ФТ полягає у маскуванні фінансових потоків для терористичних груп. Це може здійснюватися через: «чорні» фінансові канали: кошти збираються через неприбуткові організації, а потім перенаправляються за кордон для фінансування терористичних актів.

Передача коштів під виглядом допомоги: кошти, зібрані під виглядом гуманітарної допомоги, насправді використовуються для закупівлі зброї чи матеріалів подвійного призначення.

Інші злочини. Неприбуткові організації також використовуються для ухилення від податків та інших форм шахрайства. Наприклад, деякі організації заявляють про благодійні внески, які насправді є фіктивними, щоб зменшити податкові зобов’язання.

Найбільш вразливими до зловживань є благодійні та релігійні організації, а також гуманітарні фонди (особливо новостворені та організації з іноземним фінансуванням), оскільки вони часто працюють у країнах з високим рівнем корупції та мають спрощені вимоги до звітності. Їхня діяльність часто передбачає пожертви готівкою та перекази коштів за кордон, що робить їх ідеальним інструментом для злочинців.

Ризики псевдоволонтерства та неконтрольованих зборів. Псевдоволонтери, зловживаючи довірою суспільства й патріотичними настроями, організовують непрозорі збори коштів через p2p-перекази на особисті рахунки без звітності щодо їхнього цільового використання, що створює додаткові фінансові ризики.

Інструменти протидії

Заходи обачливості для мінімізації ризиків. Для зниження ризиків зловживань у неприбутковому секторі важливо впроваджувати заходи обачливості: перевірку документів, бенефіціарів, цілей діяльності та джерел фінансування.

Узагальнені типові приклади використання НПО в незаконній діяльності наведено нижче.

За даними Державної податкової служби, за період 2022 - 2025 років були виявлені факти використання неприбуткових організацій для розкрадання коштів, наданих іноземними донорами, та їх легалізації.

Приклад 2025.4.4.1. Зловживання у проєктах будівництва для ВПО

Посадові особи неприбуткової організації, шляхом завищення кошторисної вартості та обсягів будівельних робіт під час реалізації проєкту з будівництва житла для внутрішньо переміщених осіб (ВПО) коштом іноземних благодійників, здійснили розкрадання частини отриманого фінансування та подальшу легалізацію цих коштів із використанням підконтрольних фізичних осіб-підприємців (ФОП) та пов’язаних суб’єктів господарської діяльності.

Приклад 2025.4.4.2. Легалізація коштів під прикриттям релігійної організації через «безтоварні операції»

У період 2022 - 2024 років **Релігійна організація** отримувала фінансування від **Благодійного фонду**, кінцевими бенефіціарними власниками якого є іноземні громадяни. При цьому останню звітність про використання доходів (прибутків) **Релігійна організація** подавала за 2021 рік.

Аналіз подальшого використання отриманих коштів засвідчив їх перерахування на рахунки **Фізичних осіб-підприємців** із призначенням платежу «оплата за дрова». Надалі **ФОПи** здійснювали перекази цих коштів на власні рахунки або на рахунки осіб з ознаками фіктивності (так званих «дропів») із призначенням «переказ власних коштів».

Приклад 2025.4.4.3. Викрито настоятеля УПЦ (МП), який на замовлення воєнної розвідки рф коригував удари військ держави-агресора[30]

Контррозвідка Служби безпеки України затримала **Настоятеля** одного з храмів єпархії **УПЦ** (МП), який виявився коригувальником вогню російської воєнної розвідки (гру). **Настоятель** відстежував місця розташування бойових підрозділів та фортифікаційних споруд Сил оборони України й передавав ці дані до російської федерації.

За матеріалами слідства, представники ворожої **спецслужби** вийшли на **Настоятеля** дистанційно через інтернет. Після виявлення потенційних цілей російський інформатор передавав координати куратору за допомогою голосових і текстових повідомлень у месенджері.

Під час обшуку у **Настоятеля** було вилучено смартфон із доказами його співпраці з ворогом.

Слідчі Служби безпеки України повідомили клірику про підозру за ч. 2 ст. 114-2 КК України – поширення інформації про переміщення, рух або розташування Збройних Сил України чи інших військових формувань, створених відповідно до законів України.

Приклад 2025.4.4.4. Нецільове використання коштів громадською організацією, отриманих для благодійної діяльності[31]

Громадська організація отримує добровільні пожертви з метою надання гуманітарної допомоги військовим та цивільним, які постраждали внаслідок бойових дій в Україні.

Встановлено, що значна частина отриманих благодійних коштів була спрямована на погашення кредитної заборгованості одного із засновників організації.

На запит СПФМ щодо суті та правомірності проведеної операції клієнт надав пояснення, що у зв’язку з погашенням кредиту **Громадській організації** буде нібито надано право користування нерухомістю (готель, розташований у Закарпатській області).

Аналіз свідчить, що зазначена операція:

- не відповідає заявленим благодійним цілям, заради яких організація збирала пожертви;
- має ознаки нецільового та неправомірного використання благодійних коштів;
- може свідчити про використання благодійної організації в особистих інтересах засновника.

Отже, встановлено факт нецільового використання коштів, отриманих **Громадською організацією** для здійснення благодійної діяльності.

[30] https://ssu.gov.ua/novyny/sbu-zatrymala-protoiiereia-upts-mp-yakyi-na-zamovlennia-voiennoi-rozvidky-rf-koryhuvav-udary-rashystiv-po-sumshchyni

[31] За даними НБУ

Приклад 2025.4.4.5. Шахрайська схема заволодіння коштами громадян, перерахованих в якості благодійних пожертв

Держфінмоніторингом виявлено схему шахрайського заволодіння **Благодійним фондом** коштами **фізичної особи**.

Встановлено, що **Фізична особа** у пошуках постачальників автотранспорту для ЗСУ в соціальній мережі «Instagram» знайшла оголошення про продаж необхідного автомобіля **Благодійним фондом**.

В телефонному режимі було узгоджено вартість автомобіля, спосіб доставки та отримано реквізити на оплату товару.

Фізична особа внесла кошти за вказаними реквізитами у якості оплати за надання транспортного засобу.

Наступного дня представник **Благодійного фонду** додатково зателефонував, та повідомив про необхідність сплатити транспорті витрати, з метою доставки транспортного засобу в зону бойових дій.

Фізична особа додатково внесла відповідну суму у якості благодійної допомоги на потреби військових.

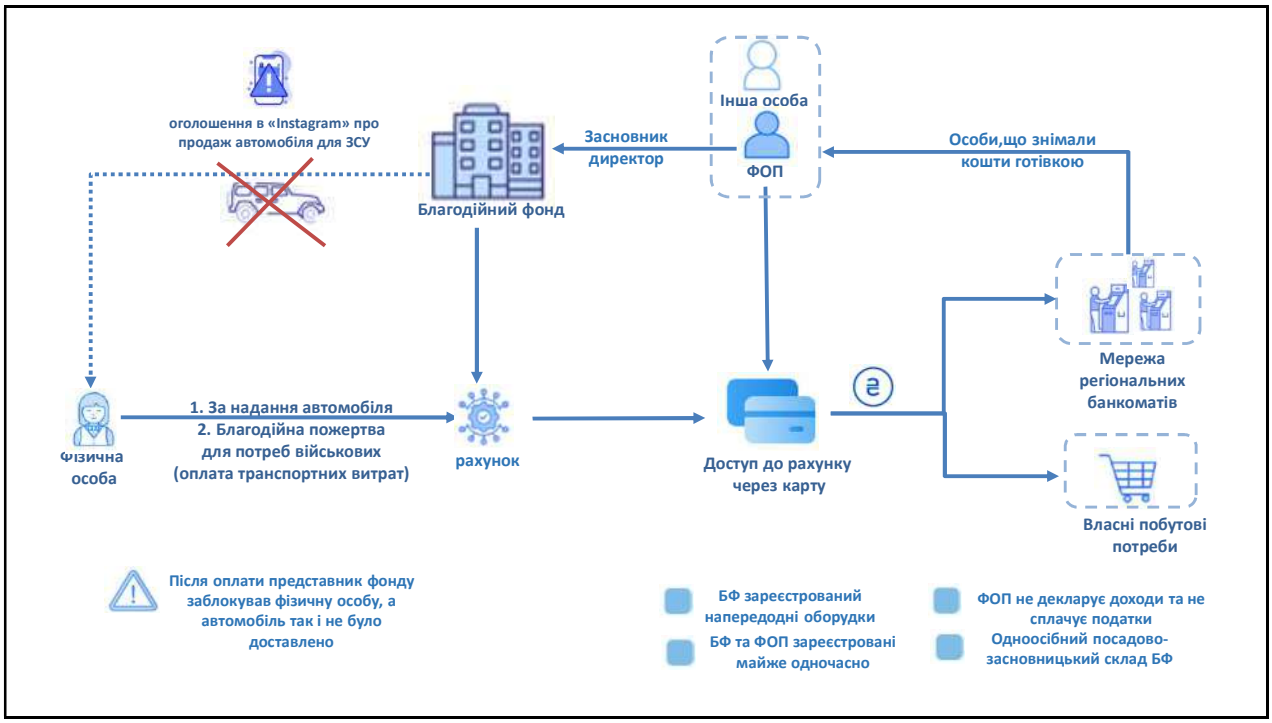
Надалі представник **Благодійного фонду** заблокував контакти **Фізичної особи**, а придбаний автомобіль для ЗСУ так і не було доставлено.

В подальшому, отримані **Благодійним фондом** кошти, виведені з рахунку за допомогою картки **засновника Благодійного фонду**, яка використовується для щоденних розрахунків підприємства та ФОП, на сплату товарів і послуг та отримання готівки **засновником Благодійного фонду** та **третьою особою**.

Привертає увагу, що **Благодійний фонд** зареєстровано менш ніж за місяць до проведення транзакцій.

Також, **засновник Благодійного фонду**, напередодні зареєструвалася як фізична особа – суб’єкт підприємницької діяльності. Водночас, дохід від такої діяльності не декларувався, податки не сплачувалися.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2025.4.4.6. Шахрайська схема заволодіння коштами, перерахованими в якості благодійних пожертв

Держфінмоніторингом, з урахуванням інформації, отриманої від правоохоронного органу та підрозділу фінансової розвідки іноземної держави виявлено схему привласнення та легалізації коштів, походженням яких були благодійні внески до **Благодійного фонду**.

Відомо, що між **Благодійним фондом (Покупець)** та **Компанією-нерезидентом А (Продавець)** укладено контракт на купівлю автомобілів для

потреб ЗСУ та сплачено передоплату на рахунок **Компанії-нерезидента А**. Згідно умов контракту товар мав бути поставлений на користь **Благодійного фонду**, а у випадку не постачання **Компанія-нерезидент А** мала повернути кошти.

Надалі **Компанією-нерезидентом А** кошти направлено на оплату логістичних послуг на користь **Компанії-нерезидента В**, що є неактивною, а також частково знято готівкою та придбано мобільні телефони марки «Apple».

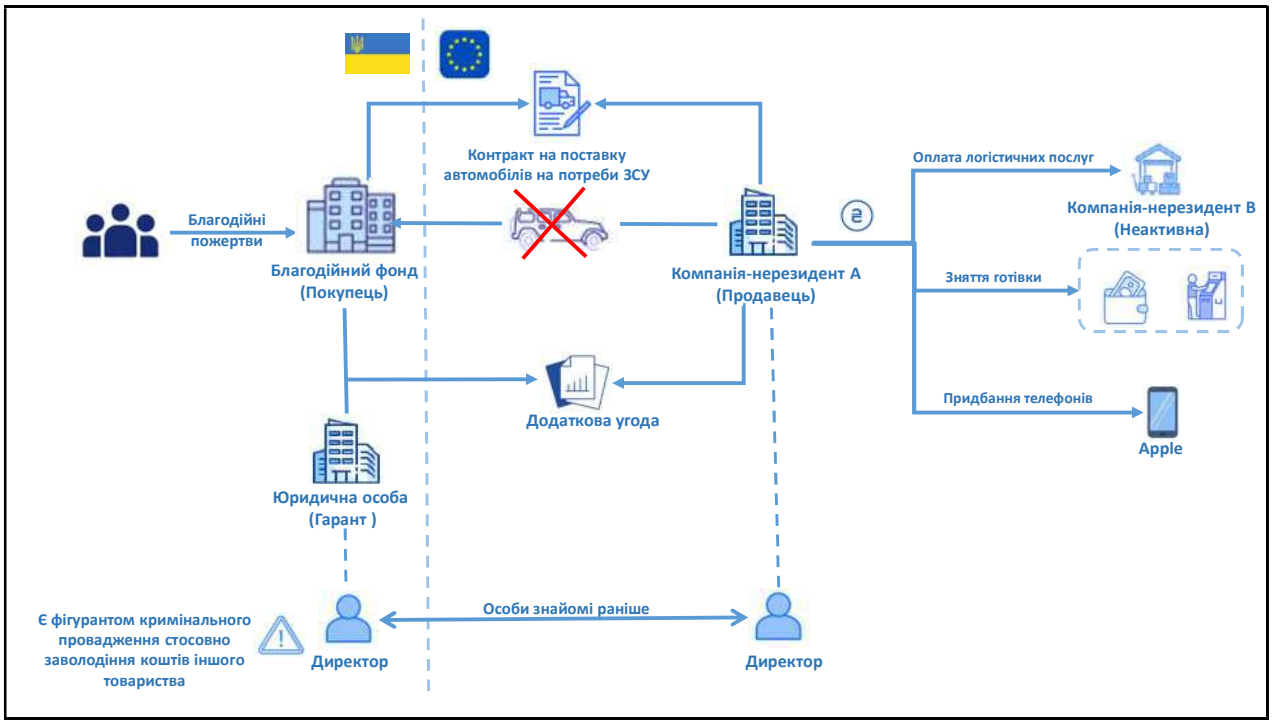
В результаті, **Благодійним фондом** не було отримано, а ні автомобілів, а ні коштів.

Варто зазначити, що відповідно до умов додаткової угоди до вищевказаного контракту, гарантом виступає **Юридична особа** в особі директора, що безпосередньо був знайомим з директором **Компанії-нерезидента А**, та є фігурантом кримінального провадження в рамках іншого розслідування.

Ними спільно було організовано схему привласнення коштів **Благодійного фонду**. Директор **Компанії-Гаранта** є фігурантом кримінального провадження щодо заволодіння коштів іншого товариства.

Таким чином, **директор Юридичної особи** та **директор Компанії-нерезидента А (Продавець)** реалізували шахрайську схему привласнення коштів **Благодійного фонду**, які мали бути спрямовані на закупівлю автомобілів для потреб Збройних Сил України.

Правоохоронним органом здійснюється досудове розслідування.



РОЗДІЛ 4.5. ТРАНСКОРДОННЕ ВІДМИВАННЯ ДОХОДІВ

Сучасна зовнішньоекономічна діяльність України здійснюється в умовах повномасштабної війни, що суттєво впливає на економіку країни та її інтеграцію у світове господарство.

Попри втрату значної частини виробничих потужностей, руйнування інфраструктури та неможливість використання раніше традиційних логістичних маршрутів, держава продовжує формувати та підписувати нові торгівельні угоди з партнерами.

За даними Державної служби статистики України, за 9 місяців 2025 року експорт товарів та послуг становив $35,3 млрд, або 93,5% порівняно із 9 місяцями 2024 року, імпорт – $65,7 млрд, або 114,9%. Торговий дефіцит товарів за 9 місяців 2025 року розширився до $30 млрд (за 9 місяців 2024 року було $24 млрд). Міжнародна допомога – основний канал компенсації дефіциту платіжного балансу (притік $31 млрд за 9 місяців).

Зовнішня торгівля у 2025 році охоплювала співпрацю з партнерами із 221 країни світу. У травні 2025 року Національний банк України ухвалив нову стимулюючу валютну лібералізацію з метою сприяння припливу додаткового капіталу в економіку України.

Зовнішньоекономічний сектор економіки залишається для несумлінних учасників ринку привабливим полем з метою переведення фінансових злочинів за межі національного рівня, переходячи на міжнародний.

Транскордонне відмивання коштів є одним з найпоширеніших та нелегальних явищ, суть якого полягає у переміщенні незаконно отриманих активів за кордон з метою приховання справжнього походження та подальшого їх використання легальним чином.

Одними з механізмів відмивання доходів у зовнішньоекономічній сфері можна вважати: заниження або завищення митної вартості товарів з метою виведення капіталів за кордон або уникнення сплати податків; підробку документів; проведення операцій через «транзитні» фірми для приховування кінцевого бенефіціарного власника.

Актуальними проблемами 2025 року залишались схеми вивозу товарів без зворотного надходження валютної виручки, а також перерахування коштів за кордон без ввезення продукції в Україну в повному обсязі або належної якості, зокрема в оборонному секторі.

Узагальнені типові приклади транскордонного відмивання доходів наведено нижче.

Приклад 2025.4.5.1. Виведення коштів з України під виглядом придбання прав на ліцензійне програмне забезпечення[32]

Компанія А (резидент), що має ознаки компанії-оболонки, уклала з **Компанією Б** (нерезидентом, що також має ознаки компанії-оболонки) договір комісії на розповсюдження в Україні програмного забезпечення (далі – ПЗ) Microsoft, розробником якого є **Компанія В** (нерезидент, офіційний розробник ПЗ та дистриб'ютор Microsoft)**.**

Однак, хоча **Компанія Б** і уклала з **Компанією В** – розробником програмного забезпечення дистриб'юторський договір на його розповсюдження, цей договір не передбачав права на продаж ПЗ Microsoft, що ставить під сумнів законність подальших операцій та може свідчити про використання договору лише формально для прикриття схеми.

Передача ПЗ кінцевому покупцю здійснювалася шляхом завантаження з офіційного сайту розробника та отримання електронного ключа (цифрового коду). При цьому підтвердженням передачі ПЗ виступали лише акти приймання-передачі, а факт передачі ключів не підтверджувався жодними документами або технічними журналами.

Кінцевими покупцями ПЗ виступали **Група українських компаній**, серед яких є щойно створені підприємства та фізичні особи-підприємці, а також група сільськогосподарських підприємств із спільним КБВ, які придбали значний обсяг ліцензій Microsoft на суму близько 10 млн грн, що є нехарактерним для їхньої діяльності.

Приклад 2025.4.5.2. Експорт агропродукції без повернення валютної виручки[33]

Податковими органами виявлено схему, за якою сільськогосподарська продукція експортувалася за межі України фіктивною компанією, що мала лише формальні ознаки господарської діяльності або взагалі їх не демонструвала.

Підприємство-експортер не мало виробничих потужностей, працівників, основних засобів та не подавало звітності, проте подавало до митниці документи, що засвідчували нібито легальне походження товару.

У реальності документи містили недостовірні відомості, а ланцюг постачання продукції до **Фірми-експортера** не підтверджувався жодними податковими чи реєстровими даними. Валютна виручка за експортними контрактами не надходила в Україну, а рахунки компаній закривалися до настання строків її повернення.

Таким чином було здійснено безтоварний або «тіньовий» експорт, що вказує на транскордонну схему ухилення від валютного контролю та відмивання доходів.

[32] За даними НБУ

[33] За даними Державної податкової служби

В окремих випадках схема модифікувалася: експорт сільськогосподарської продукції здійснювався через залучення **Комісіонерів** за договорами комісії, де комісіонер формально виступав стороною зовнішньоекономічного контракту та відповідальним за фінансове врегулювання, тоді як фактичне право власності на товар зберігалося за комітентом. Це ускладнювало встановлення реального вигодонабувача та джерела походження продукції.

Приклад 2025.4.5.3. Схема з фіктивним продавцем та зустрічним експортом[34]

ДПС встановлено, що фактичним відправником сільськогосподарської продукції є підприємство реального сектору економіки, яке має необхідні виробничі потужності та трудові ресурси. Водночас стороною зовнішньоекономічного контракту виступає фіктивно створена компанія, відповідальна за фінансове врегулювання.

Уся логістика здійснюється фактичним власником товару, а облік передачі продукції фіктивному підприємству відсутній.

Експорт здійснюється за реквізитами фіктивного підприємства, валютна виручка не повертається. У схемах задіяні також компанії-нерезиденти, створені без мети ведення реального бізнесу. Їхніми посадовими особами часто виступають підставні українські чи іноземні громадяни.

Крім цього, виявлено випадки зустрічного експорту: нелегальний експорт продукції супроводжується імпортом фруктів та овочів на територію України з метою їх подальшої реалізації за готівку.

Приклад 2025.4.5.4. Схема ухилення від сплати податків при імпорті вживаних автомобілів

Держфінмоніторингом, з урахуванням інформації, отриманої від банківських установ, ПФР іноземної держави, правоохоронних органів та з відкритих джерел, виявлено схему за участю українських компаній та компаній-нерезидентів, спрямовану на ухилення від сплати податків шляхом формування незаконного податкового кредиту при здійсненні імпорту вживаних автомобілів.

Встановлено, що з рахунків **Групи юридичних осіб** було здійснено перерахування коштів як оплати за автомобілі на користь **Групи компаній-нерезидентів**, які в подальшому імпортували вживані авто на територію України. Джерелом походження коштів для розрахунків з нерезидентами є надходження від великої кількості юридичних та фізичних осіб. Фінансові операції мають транзитний характер, а також спостерігається невідповідність змісту вхідних та вихідних платежів.

[34] За даними Державної податкової служби

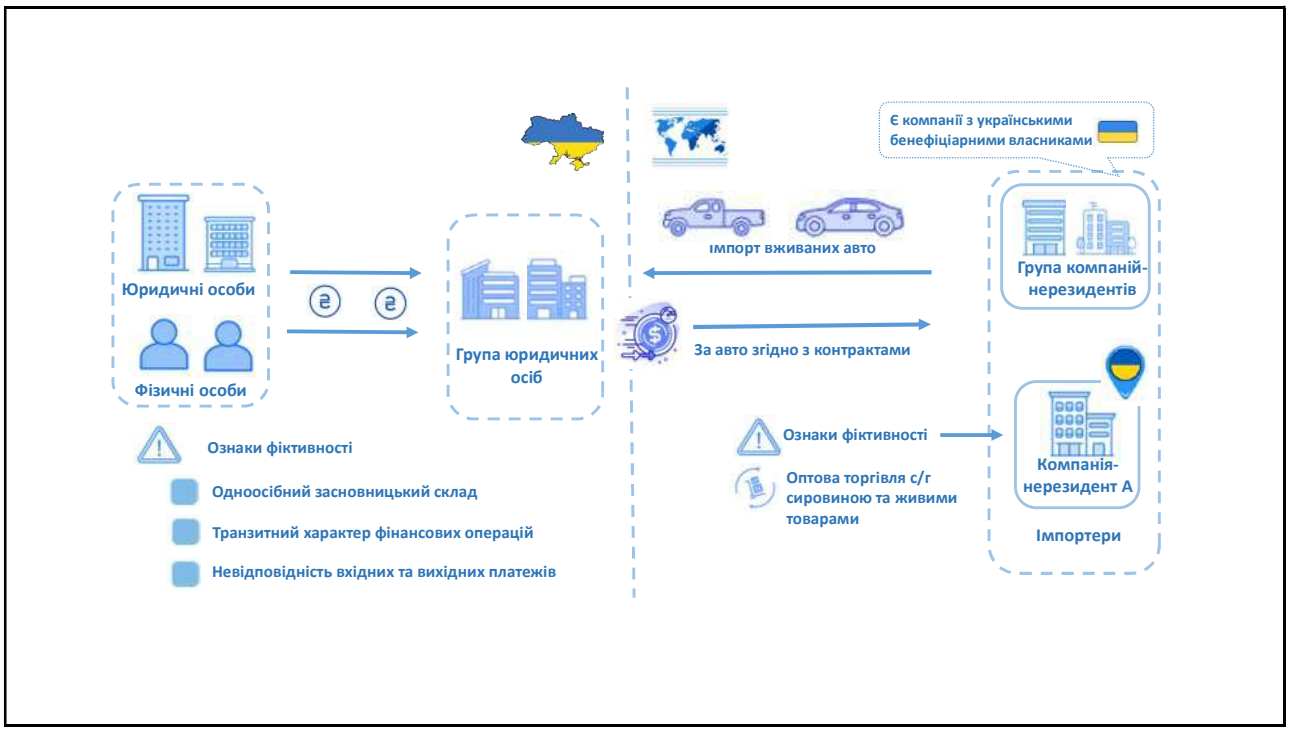
Групою юридичних осіб у податковому обліку відображено реалізацію автомобілів у значно меншій кількості, ніж фактично ввезено на митну територію України. Це дозволило мінімізувати податкові зобов'язання з податку на прибуток та податку на додану вартість, що призвело до ненадходження коштів до бюджету.

Також встановлено, що компанії з **Групи юридичних осіб** мають одноосібний засновницький склад, а необхідні умови для здійснення реальної підприємницької та економічної діяльності – відсутні. Це свідчить про можливі ознаки фіктивності таких суб'єктів.

Виявлено, що серед **Групи компаній-нерезидентів** є компанії, бенефіціарними власниками яких є громадяни України. Зокрема, **Компанія-нерезидент А** має ознаки фіктивності, а її основний вид діяльності – оптова торгівля сільськогосподарською сировиною та живими товарами, що не відповідає характеру операцій з імпорту автомобілів.

Таким чином, є підстави вважати, що рахунки **Групи юридичних осіб** використовуються для проведення схемних операцій з метою «замовлення послуг» із прихованого обготівковування та мінімізації податкових зобов'язань.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2025.4.5.5. Схема незаконного експорту сільськогосподарської продукції без зворотного надходження валютної виручки

Держфінмоніторингом, з урахуванням інформації правоохоронного органу, виявлено масштабну схему за участю професійної мережі з надання незаконних послуг з відмивання доходів та сприяння в ухиленні від сплати податків.

Встановлено, що **Групою українських компаній А** здійснюється експорт сільськогосподарської продукції на користь **Групи нерезидентів А**. При цьому, за інформацією банківських установ, відсутнє надходження валютної виручки за експортовану продукцію на рахунки, зазначені у зовнішньоекономічних контрактах.

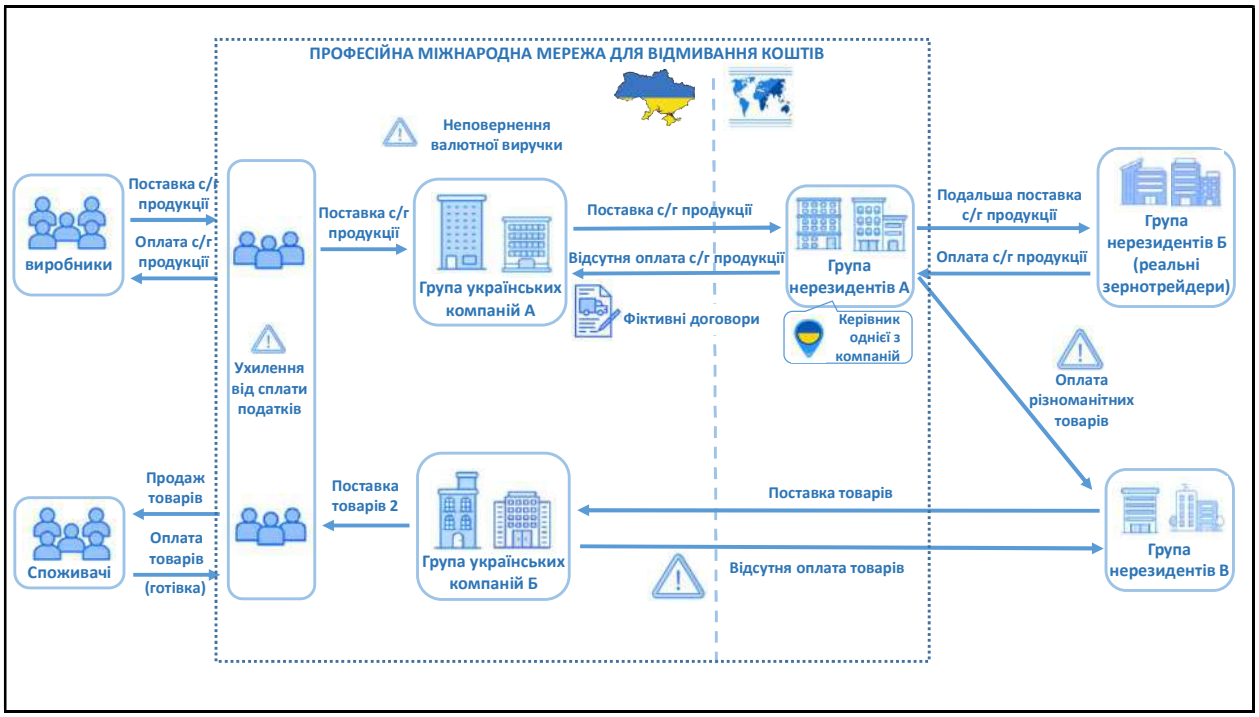
У подальшому за межами України **Група нерезидентів А** перепродала отриману сільськогосподарську продукцію **Групі нерезидентів Б** (реальним зернотрейдерам), отримуючи при цьому оплату за товар. За рахунок отриманих коштів **Група нерезидентів А** здійснила оплату за товари широкого асортименту (наприклад, промислові товари) на користь **Групи нерезидентів Б** (зареєстрованих переважно в країнах Азії).

У свою чергу **Група нерезидентів Б** експортувала інші товари широкого асортименту (наприклад, промислові товари) на користь **Групи українських компаній Б**, не отримуючи при цьому від них зворотної оплати.

Відомо, що імпортований товар у подальшому реалізується на оптово-роздрібних ринках України переважно за готівкові кошти. Ці кошти частково перерозподіляються в якості винагороди між учасниками схеми, а частково по новому колу спрямовуються на придбання сільськогосподарської продукції у реальних виробників з метою подальшого експорту.

Встановлено, що більшість компаній-нерезидентів із **Групи А** є компаніями-оболонками, мають українських засновників і створені для участі у зазначеній схемі. Також зафіксовано факти фальсифікації зовнішньоекономічних договорів, на підставі яких здійснювався експорт продукції.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2025.4.5.6. Схема незаконного виведення коштів за відсутності фактичної поставки товарів на митну територію України

Держфінмоніторингом, з урахуванням інформації, отриманої від ПФР іноземної держави, правоохоронного органу та з відкритих джерел, виявлено схему незаконного виведення коштів за кордон, учасниками якої є фінансові компанії.

Встановлено, що українською **Групою юридичних осіб** перераховано кошти на користь **Групи компаній-нерезидентів А** у якості попередньої оплати за насоси, деталі до них та лампи згідно з укладеними зовнішньоекономічними контрактами.

Основним джерелом походження коштів для купівлі валюти, яка у подальшому була переказана на користь **Групи компаній-нерезидентів А**, були надходження від **Фінансових компаній** у якості надання позики на умовах фінансового кредиту. Відомо, що ці компанії мають негативну репутацію та є учасниками схем переведення безготівкових коштів у готівку. Крім того, підприємства з **Групи юридичних осіб** мають одноосібний посадово-засновницький склад та здійснюють фіктивну господарську діяльність.

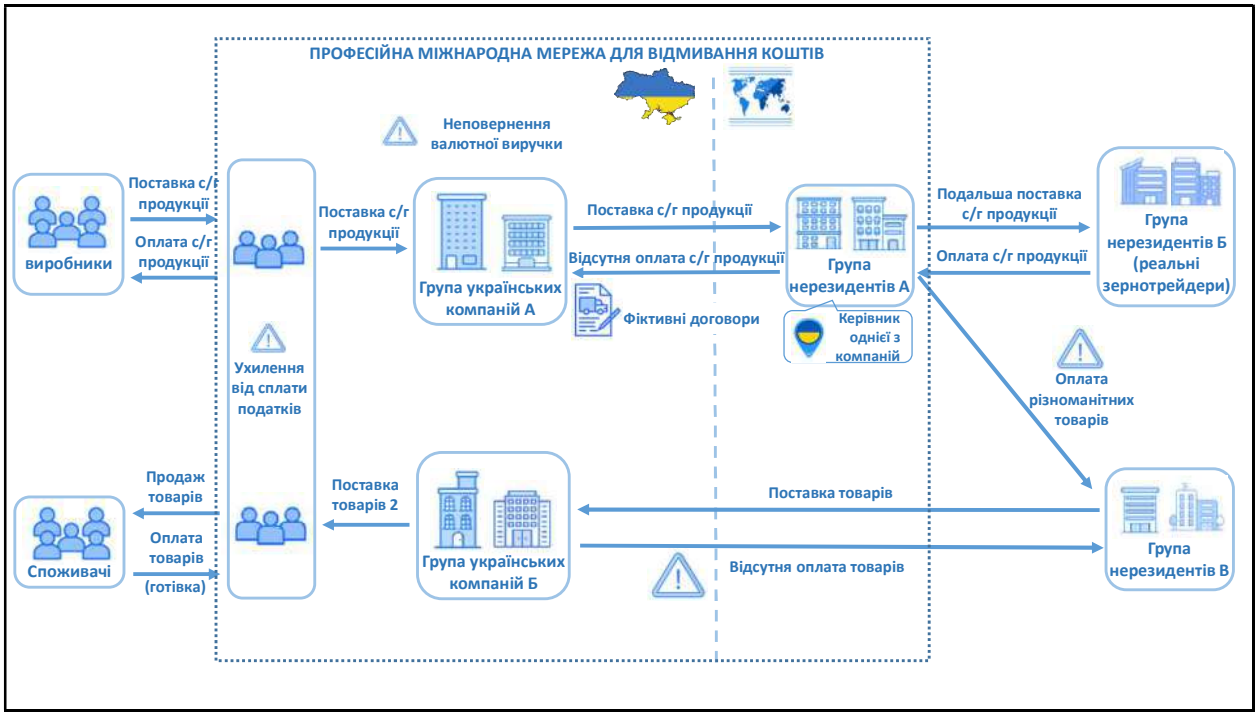
Встановлено, що **Група компаній-нерезидентів А** не здійснювала поставок оплаченої продукції на митну територію України згідно з укладеними контрактами, унаслідок чого розрахунки залишаються незавершеними.

У свою чергу, деякими підприємствами з **Групи юридичних осіб** подано позовні заяви до Господарського суду щодо повернення коштів **Групою компаній-нерезидентів А**. Це зроблено, ймовірно, з метою приховування реальної мети виведення коштів за кордон, оскільки під час судового розгляду не нараховуються пеня та штрафи за порушення строків поставки.

За інформацією ПФР іноземної держави встановлено, що в подальшому **Група компаній-нерезидентів А**, яка не є виробником оплаченої продукції, переказувала кошти не за призначенням іншій **Групі юридичних осіб Б**, які здійснюють інший вид діяльності.

Таким чином, є підстави вважати, що діяльність **Групи юридичних осіб**, **Фінансових компаній** та **Групи компаній-нерезидентів А** спрямована на незаконне виведення коштів за кордон та надання послуг іншим суб'єктам господарювання, пов'язаних із мінімізацією оподаткування.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2025.4.5.7. Виведення коштів за межі України за участю компанії-нерезидента з ознаками фіктивності

Держфінмоніторингом, з урахуванням інформації, отриманої від суб'єктів первинного фінансового моніторингу, ПФР іноземної держави та з відкритих джерел, виявлена схема незаконного виведення коштів за межі України за участю **Компанії-нерезидента А** з ознаками фіктивності.

Встановлено, що українським **Підприємством А** здійснено перекази за межі України на користь **Компанії-нерезидента А** згідно з укладеними зовнішньоекономічними договорами, а саме:

a) погашення боргу згідно з договором про відступлення прав вимоги, укладеним між **Підприємством А** (боржник), **Компанією-нерезидентом А** (новий кредитор) та **Компанією-нерезидентом Б** (первісний кредитор);

b) попередня оплата згідно з договором на поставку товарів, укладеним між **Підприємством А** та **Компанією-нерезидентом А**.

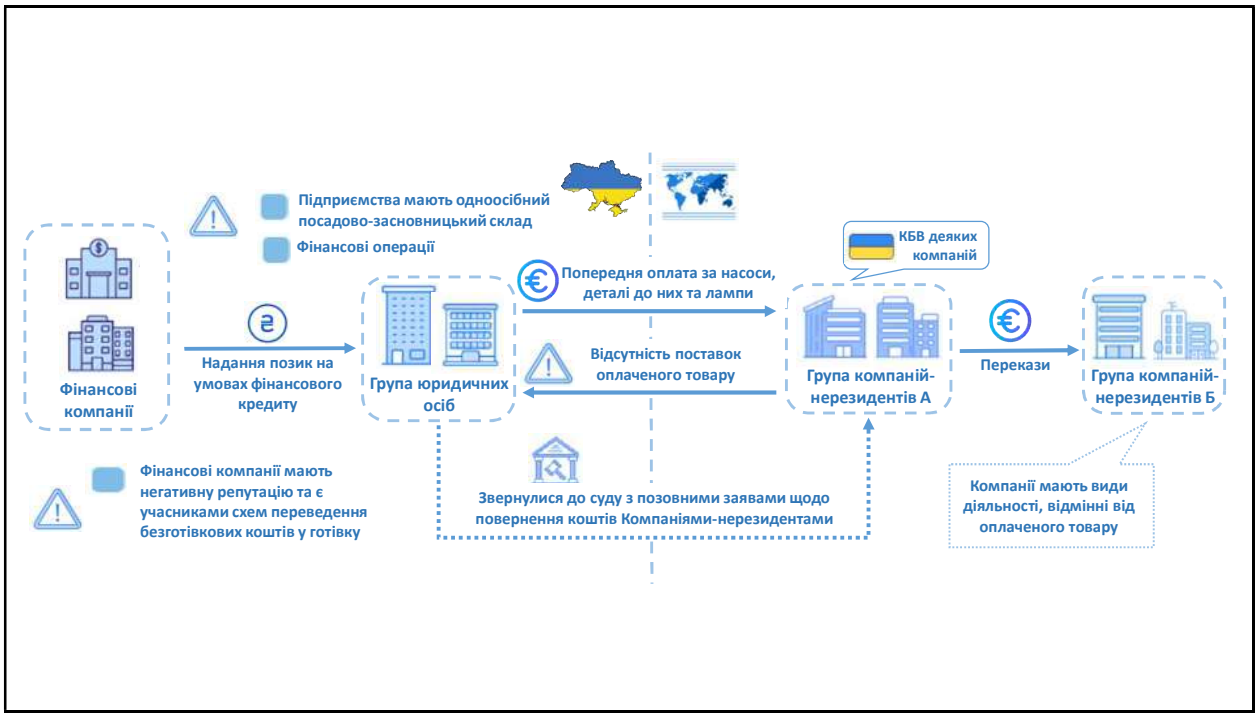
Відомо, що попередньо між **Підприємством А** та **Компанією-нерезидентом Б** укладено договір, згідно з яким **Компанія-нерезидент Б** поставила на митну територію України певну кількість товарів. Разом із цим встановлено, що вартість поставлених товарів значно менша, ніж сума боргу, зазначена у договорі про відступлення прав вимоги. Також відсутня поставка товарів від **Компанії-нерезидента А** на користь **Підприємства А**.

Джерелом походження коштів на рахунку **Підприємства А**, які в подальшому були перераховані на користь **Компанії-нерезидента А**, є надходження від **Групи юридичних осіб**, що здійснюють підозрілу діяльність та/або є учасниками кримінальних проваджень за підозрою в ухиленні від сплати податків.

Відповідно до інформації ПФР іноземної держави встановлено, що **Компанія-нерезидент А**, яка перебуває в стадії ліквідації, надавала широкий спектр послуг, здійснювала підозрілі транзакції з великою кількістю інших компаній, серед яких є «компанії-оболонки». У відкритих джерелах наявна негативна інформація щодо пов'язаних компаній, частина з яких має бенефіціарних власників з України та білорусі, а IP-адреси деяких зареєстровані в росії. Також встановлено, що кінцевий бенефіціарний власник **Компанії-нерезидента А** є громадянином України.

Враховуючи вищенаведене, є підстави вважати, що **Підприємство А** та **Компанія-нерезидент А** мають ознаки фіктивності та є учасниками схеми незаконного виведення коштів за межі України без фактичної поставки товару з метою подальшої легалізації незаконних доходів за кордоном.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2025.4.5.8. Привласнення коштів державного банку з використанням зовнішньоекономічних операцій

Держфінмоніторингом виявлено шахрайську схему привласнення коштів державного банку з використанням зовнішньоекономічних операцій та залученням компаній-нерезидентів.

Встановлено, що **Підприємством А** укладено генеральний кредитний договір з українським державним **Банком** щодо формування покриття за акредитивами для закупівлі природного газу за кордоном за умов його подальшої реалізації на території України. На підставі цього договору Банком відкрито непокритий безвідкличний акредитив та здійснено оплату придбання газу у **Компанії-нерезидента А**.

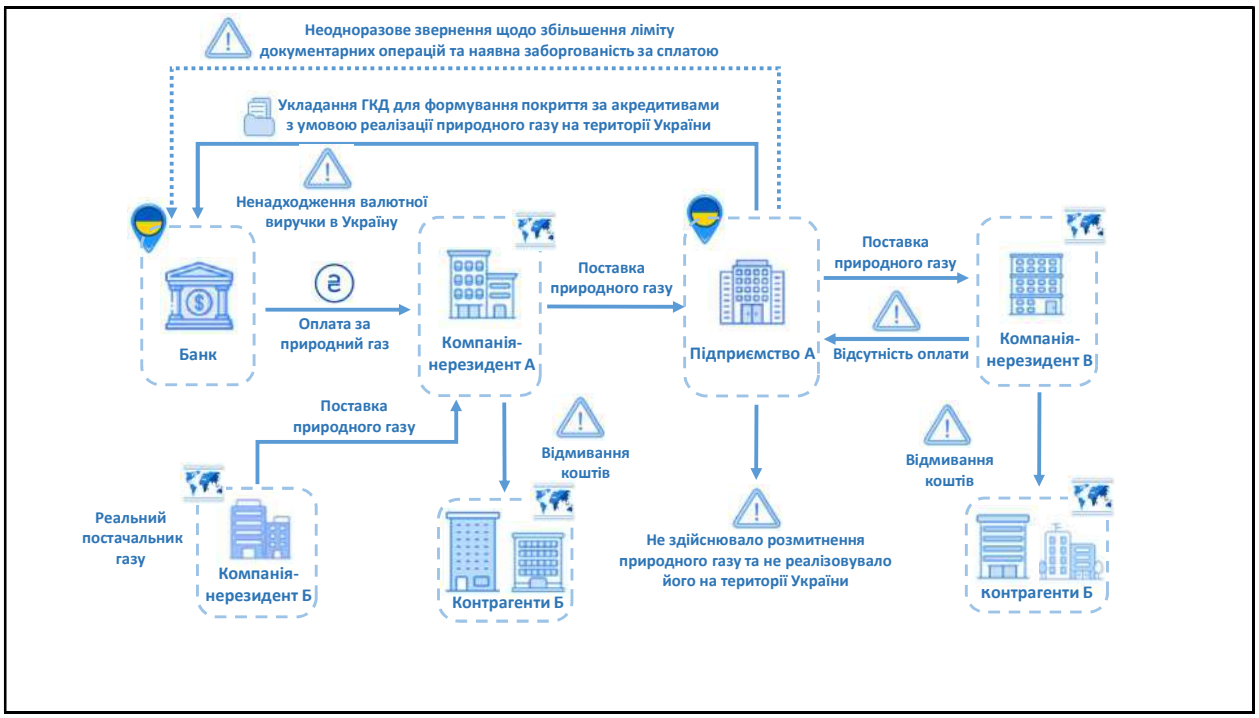
У свою чергу, **Компанія-нерезидент А** виступала посередником та закуповувала природний газ у реального постачальника — **Компанії-нерезидента Б**.

Водночас оплачений природний газ **Компанією-нерезидентом А** не було поставлено на митну територію України. Замість цього газ реалізовано за кордоном на користь **Компанії-нерезидента В** без відповідного митного оформлення та без отримання валютної виручки від його реалізації, що призвело до непогашення заборгованості за акредитивами.

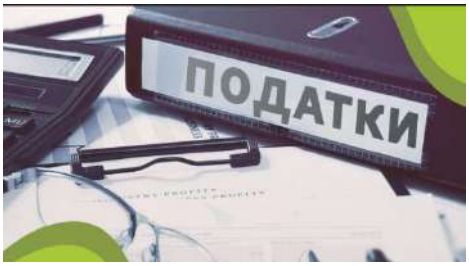
Відомо, що **Підприємство А**, попри наявну заборгованість, неодноразово зверталося до **Банку** з проханням збільшити ліміт документарних операцій. Також встановлено, що **Підприємство А** та **Компанія-нерезидент А** пов’язані між собою посадово-засновницькими зв’язками.

Враховуючи вищенаведене, є підстави вважати, що **Підприємством А** організовано схему незаконного заволодіння кредитними коштами державного **Банку** з використанням зовнішньоекономічних операцій та залученням пов’язаних компаній-нерезидентів з метою подальшої легалізації злочинних доходів за межами України.

Правоохоронним органом здійснюється досудове розслідування.


Неодноразове звернення щодо збільшення ліміту документарних операцій та наявна заборгованість за сплатою
Укладання ГКД для формування покриття за акредитивами з умовою реалізації природного газу на території України
Ненадходження валютної виручки в Україну
Банк
Оплата за природний газ
Компанія-нерезидент А
Поставка природного газу
Підприємство А
Поставка природного газу
Відсутність оплати
Компанія-нерезидент В
Поставка природного газу
Реальний постачальник газу
Компанія-нерезидент Б
Відмивання коштів
Контрагенти Б
Не здійснювало розмитнення природного газу та не реалізовувало його на території України
Відмивання коштів
контрагенти Б

РОЗДІЛ 4.6. ПОДАТКОВІ ЗЛОЧИНИ ТА СХЕМИ УХИЛЕННЯ ВІД ОПОДАТКУВАННЯ



У 2022-2025 роках в Україні зафіксовано активізацію податкових правопорушень, пов'язаних із ухиленням від оподаткування, легалізацією доходів, отриманих злочинним шляхом, та масовим використанням непрозорих фінансових інструментів.

Суб'єкти підприємницької діяльності з ознаками фіктивності формально ведуть господарську діяльність, однак не мають фактичних виробничих чи матеріальних ресурсів.

До таких схем також входить:

- створення **мережі ФОПів** для штучного «дроблення бізнесу»;
- **безтоварні операції**, що не супроводжуються реальними поставками товарів чи послуг;
- **транзит коштів без економічної мети** - із мінімальним залишком на рахунках наприкінці дня;
- **наявність негативної ділової репутації** та зв'язків із суб'єктами, що є фігурантами кримінальних проваджень;
- **переведення безготівкових коштів у готівку** через транзитні рахунки.

Одним із найпоширеніших інструментів у таких схемах є використання карткових рахунків фізичних осіб (так званих «дропів») або ФОПів, що дозволяє маскувати реальне походження коштів, здійснювати їх дроблення та подальше виведення в готівку.

Найбільш поширеними схемами податкових зловживань залишаються:

- **маніпуляції з ПДВ** – проведення фіктивних фінансово-господарських операцій із метою заниження податку на додану вартість;
- **незаконне виробництво підакцизної продукції** – особливо контрафактного алкоголю та тютюну;
- **реалізація товарів без акцизного маркування** – зокрема, використання фальшивих марок або їх повна відсутність;
- **конвертаційні центри** – переведення безготівкових коштів у готівку з метою ухилення від податків;
- **контрабанда** – переміщення товарів через кордон з порушенням митних процедур;
- **тіньовий ринок нерухомості** – приховування доходів від оренди та продажу, заниження ринкової вартості;
- **офшоризація прибутків** – використання закордонних компаній для уникнення оподаткування в Україні.
- **«сіра» зарплата** – виплата зарплат «у конвертах» без належного обліку та сплати податків.

4.6.1 Використання готівкових коштів

Готівкові кошти залишаються одним із ключових чинників ризику у фінансовій системі, особливо під час війни.

В умовах військової агресії їхнє застосування суттєво зростає, оскільки готівка дає змогу здійснювати непрозорі операції поза межами банківських установ - що робить її зручним інструментом для відмивання коштів, фінансування тероризму або інших незаконних дій.

Баланс між ризиками та необхідністю: роль готівки в умовах війни. В умовах війни наявність певного обсягу готівкових коштів залишається важливою з огляду на безпекові виклики - зокрема у разі відключень електроенергії та неможливості здійснення безготівкових розрахунків.

Сьогодні операції з готівкою належать до найризикованіших, оскільки їхня доступність і анонімність сприяють відмиванню доходів, фінансуванню тероризму та іншим злочинам, обходячи формалізовані канали фінансового моніторингу.

Використання готівкових коштів для ВК. У 2025 році готівкові кошти продовжують широко використовуватись для відмивання доходів, отриманих від незареєстрованої, прихованої або злочинної діяльності. Такі кошти спрямовуються на фінансування незаконних операцій, придбання активів або виплату винагороди за нелегальні послуги. На тлі триваючої війни і великої кількості внутрішньо переміщених осіб зберігається практика виплати неофіційної заробітної плати готівкою. Популярність використання готівки в різноманітних схемах, як і раніше, обумовлена складнощами її виявлення та відстеження переміщення між учасниками.

Використання готівкових коштів для ФТ. У 2025 році готівкові кошти залишаються одним із головних інструментів для фінансування тероризму, зокрема через їхню анонімність. Особливо в умовах війни готівка може бути використана для фінансування диверсій, колабораційної діяльності (до таких схем може залучатись підставні особи («дропи»)).

Інші злочини. Готівка використовується у схемах ухилення від оподаткування, підкупу посадовців, фінансування незаконного обігу зброї, наркотиків, торгівлі людьми, а також для забезпечення тіньового сектору економіки.

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

Приклад 2025.4.6.1.1. Схема фіктивного продажу товару за готівку з метою ухилення від сплати податків

Держфінмоніторингом виявлено схему, яка забезпечує незаконне виведення безготівкових коштів реального сектору економіки у тіньовий обіг, у тому числі в обхід системи оподаткування, за рахунок фіктивного продажу товарів за готівку.

Виявлено фінансові операції, пов'язані з акумулюванням коштів на рахунках **Групи юридичних осіб А**, отриманих від **Групи ФОПів** та **Групи юридичних осіб Б** у якості оплати за будівельні матеріали/послуги, обладнання, аграрну продукцію/обладнання, металобрухт. У подальшому ці кошти були спрямовані на користь **Компанії А** за рибну продукцію, яку вона імпортує від **Компаній-нерезидентів**. Очевидна невідповідність вхідних та вихідних призначень платежів свідчить про використання механізму «скрутки».

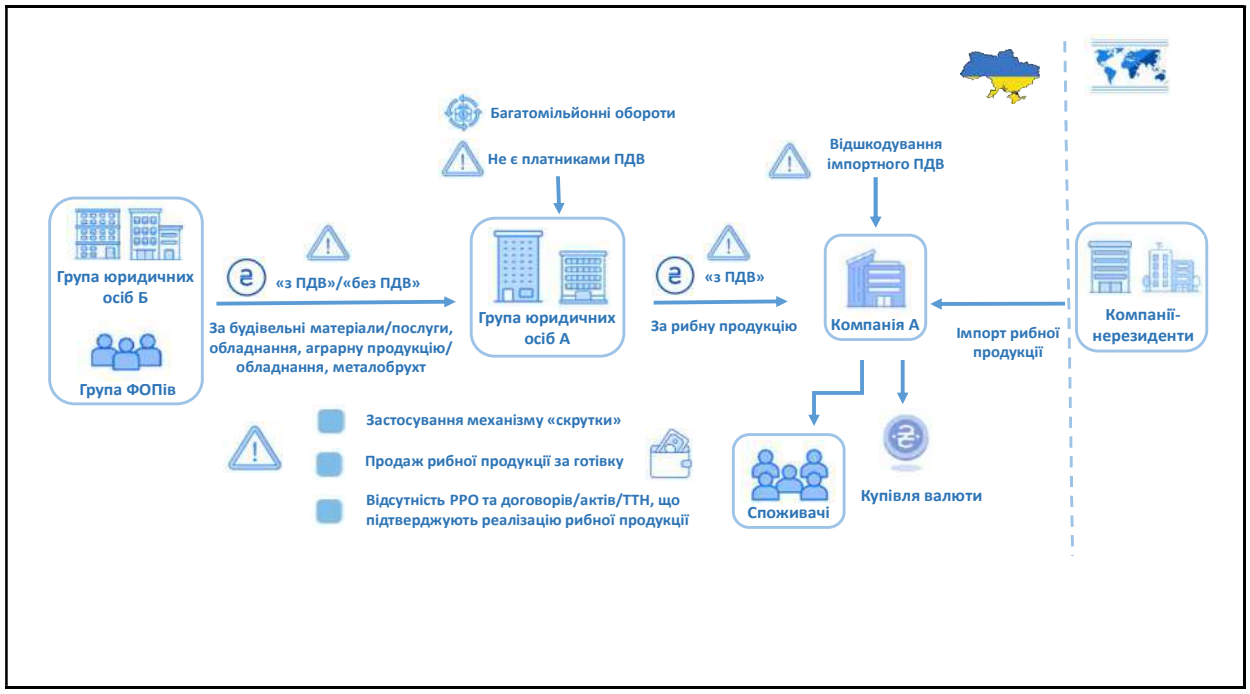
Привертає увагу, що на рахунки **Групи юридичних осіб А** кошти зараховуються як «з ПДВ», так і «без ПДВ» за один і той самий товар, тоді як перерахування на користь **Компанії А** здійснюється вже «з ПДВ». Водночас відповідно до відкритої інформації, **Група юридичних осіб А** не реєструвалась платником ПДВ, попри багатомільйонні обороти по рахунках.

Існують підозри, що **Компанія А** реалізує рибну продукцію переважно за готівку, проте не вносить її на власні рахунки як інкасовану. Це підтверджується відсутністю РРО, договорів, актів та товарно-транспортних накладних, які б засвідчували легальну реалізацію цієї продукції.

У свою чергу **Група юридичних осіб А** перераховує на користь **Компанії А** кошти, які можуть мати незаконне походження, зокрема отримані шляхом неправомірного завищення ціни на бюджетних тендерах.

Таким чином, виявлено схему прихованої конвертації безготівкових коштів у готівкові із застосуванням механізму «скрутки» та фіктивного продажу товару з метою відшкодування імпортного ПДВ, що призводить до ненадходження податків до Державного бюджету України.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2025.4.6.1.2. Використання готівки з метою приховування джерел походження коштів та ухилення від сплати податків

Держфінмоніторингом, з урахуванням інформації, отриманої від державного органу, виявлено схему, пов’язану з приховуванням джерела походження коштів шляхом придбання часток у статутному капіталі за заниженою вартістю з метою мінімізації податків продавцями часток та легалізації (відмивання) доходів, одержаних злочинним шляхом.

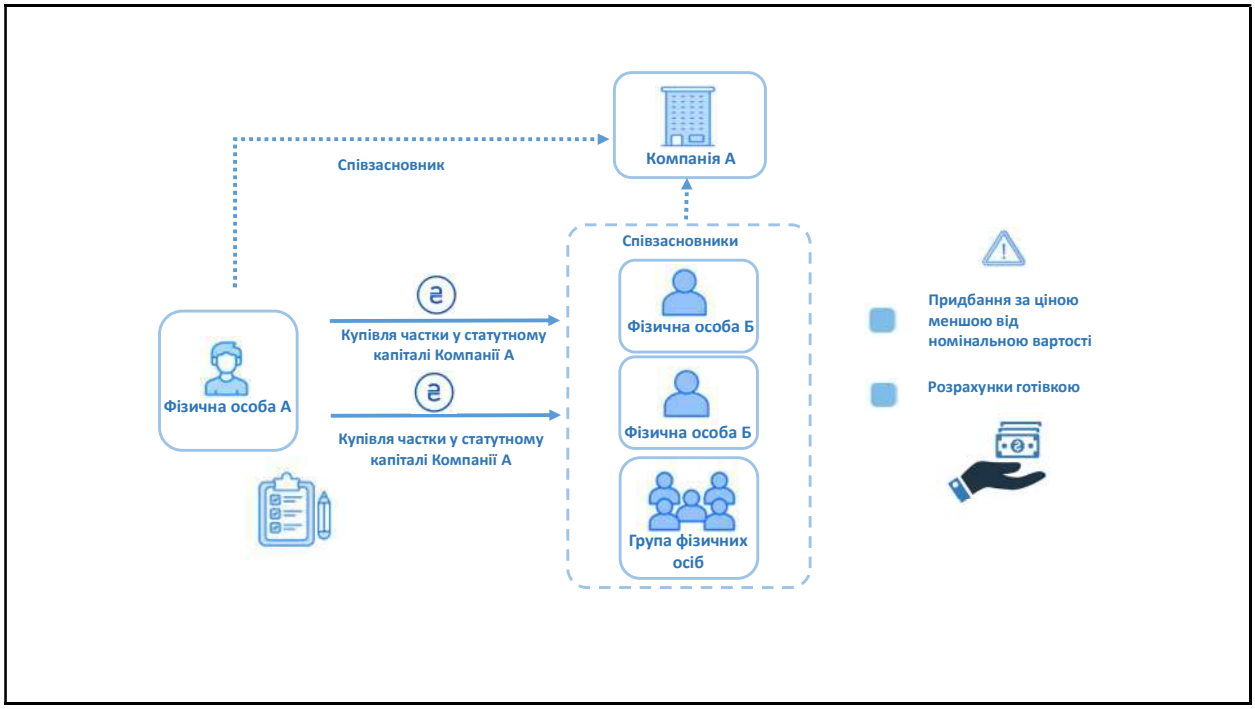
Встановлено, що **Фізичною особою А** укладено договори придбання часток у статутному капіталі **Компанії А** з двома фізичними особами з метою збільшення своєї участі у статутному капіталі цієї компанії.

Привертає увагу, що договірна ціна придбання часток у статутному капіталі майже у 20 разів менша за їх номінальну вартість. При цьому договорами передбачено, що розрахунки покупця з продавцями здійснюються виключно готівкою.

Таким чином, розрахунок відбувався поза межами банківської системи, ймовірно з метою уникнення фінансового моніторингу та необхідності підтвердження джерел походження коштів.

Враховуючи вищенаведене, є підстави вважати, що **Фізичною особою А** використано готівкові кошти для розрахунків за правочинами з метою приховати джерело походження коштів та уникнути сплати відповідних податків.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2025.4.6.1.3. Ухилення від сплати податків та відмивання коштів за участю групи ФОПів

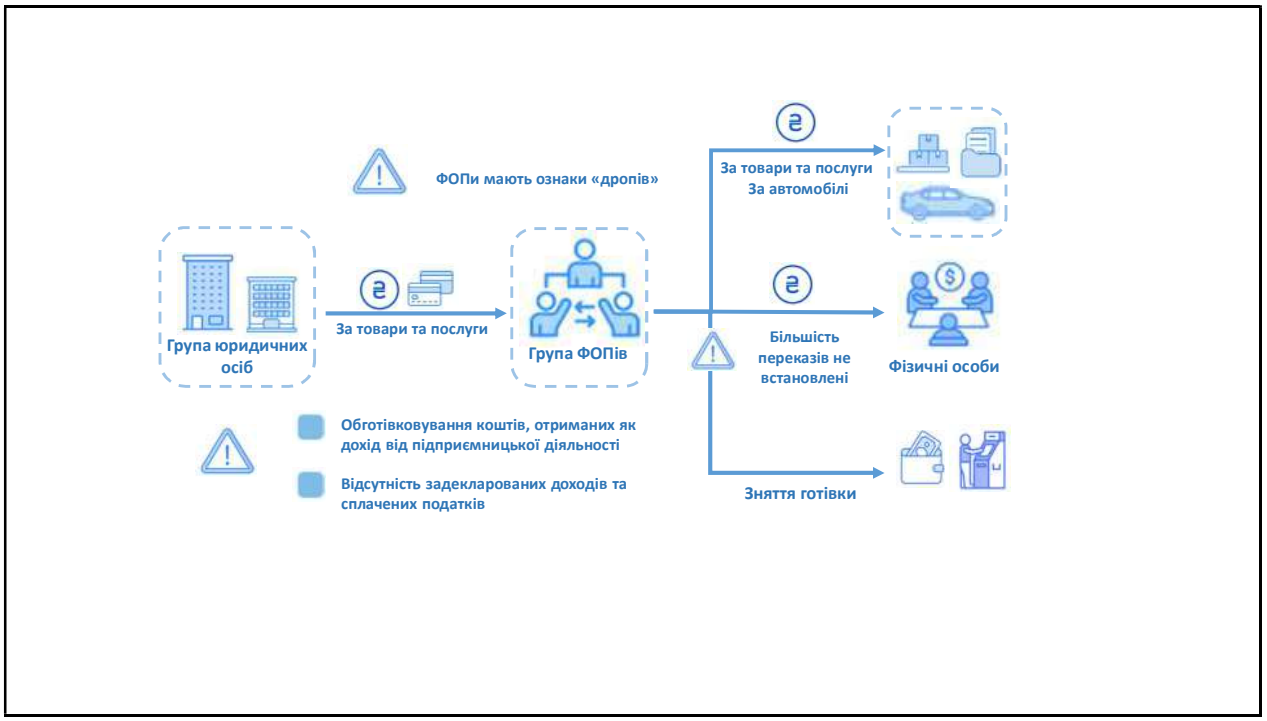
Держфінмоніторингом виявлено схему переведення коштів у готівку за участю **групи фізичних осіб-підприємців (ФОПів)**, яка пов'язана з ухиленням від оподаткування та відмиванням злочинних доходів.

Встановлено, що на рахунки **Групи ФОПів** зараховувалися безготівкові кошти від **Групи юридичних осіб** за товари та послуги. У подальшому частина коштів обготівковувалася, а інша розпорошувалася як P2P-перекази між фізичними особами або спрямовувалася в оплату товарів/послуг та придбання автомобілів.

Існують підозри, що зазначені фізичні особи та зареєстровані на них **ФОПи** мають ознаки «дропів», а їхні рахунки використовуються для транзитного переміщення коштів та переведення безготівкових надходжень - отриманих нібито як дохід від підприємницької діяльності - у готівку без документально підтвердженої господарської діяльності.

Зазначене може свідчити про функціонування **організованої злочинної групи**, діяльність якої спрямована на автономне відмивання коштів.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2025.4.6.1.4. Використання готівки в операціях купівлі-продажу металобрухту за участю фізичних осіб та фізичних осіб-підприємців з ознаками фіктивності

Держфінмоніторингом, з урахуванням інформації, отриманої від банківських установ та правоохоронного органу, виявлено схему використання готівки в операціях купівлі-продажу металобрухту з метою ухилення від сплати податків за участю **Фізичних осіб** та **Фізичних осіб-підприємців** з ознаками фіктивності.

Встановлено, що на рахунки **Групи юридичних осіб А** від **Групи юридичних осіб Б**, серед яких є учасники реального сектору економіки, перераховано значні суми коштів у якості оплати за металобрухт та зворотної фінансової допомоги. У подальшому ці кошти були перераховані:

a) **Групі юридичних осіб В** – за металобрухт, зворотну фінансову допомогу та згідно з договором комісії;

b) **Групі ФОПів** – з призначенням платежу «плата згідно з договором», які надалі обготівковували ці кошти та здійснювали перекази на інші власні рахунки як «перерахування чистого прибутку»;

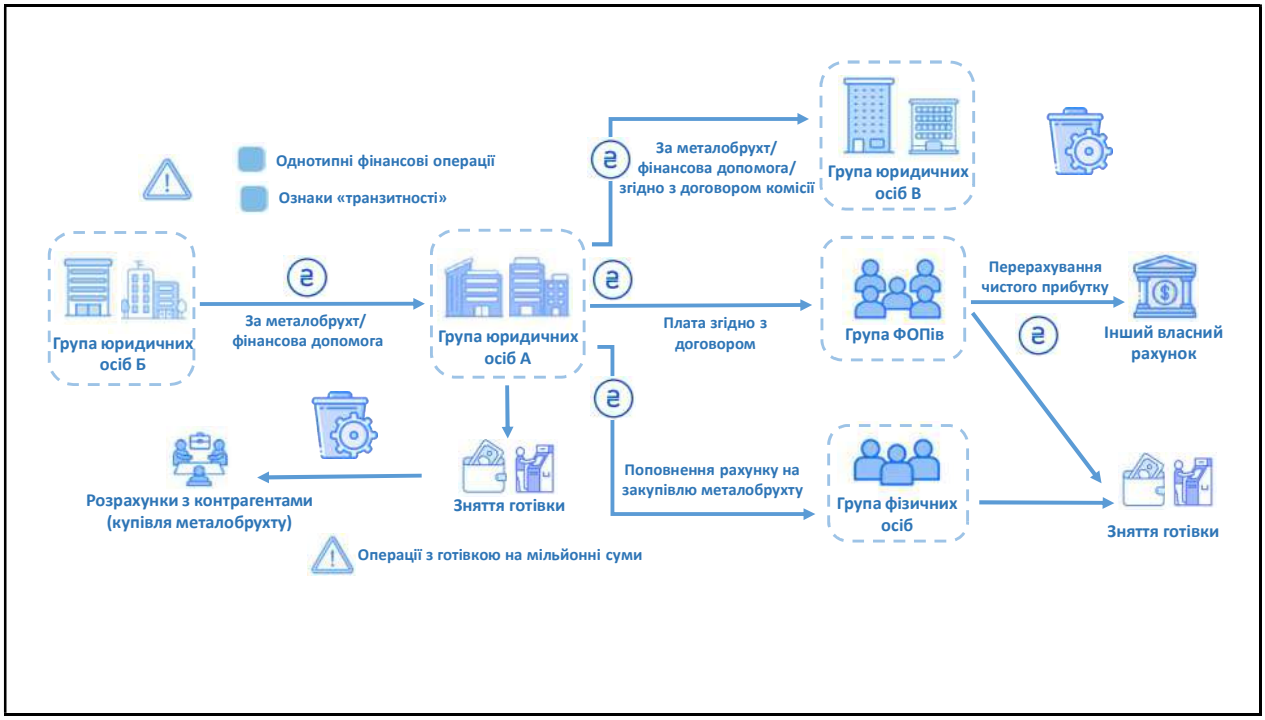
c) **Групі фізичних осіб** – у вигляді поповнення рахунку на закупівлю металобрухту, які в подальшому конвертували ці кошти у готівку.

Крім цього, **Група юридичних осіб А** також здійснювала зняття готівки для подальших розрахунків із контрагентами під час закупівлі металобрухту.

Привертає увагу, що зазначені фінансові операції мали транзитний характер: залишки коштів на рахунках постійно були незначними або нульовими за умов значних оборотів. Операції за своєю суттю однотипні. **Фізичні особи-підприємці**, які були задіяні у схемі, мають подібні характеристики ведення діяльності - однакові суми задекларованих доходів, мінімальні податкові зобов'язання, більшість зареєстрована в одній області та в один і той самий період. Відносно частини таких осіб наявна негативна інформація СПФМ.

Таким чином, є підстави вважати, що зазначена схема використання готівки була організована з метою надання незаконних послуг суб'єктам господарської діяльності реального сектору економіки для ухилення від сплати податків, виведення коштів у тіньовий сектор та переведення безготівкових коштів у готівку.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2025.4.6.1.5. Використання механізму «зустрічних потоків» для ухилення від сплати податків та «прихованої конвертації» безготівкових коштів у готівку

Держфінмоніторингом, з урахуванням інформації СПФМ, виявлено схему, пов'язану з наданням професійною мережею для відмивання коштів послуг з «прихованої конвертації» безготівкових коштів у готівку із використанням механізму «зустрічних потоків».

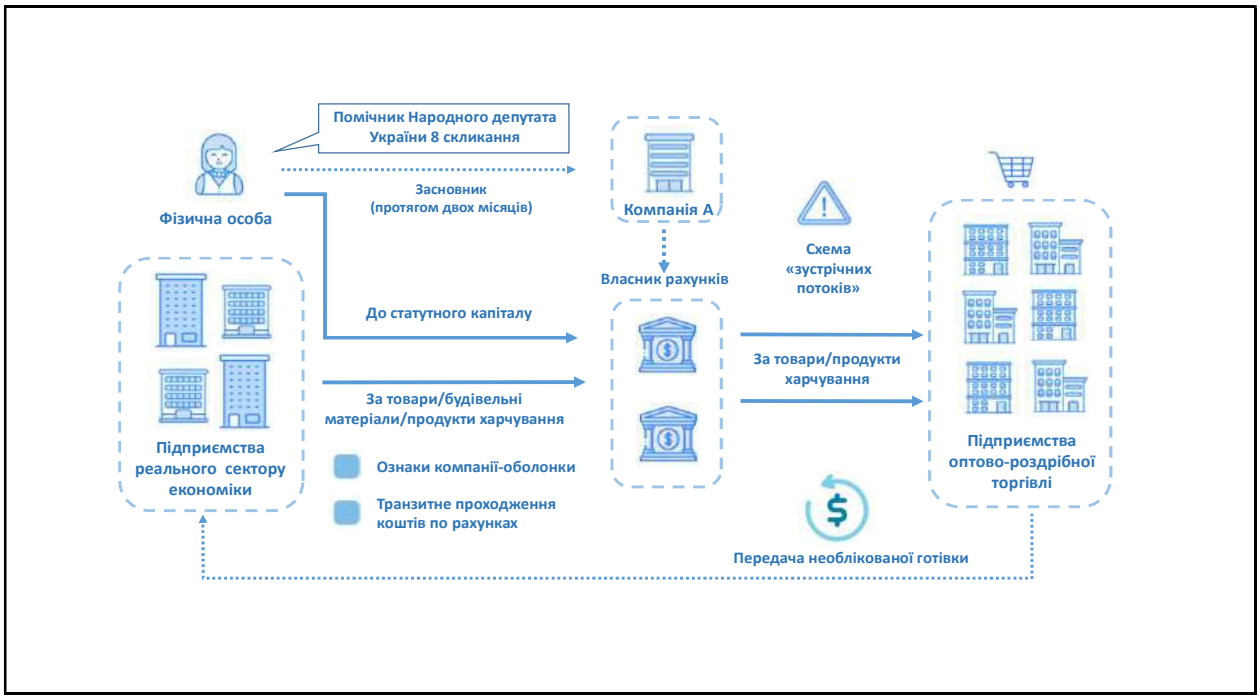
Встановлено, що на рахунки **Компанії А** переказувалися кошти від великої кількості юридичних осіб, серед яких є **підприємства реального сектору економіки**, у вигляді оплати за товар, будівельні матеріали та продукти харчування. У подальшому отримані кошти, з призначенням «оплата за товар/продукти харчування», транзитом перераховувалися на користь **підприємств оптово - роздрібної торгівлі**, які можуть мати значні обсяги необлікованої готівки та надавати послуги з «прихованої конвертації» безготівкових коштів у готівкові. При цьому застосовано механізм «зустрічних потоків», тобто проведення фіктивних безтоварних операцій.

Також встановлено, що на рахунок **Компанії А** було зараховано кошти з рахунку **Фізичної особи** у вигляді внеску до статутного капіталу. Надалі ці кошти також були перераховані на користь **підприємств оптово-роздрібної торгівлі**. Привертає увагу, що зазначена **Фізична особа** була помічником народного депутата України 8 скликання та входила до посадово - засновницького складу **Компанії А** лише протягом двох місяців.

Компанія А має ознаки фіктивності (компанії - оболонки): одноосібний посадово-засновницький склад, відсутність працівників, недекларування доходів, сплата мінімальних податків, здійснення транзитних фінансових операцій, що не мають очевидної економічної або законної мети.

Враховуючи викладене, є підстави вважати, що фінансові операції **Компанії А** спрямовані на сприяння ухиленню від сплати податків та приховане переведення безготівкових коштів у готівку.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2025.4.6.1.6. Схема «прихованої конвертації» безготівкових коштів в готівкові через підприємства оптово-роздрібної торгівлі

Держфінмоніторингом виявлено схему, пов'язану з діяльністю професійної мережі, що надає незаконні послуги суб'єктам реального сектору економіки, спрямовані на ухилення від сплати податків та легалізацію незаконних доходів шляхом «прихованої конвертації» безготівкових коштів у готівкові з використанням підприємств, задіяних у сфері оптово-роздрібної торгівлі.

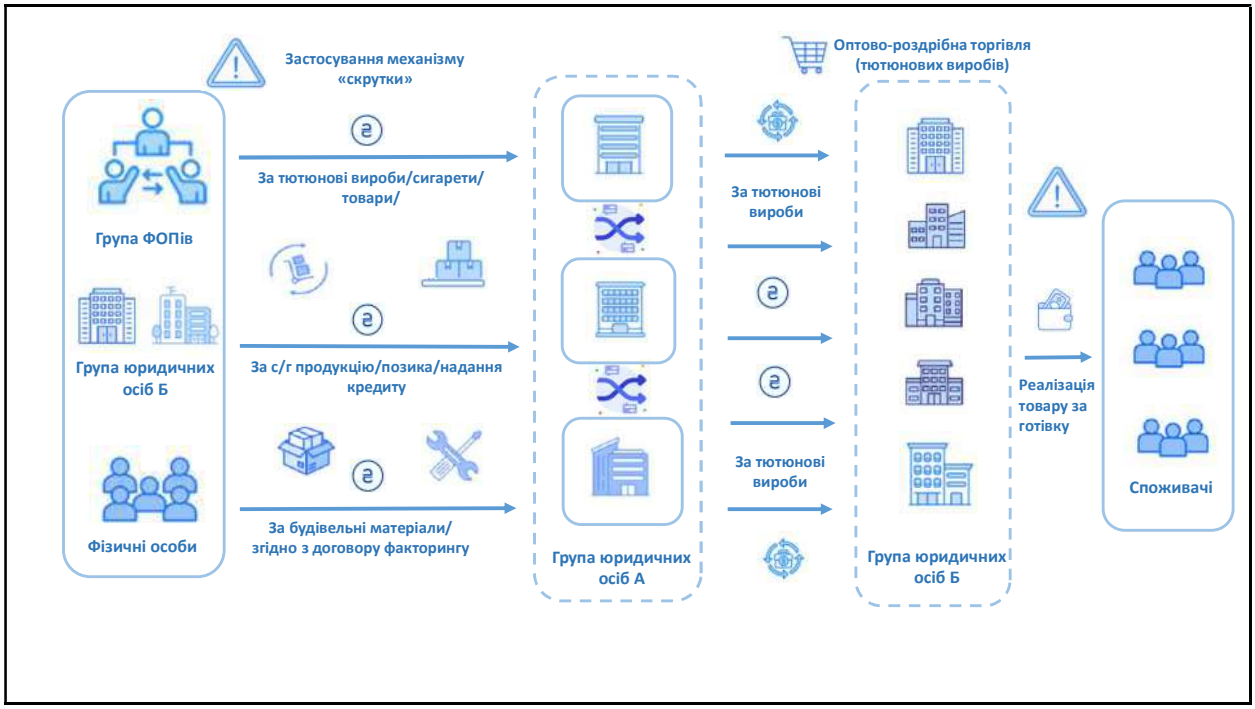
Встановлено, що на рахунки **Групи юридичних осіб А** надходили кошти від великої кількості юридичних осіб, фізичних осіб-підприємців та фізичних осіб з різноманітними призначеннями платежів - у якості оплати за тютюнові вироби, сигарети та інші товари, за будівельні матеріали, за послуги, за надання позики/фінансової допомоги, згідно з договором факторингу тощо. Зазначені кошти транзитом перераховувались на рахунки **Групи юридичних осіб Б** у вигляді оплати за тютюнові вироби та сигарети.

Відомо, що **Група юридичних осіб Б** є підприємствами, задіяними у сфері оптово-роздрібної торгівлі, зокрема тютюновими виробами. Підприємства цієї групи мають розгалужену торговельну мережу та здійснюють реалізацію товарів за готівку, що дає можливість коригувати документальні обсяги реалізації й приховувати фактичні обсяги продажу, отримуючи при цьому значні обсяги необлікованої готівки.

Підприємства **Групи юридичних осіб А** мають ознаки фіктивності: здійснюють «безтоварні» фінансові операції із постійно незначним залишком коштів на кінець дня, не мають виробничих потужностей, торговельно-складських приміщень чи інших активів, необхідних для ведення задекларованої господарської діяльності, та не мають ліцензій на продаж тютюнових виробів.

Таким чином, виявлено організовану схему, спрямовану на приховування частини отриманого доходу шляхом застосування механізму «скрутки» товарів, що використовується у схемах ухилення від сплати податків та фіктивного підприємництва.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2025.4.6.1.7. Схема обготівковування та ухилення від сплати податків за участю групи пов'язаних юридичних осіб та ФОП

Держфінмоніторингом виявлено схему за участю юридичних осіб та фізичних осіб-підприємців, яка забезпечувала незаконне виведення безготівкових коштів реального сектору економіки у тіньовий, неконтрольований державою обіг шляхом обготівковування коштів **фізичними особами-підприємцями (ФОПами)**, отриманих від підприємств, що займаються оптовою торгівлею сільськогосподарською продукцією.

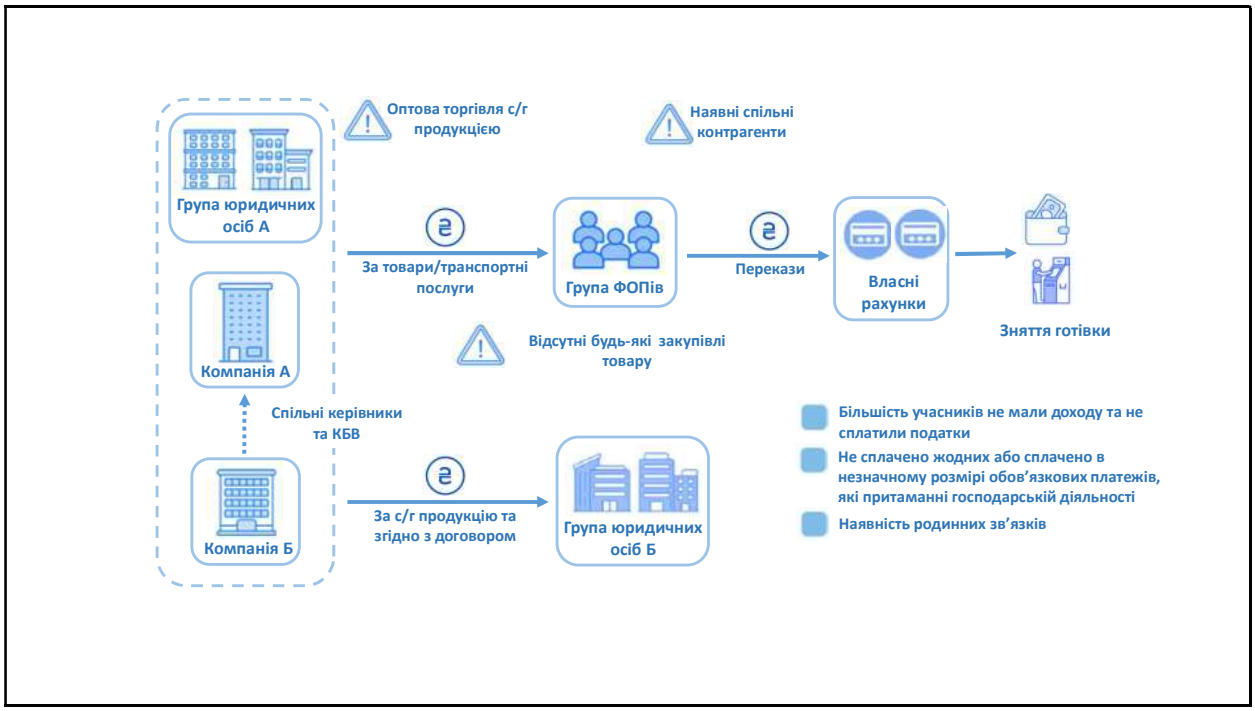
Встановлено, що **Групою юридичних осіб А**, у тому числі **Компанією А** та **Компанією Б**, які здійснюють оптову торгівлю сільськогосподарською продукцією, перераховано кошти на користь **Групи ФОПів** у якості оплати за товари та транспортні послуги, а також на користь **Групи юридичних осіб Б** за сільськогосподарську продукцію згідно з укладеними договорами. У подальшому **Група ФОПів** здійснювала переказ коштів на власні рахунки з подальшим їх обготівковуванням.

Привертає увагу, що підприємства з **Групи А** мають спільних контрагентів серед **Групи ФОПів**, а **Компанія А** та **Компанія Б** мають одного й того самого керівника та кінцевого бенефіціарного власника. Виявлені фінансові операції мають ознаки схемності та не мають очевидної економічної чи законної мети.

Для **Групи ФОПів** характерне їх нещодавнє створення, наявність родинних зв'язків між ними, відсутність задекларованих доходів та сплати податків. Більшість таких ФОПів не сплачували або сплачували в незначному розмірі обов'язкові платежі, притаманні господарській діяльності.

Враховуючи вищенаведене, є підстави вважати, що пов'язані між собою суб'єкти господарювання здійснюють незаконне виведення безготівкових коштів реального сектору економіки у тіньовий неконтрольований державою обіг та надають послуги з ухилення від сплати податків.

Правоохоронним органом здійснюється досудове розслідування.



4.6.2. Використання підставних осіб «дропів» та фізичних осіб-підприємців у схемах ухилення від оподаткування та відмивання коштів

У сучасних умовах практика використання підставних осіб («дропів») для проведення незаконних фінансових операцій залишається поширеною.

Зловмисники активно залучають соціально вразливі категорії населення – студентів, пенсіонерів, осіб із низьким рівнем доходів або тих, хто перебуває у складних життєвих обставинах з метою маскування кінцевих бенефіціарів фінансових потоків.

Основні тенденції:

Фізичні особи-підприємці (ФОП) в ролі «дропів» – тобто підставних суб'єктів для зарахування коштів, конвертації або транзитування коштів, що походять від незаконної діяльності.

Дроблення операцій – щоб не перевищувати встановлені ліміти, злочинці проводять велику кількість дрібних переказів через різних дропів.

Імітація законної фінансової діяльності під звичайну діяльність – операції виглядають легальними та не викликають автоматичних спрацювань систем моніторингу.

Широке застосування підставних осіб (дропів) – дозволяє злочинцям розшаровувати незаконні доходи, ускладнюючи їхнє відстеження.

Запровадження нових обмежень не усуває проблему повністю, а лише змінює поведінку учасників схем, які починають шукати «сірі» зони для проведення операцій.

Основні ризики, інструменти та наслідки використання дроп-схем

Ризики: масове використання «формально» легальних рахунків для приховування бенефіціарів;

Ключові інструменти: P2P-перекази, крипто-конверсії, онлайн-казино;

Наслідок: ускладнення відстеження та легалізації незаконних доходів.

Приклад 2025.4.6.2.1. Використання дропів в шахрайських схемах

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

Приклад 2025.4.6.2.2. Використання дропів для диверсійної діяльності.

Злочинці для фінансування протиправної та диверсійної діяльності використовують масові P2P-перекази, конвертацію криптовалюти у фіат і надходження від онлайн-казино на карткові рахунки дропів.

Приклад 2025.4.6.2.3. Використання готівки невідомого походження в операціях фізичних осіб, які мають ознаки «дропів»

Держфінмоніторингом, з урахуванням інформації СПФМ, виявлено аномальні фінансові потоки **Групи фізичних осіб**, які мають «транзитний» характер та здійснюються із використанням готівки невідомого походження.

На рахунок **Фізичної особи** молодого віку, що належить до соціально вразливих верств населення (студента), зараховувались кошти від **Групи фізичних осіб А** у вигляді P2P-переказів через платіжні сервіси або шляхом поповнення готівкою у відділенні без використання банківської картки.

Після зарахування коштів вони транзитом переказувались:

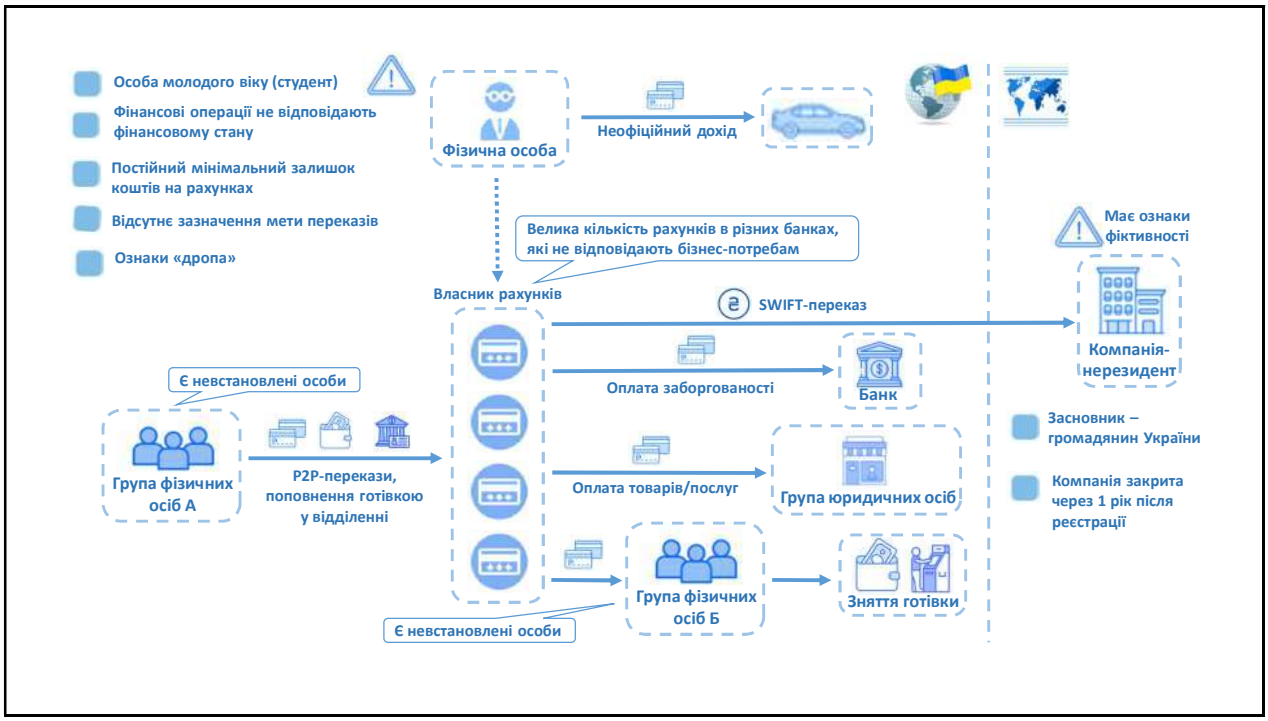
- на рахунки **Групи фізичних осіб Б** з подальшим обготівковуванням;
- на рахунки **Групи юридичних осіб** як оплата товарів/послуг;
- на рахунок **Банку** як оплата заборгованості;
- на користь **Компанії-нерезидента**, яка має ознаки фіктивності та пов'язана з українським громадянином.

Встановлено, що **Фізична особа** не має офіційно задекларованих доходів та сплачених податків, не є учасником діяльності суб'єктів господарювання та не зареєстрована як фізична особа-підприємець. Водночас наявні факти придбання нею рухомого майна, що може свідчити про легалізацію коштів невідомого походження.

Фінансові операції **Фізичної особи** є нехарактерними та не відповідають її задекларованому фінансовому стану. Операції мають виражений «транзитний» характер, що підтверджується постійним мінімальним або нульовим залишком на рахунках. Наявність великої кількості рахунків та банківських карток у різних банках не відповідає реальним потребам цієї особи, а під час переказів не зазначалась мета платежу.

Враховуючи викладене, є підстави вважати, що **Фізична особа** має ознаки «дропа», а фінансові операції по її рахунках здійснюються від імені та/або на користь іншої особи, яка не встановлена, у тому числі з використанням готівки невідомого походження.

Правоохоронним органом здійснюється досудове розслідування.



Використання ФОП як інструменту ухилення від оподаткування.

Можливі ознаки: по рахунках клієнта новоствореного ФОП відбувається сплеск зарахувань від аномальної кількості від фізичних осіб; рух коштів має транзитний характер; наявна активність в нічний час. Надалі кошти можуть бути зняті/перераховані на власну карту фізичної особи зі зняттям готівки чи здійсненням перерахувань (P2P) третім особам.

Також наявні випадки перерахування з рахунку ФОП коштів на рахунки інших ФОП/фізичних осіб (переважно в інші банки). Призначення платежу зазвичай не містять конкретизації суті наданих послуг чи товару, розповсюдженим є призначення платежі «надання фінансової допомоги», «надання позики», «повернення боргу» тощо. Іноді призначення платежу містить реальну інформацію щодо суті операції, зокрема «крипта» або «обмін валют».

Використання механізмів так званого «дроблення бізнесу»

Деякі суб'єкти застосовують механізми так званого «дроблення бізнесу» шляхом залучення суб'єктів господарювання ФОП.

«Дроблення бізнесу» - штучний поділ великих чи середніх прибуткових компаній на десятки, чи сотні ФОП, які працюють на спрощеній системі оподаткування. На практиці, після того як один ФОП досягає граничного обсягу доходу (ліміту) відповідної групи платника єдиного податку, відбувається введення до схеми іншого.

Використання таких механізмів свідчить про штучний розподіл і ведення бізнесу через інших суб'єктів господарювання, зокрема через залучення фізичних осіб-підприємців, які мають право застосовувати спрощену систему оподаткування. Зазначені механізми не містять жодної ділової мети та використовуються з метою ухилення від сплати податків.

Схеми «Дроблення бізнесу» мають наступні характерні ознаки, що свідчать про взаємозв'язки між ФОП, зокрема спільних контрагентів, адреси, керівників, контактні дані або однотипні фінансові операції.

Ознаки схем «дроблення бізнесу»:

- спільні IP-адреси, електронні пошти, адреси реєстрації;
- здійснення господарської діяльності під однією торговою маркою (брендом/торговою мережею);
- спільні представники, бухгалтери, довірені особи, наймані працівники;
- спільне місце реалізації товарів та послуг (адреса магазину, інтернет-сайту);
- наявність єдиного центру ухвалення рішень, який координує діяльність усіх ФОП;
- найчастіше залучаються особи з малозабезпечених верств населення, зокрема, безробітні особи, студенти, особи похилого віку (пенсіонери), ВПО тощо.

Приклад 2025.4.6.2.4. Застосування інструменту «дроблення бізнесу» для ухилення від сплати податків та переведення коштів у готівку

Держфінмоніторингом, з урахуванням інформації, отриманої від суб'єктів первинного фінансового моніторингу, виявлено схему, пов'язану з наданням незаконних послуг з ухилення від сплати податків та конвертації безготівкових коштів у готівку у великих обсягах шляхом застосування інструменту «дроблення бізнесу» за участю **Групи фізичних осіб-підприємців (ФОПів)** з ознаками фіктивності.

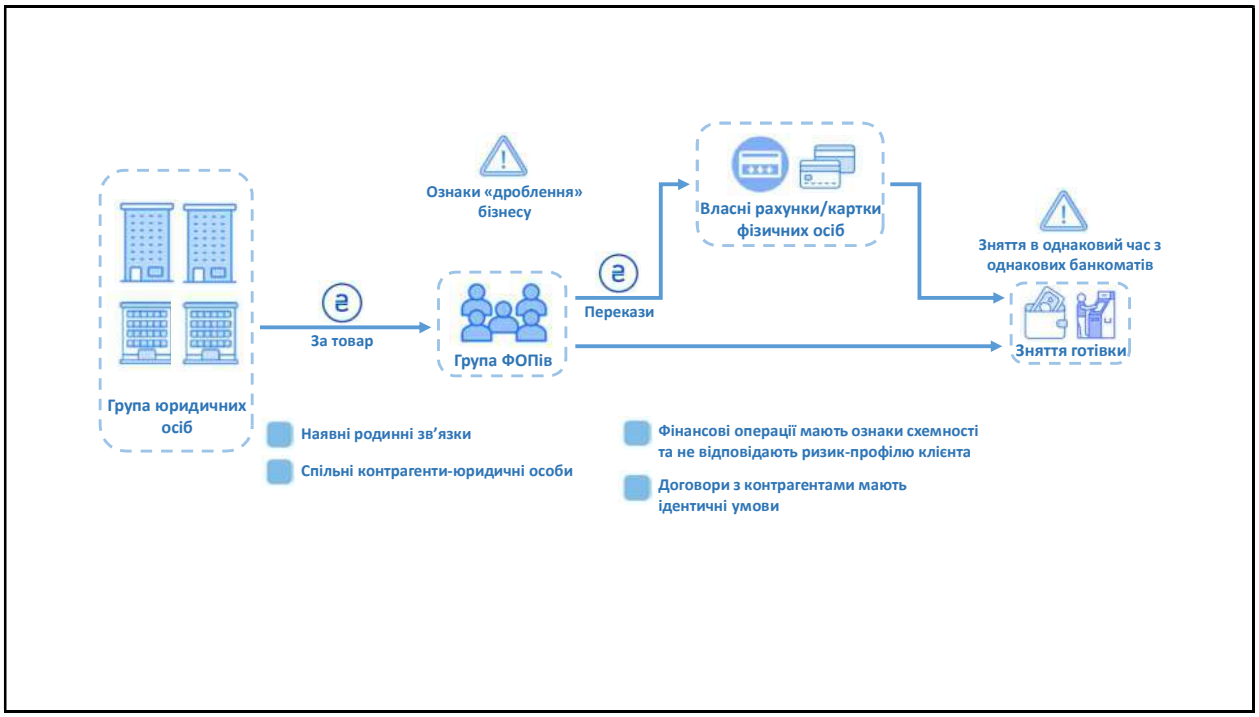
Встановлено, що на рахунки значної **Групи ФОПів** було зараховано кошти від **Групи юридичних осіб** у якості оплати за товар. Надалі отримані кошти переважно було знято готівкою та частково перераховано на власні рахунки або банківські картки інших фізичних осіб.

Готівка знімалася в повному обсязі переважно в один і той самий час з одних і тих самих банкоматів. Окрім цього, готівкові операції проводилися (структурувалися) таким чином, щоб обійти нормативні вимоги щодо порогових фінансових операцій.

Фінансові операції **Групи ФОПів** не відповідають ризик - профілю клієнтів та мають ознаки схемності. Група характеризується наявністю спільних контрагентів - юридичних осіб та родинними зв'язками між окремими ФОПами. Договори з **Групою юридичних осіб** щодо розрахунків і умов оплати є ідентичними.

Враховуючи вищенаведене, є підстави вважати, що діяльність зазначених фізичних осіб є елементом схеми «дроблення бізнесу», спрямованої на зменшення податкового навантаження та приховане обготівковування коштів.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2025.4.6.2.5. Використання мережі ФОП у схемі «дроблення бізнесу» для ухилення від оподаткування та легалізації доходів

Державною податковою службою встановлено масштабну схему штучного поділу бізнесу великих торгівельних мереж між сотнями фізичних осіб-підприємців. Її метою було мінімізація податкових зобов'язань та створення передумов для можливого відмивання доходів, одержаних злочинним шляхом.

Виявлено 7 торгівельних мереж (6 у сфері техніки та електроніки та 1 у сфері реалізації одягу), діяльність яких була формально розподілена між 491 ФОП із загальним оборотом понад 4 млрд грн. Попри декларовану незалежність підприємців, аналіз вказував на фактичне централізоване управління всіма процесами.

Дослідження встановило використання однакових IP-адрес, спільних адрес реєстрації та торгових точок, єдиної торгової марки та спільного персоналу. Це підтвердило штучний характер поділу бізнесу та узгодженість дій між ФОП.

За результатами перевірок ДПС визначено недоотримання бюджетом 668,5 млн грн ПДВ. Матеріали передано до Бюро економічної безпеки України для подальшого розслідування.

Ключові індикатори ризику включають: масову реєстрацію пов'язаних ФОП, відсутність ознак самостійної діяльності, надмірні для ФОП обороти, централізацію фінансових потоків та концентрацію операцій у межах однієї мережі.

РОЗДІЛ 4.7. ВІДМИВАННЯ ДОХОДІВ, ОТРИМАНИХ ВІД ШАХРАЙСЬКИХ ДІЙ ТА КІБЕРЗЛОЧИНІВ

У 2025 році шахрайство й кіберзлочинність значно зросли. Злочинці дедалі частіше застосовують соціальну інженерію, фішингові ресурси, deepfake та генеративний ШІ, націлюючись передусім на молодь і людей похилого віку.

Отримані злочинним шляхом кошти проходять через мережі підставних осіб («дропів») або розподіляються на рахунки підставних ФОПів та переводяться у готівку або криптовалюту. Найчастіше використовуються анонімні фінансові сервіси, зокрема P2P-перекази, електронні гаманці, криптовалютні біржі та платіжні системи з мінімальними вимогами до ідентифікації. Такі операції супроводжуються дробленням платежів, використанням міксерів, анонімних монет і cross-chain мостів.

Використання кол-центрів у злочинних мережах

Незаконні кол-центри перетворилися на багатофункціональний інструмент організованої злочинності, що використовується як в Україні, так і за її межами.

Через такі структури реалізується широкий спектр протиправної діяльності – від різних форм шахрайства (телефонного, інвестиційного, кредитного, фішингового) до вербування осіб, торгівлі людьми, збуту наркотичних засобів, вимагання, відмивання коштів та технічного супроводу кіберзлочинів.

Такі кол-центри мають гнучку структуру, цифрову анонімність та використовують зашифровані канали комунікації, що робить кол-центри одним із найнебезпечніших елементів сучасного кримінального середовища.

Приклади злочинів через кол-центри:

Телефонне шахрайство: це найбільш поширений вид злочинів. Зловмисники видають себе за співробітників банків, державних органів, правоохоронців або мобільного оператора, щоб виманити у жертв персональні дані, номери банківських карток, паролі або коди доступу.
Інвестиційне шахрайство: злочинці обіцяють жертвам надприбутки від інвестицій у криптовалюти, акції, цінні метали чи інші активи. Вони створюють фейкові платформи та сайти, які імітують легальні брокерські компанії, а потім виводять кошти жертв, не здійснюючи жодних реальних інвестицій.

Шахрайство під виглядом допомоги: в умовах війни, шахраї створюють фейкові благодійні фонди або волонтерські організації, щоб виманити кошти у небайдужих громадян, які хочуть допомогти Збройним Силам України або постраждалим від війни.

Вербування та торгівля людьми:

Трудове рабство: під виглядом високооплачуваної роботи оператором кол-центру, людей вербують та змушують працювати в «жахливих» умовах, фактично утримуючи в неволі. Паспорти вилучають, а будь-які спроби втечі придушують.

Вербування для злочинної діяльності: деякі кол-центри займаються вербуванням нових «співробітників» для своєї злочинної мережі. Жертвами стають молоді люди, які шукають роботу і не усвідомлюють, що їх залучають до кримінальної діяльності. Шахраї пропонують «легкі гроші» за виконання злочинних завдань, наприклад, підпалів автомобілів військовослужбовців або об'єктів інфраструктури.

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

Приклад 2025.4.7.1. Шахрайство з використанням deepfake-технології під час верифікації фізичної особи[35]

Банківською установою зафіксовано випадок використання технологій штучного інтелекту (ШІ) з метою незаконного проходження дистанційної ідентифікації та отримання доступу до рахунку клієнта.

Зловмисниками було застосовано інструменти **створення візуальних масок (deepfake)**, які накладалися поверх відеозображення іншої особи під час проходження процедури відеоверифікації.

Крім того, для введення в оману системи біометричного контролю було використано технології, що дозволили успішно пройти **liveness detection** — перевірку на ознаки «живого» обличчя, яке є стандартним елементом комплексної KYC-процедури.

Застосування deepfake-технологій дало можливість зловмисникам створити штучне враження, що процедуру проходить реальний власник рахунку, що, своєю чергою, дозволило ініціювати подальші фінансові операції від його імені.

Використання вдосконалених методів підміни обличчя та обходу систем біометричної автентифікації свідчить про **підвищення рівня шахрайських схем**, що спираються на сучасні технології штучного інтелекту.

[35] За даними НБУ

Приклад 2025.4.7.2. Використання підроблених документів для шахрайського заволодіння коштами банківської установи

Держфінмоніторингом, з урахуванням інформації, отриманої від суб'єктів первинного фінансового моніторингу та правоохоронного органу, виявлено схему шахрайського заволодіння грошовими коштами банківської установи на підставі умисно підроблених документів.

Відомо, що **Група фізичних осіб**, пов'язаних між собою родинними зв'язками, відкрила у **Банку А** валютні та депозитні рахунки, на які протягом певного часу здійснювала внесення готівки. Зняття коштів з цих рахунків також здійснювалося готівкою. При цьому сума задекларованих офіційних доходів **Групи фізичних осіб** є значно меншою, ніж сума внесених на депозит коштів. Більшість вкладів мали «циклічний» характер – відкривались на однакові суми та на однакові періоди. Відсутня інформація про заборгованість **Банку А** перед **Групою фізичних осіб** щодо повернення депозитів.

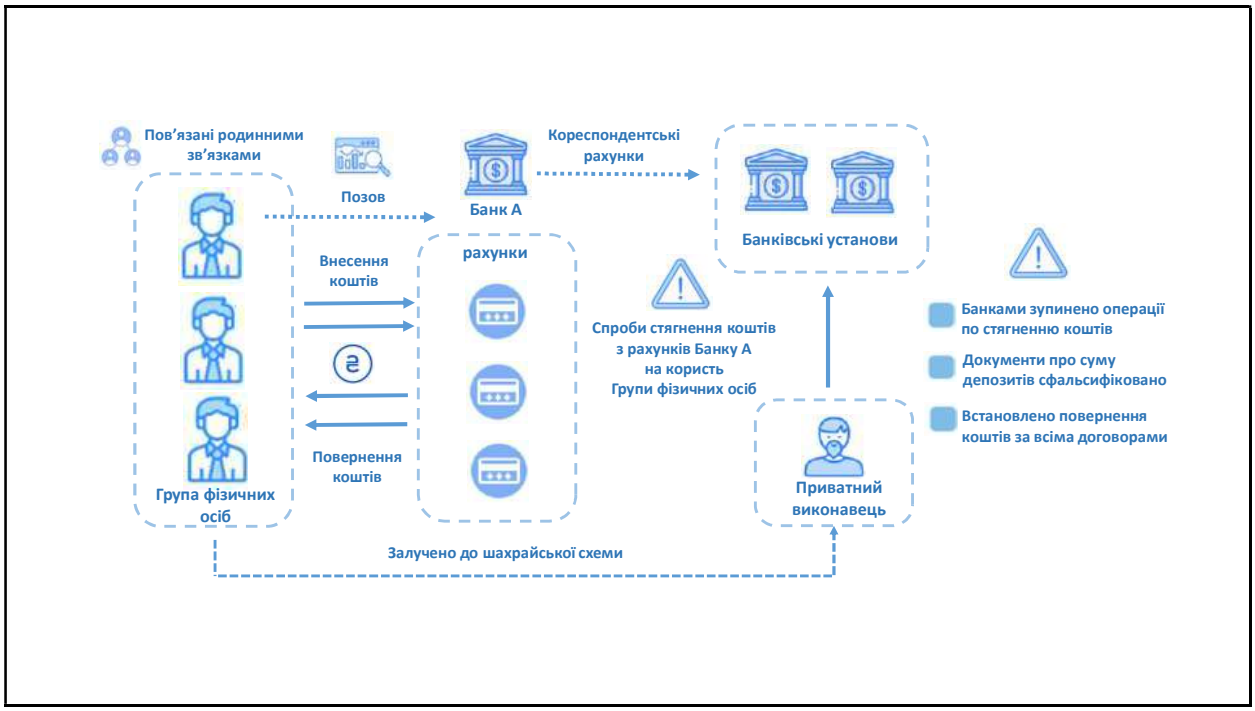
Разом із цим встановлено, що одна **Фізична особа** з групи звернулася до суду з позовом до **Банку А** про нібито шахрайські дії керівника одного з відділень банку та привласнення ним коштів, внесених на депозити.

Для обґрунтування позову було подано умисно підроблені документи, які начебто підтверджували суми внесених на депозит коштів. За зазначеним фактом відкрито кримінальне провадження.

Встановлено, що до реалізації злочинної схеми залучено **Приватного виконавця**, який здійснив спроби стягнути кошти з кореспондентських рахунків **Банку А**, відкритих в інших банківських установах, в інтересах **Групи фізичних осіб**, на підставі сфальсифікованих документів.

Враховуючи ознаки шахрайських дій, банківськими установами та Держфінмоніторингом було прийнято рішення про зупинення фінансових операцій, пов'язаних зі стягненням коштів **Банку А** на користь **Групи фізичних осіб** через **Приватного виконавця**.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2025.4.7.3. Шахрайське заволодіння коштами фізичних осіб під виглядом продажу нерухомості

Держфінмоніторингом, з урахуванням інформації, отриманої від суб'єктів первинного фінансового моніторингу та правоохоронного органу, виявлено схему, пов'язану з шахрайським заволодінням коштів фізичних осіб під виглядом продажу нерухомості незавершеного будівництва.

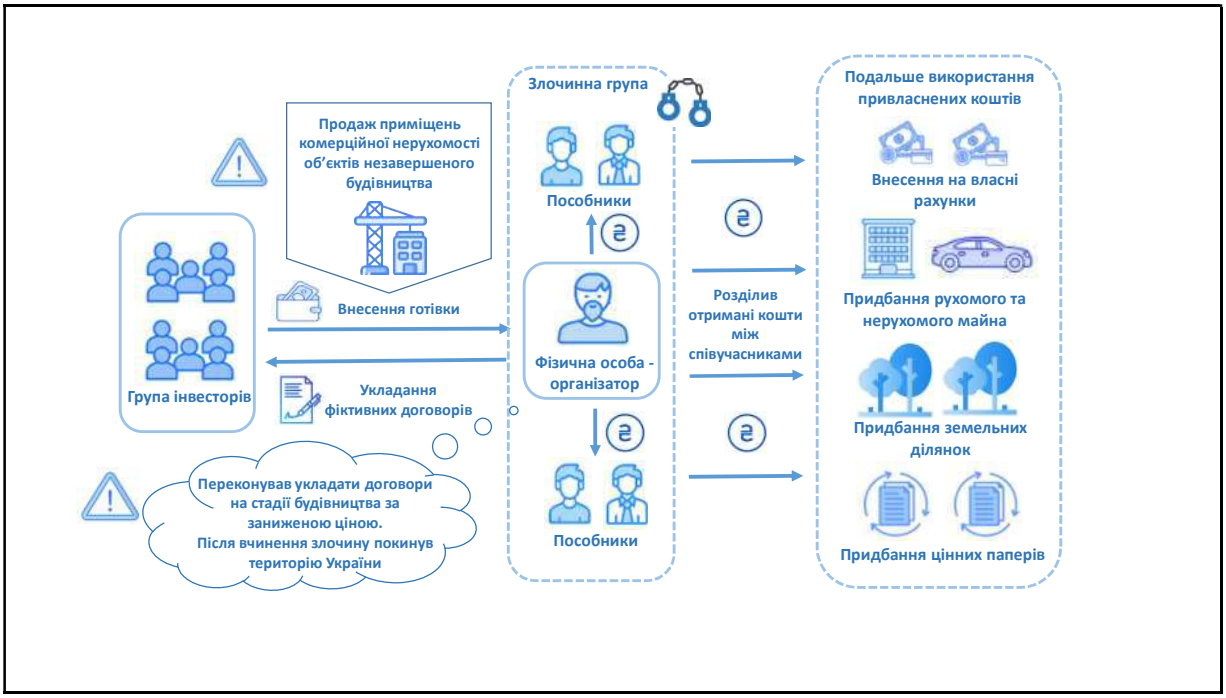
Правоохоронним органом встановлено, що **Фізичною особою** організовано злочинну схему із заволодіння коштами фізичних осіб шляхом продажу приміщень комерційної нерухомості, до будівництва якої вона не мала законного відношення. **Фізична особа** переконувала потенційних інвесторів, що придбання об'єктів на стадії будівництва відбудеться за значно заниженою вартістю, яка зросте після введення нерухомості в експлуатацію, та укладала фіктивні договори цивільно-правового характеру.

Ошукані інвестори розраховувалися з **Фізичною особою** готівковими коштами, які вона привласнювала та розподіляла між співучасниками злочинної групи.

Встановлено, що **Фізичною особою** та її пособниками до банківських установ внесено значні суми готівки, які суттєво перевищують їх офіційно задекларовані доходи. Частина коштів була внесена на власні банківські рахунки, інша частина – використана для придбання автомобілів, нерухомості, земельних ділянок, цінних паперів та для здійснення переказів між власними рахунками.

Відомо, що після вчинення злочину **Фізична особа** залишила територію України.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2025.4.7.4. Шахрайські дії під виглядом зборів коштів на потреби Збройних сил України

Держфінмоніторингом, з урахуванням інформації правоохоронного органу, виявлено схему незаконного заволодіння коштами фізичних осіб під виглядом збору коштів на потреби Збройних сил України.

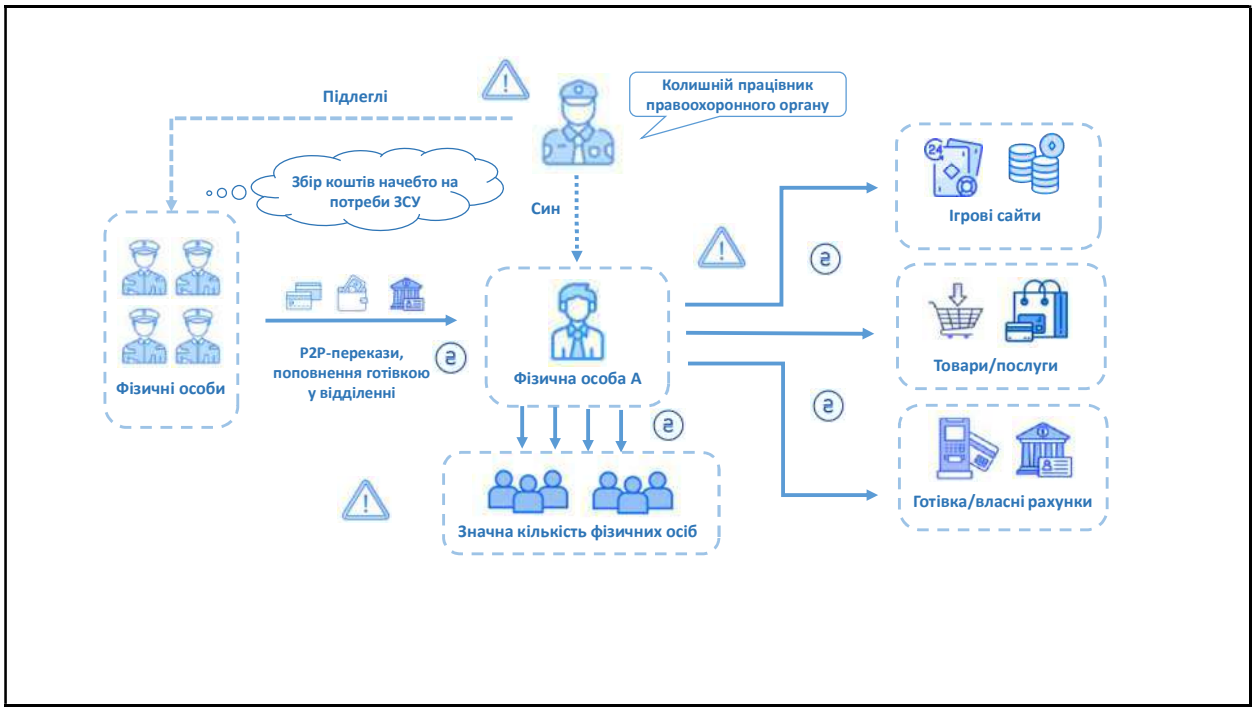
Встановлено, що колишній працівник правоохоронного органу з метою незаконного збагачення організував збір коштів від підпорядкованих працівників нібито на потреби одного з підрозділів ЗСУ. Кошти збиралися як у готівковій формі, так і шляхом зарахування на банківські рахунки його сина.

Виявлено, що на рахунки **Фізичної особи А**, яка є сином організатора шахрайської схеми, зараховувалися кошти від значної кількості фізичних осіб, у тому числі готівкою та P2P-переказами через банківські платіжні сервіси. Списання коштів здійснювалося переважно для власних потреб: оплата розваг на ігрових сайтах, оплата товарів/послуг, зняття готівки, перерахування коштів на користь значної кількості третіх осіб.

Жодного перерахування коштів, яке могло б бути пов'язане з потребами Збройних сил України, за рахунками не виявлено.

Таким чином, зазначена схема збору коштів була організована колишнім працівником правоохоронного органу шляхом зловживання службовим впливом виключно з метою власного незаконного збагачення.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2025.4.7.5. Шахрайське заволодіння коштами фізичних осіб шляхом обману чи зловживання довірою

Держфінмоніторингом, з урахуванням інформації суб'єкта первинного фінансового моніторингу, виявлено схему заволодіння коштами фізичних осіб на значні суми шляхом обману або зловживання довірою.

Встановлено, що **Фізичною особою А** за короткий період відкрито власні рахунки у великій кількості банківських установ. Через деякий час більшість цих рахунків були заблоковані банками через підозри у шахрайстві.

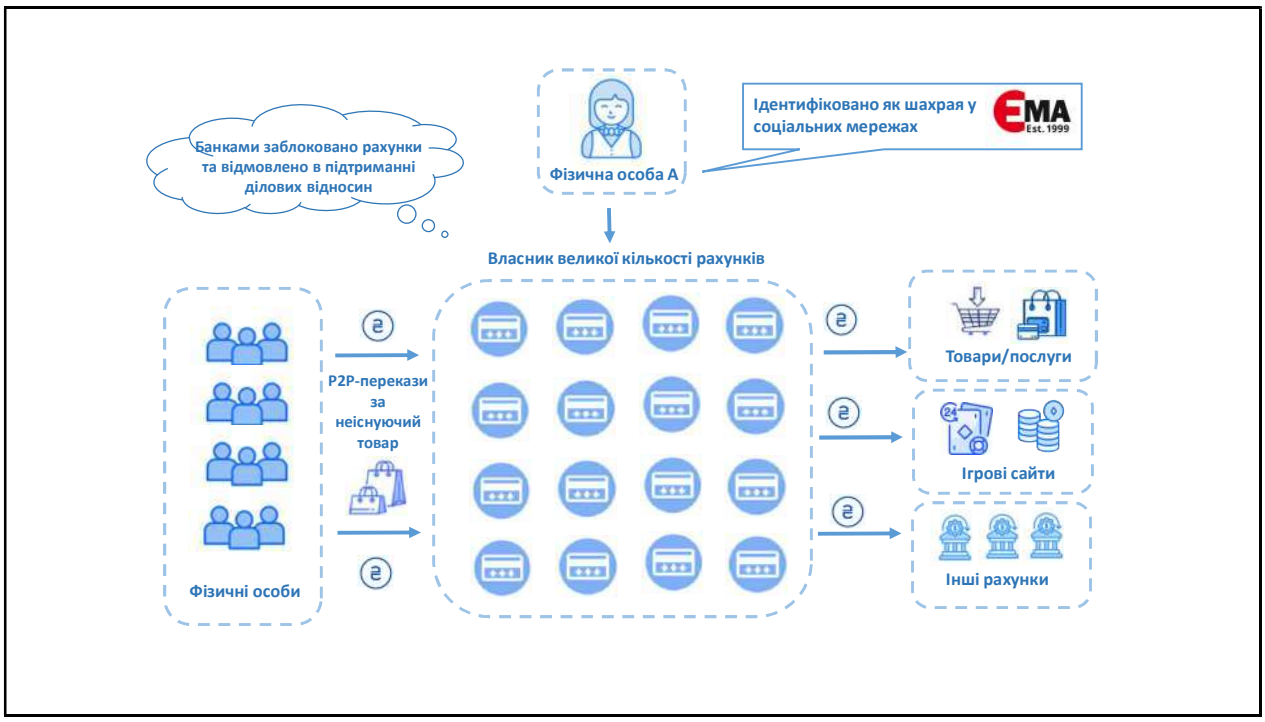
Загалом Держфінмоніторингом отримано 10 повідомлень про підозрілі фінансові операції (діяльність) **Фізичної особи А**, а ще 11 банківських установ відмовили у встановленні або підтриманні ділових відносин через визначення клієнта як такого, що має неприйнятно високий ризик.

За інформацією з форуму Асоціації ЄМА (об'єднання українських банків – членів платіжних систем), **Фізичну особу А** ідентифіковано як шахрая, який ошукує потенційних жертв через соціальні мережі, отримуючи передоплату за неіснуючий товар. Також відомо, що банківські установи обмінювалися між собою інформацією щодо підозр про шахрайську діяльність **Фізичної особи А**.

Встановлено, що на рахунки **Фізичної особи А** зараховувалися кошти у вигляді великої кількості P2P-переказів, при цьому мета платежу та відправники коштів не зазначалися. Надалі отримані кошти перераховувалися на оплату товарів/послуг, у вигляді P2P-переказів, на оплату участі в азартних іграх, а також знімалися готівкою.

Таким чином, є підстави вважати, що фінансові операції **Фізичної особи А** спрямовані на легалізацію злочинних доходів, отриманих внаслідок шахрайського заволодіння коштами великої кількості фізичних осіб.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2025.4.7.6. Шахрайські дії громадянина України з використанням рахунку, відкритого в іноземному банку

Держфінмоніторингом, з урахуванням інформації, отриманої від ПФР іноземної країни, виявлено шахрайську схему, організовану громадянином України з використанням рахунку, відкритого в іноземному банку.

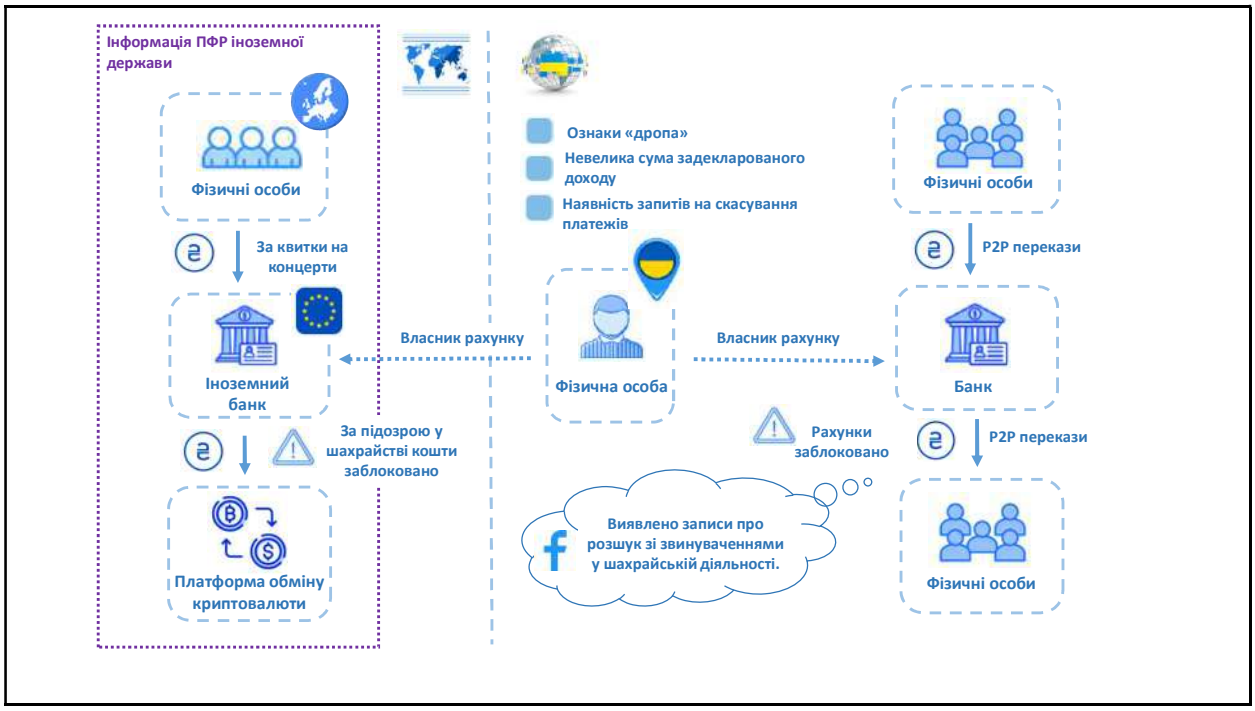
ПФР іноземної країни повідомлено про підозрілу діяльність за рахунком **Фізичної особи – громадянина України**, відкритим в іноземному банку. Невдовзі після відкриття рахунку **Фізична особа** почала отримувати численні грошові перекази на невеликі суми нібито за продаж квитків на різні концерти від відправників з різних країн. Після надходження коштів на рахунок вони переказувалися на криптовалютну біржу.

Відомо про надходження до іноземного банку запитів від іноземної платіжної установи щодо скасування здійснених платежів. **Фізична особа** не змогла надати банку жодних документів, що підтверджують законний характер операцій, у зв’язку з чим її рахунок було заблоковано за підозрою у шахрайстві.

Також встановлено, що в одній із соціальних мереж публікувалися оголошення про розшук **Фізичної особи** зі звинуваченнями у шахрайстві. З коментарів користувачів випливає, що **Фізична особа** вимагала передоплату за неіснуючі товари, після отримання коштів зникала та не відповідала у месенджерах.

Встановлено, що **Фізична особа** має також рахунок в українському банку, щодо якого наявна інформація про підозрілу діяльність. Банком відмовлено у підтриманні ділових відносин, а клієнту встановлено неприйнятно високий ризик через наявні ознаки «дропа». Характер переказів, здійснених з використанням електронних платіжних засобів, був транзитним та свідчив про їх використання з протиправною метою.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2025.4.7.7. Схема шахрайського заволодіння коштами іноземних громадян

Держфінмоніторингом, з урахуванням інформації, отриманої від ПФР іноземної держави та СПФМ, виявлено шахрайські дії, спрямовані на заволодіння коштами іноземних громадян.

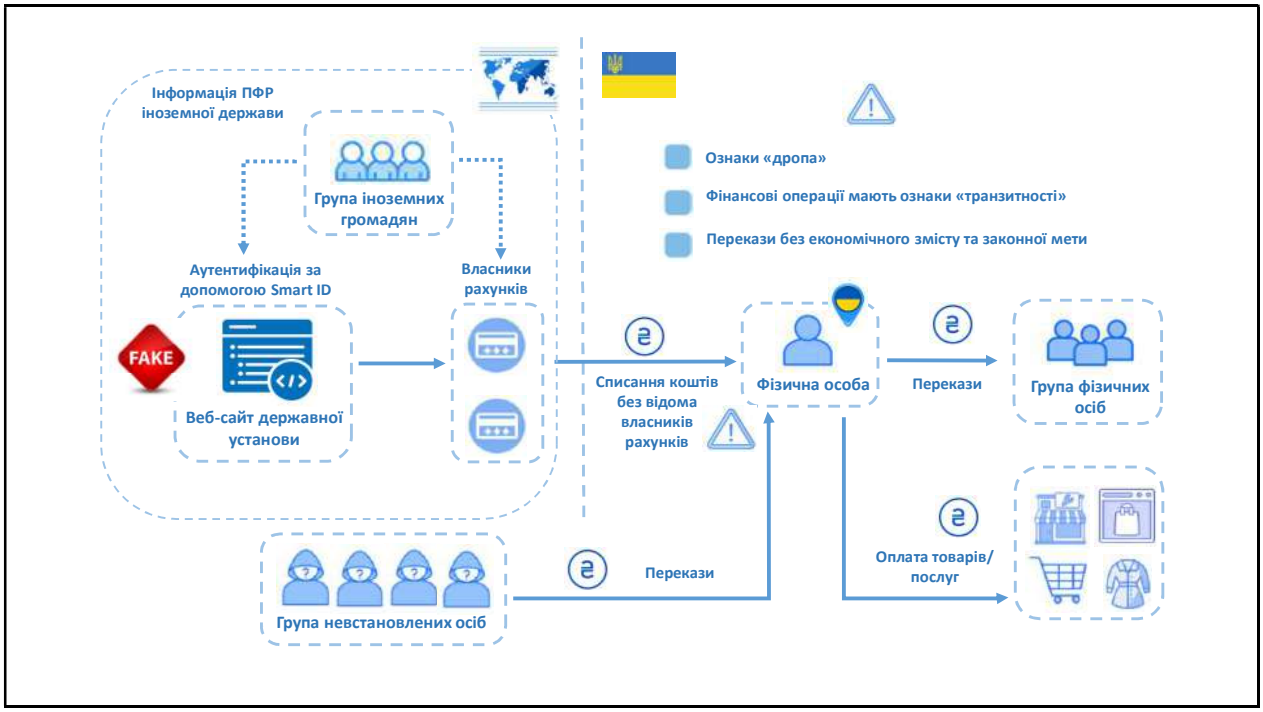
ПФР іноземної держави повідомлено про несанкціоноване списання коштів з рахунків громадян після проходження автентифікації за допомогою Smart ID на офіційному сайті державного органу цієї країни. Встановлено, що громадяни стали жертвами після входу на підроблений вебсайт державного органу, де вони розкрили особисті дані та дані банківських рахунків, після чого кошти були без їх відома незаконно списані на рахунок **Фізичної особи А** – громадянина України.

Щодо фінансових операцій **Фізичної особи А** СПФМ надано повідомлення про підозрілу діяльність, пов’язану з транзитними операціями без очевидного економічного змісту, а також з використанням коштів невідомого походження. Крім того, клієнт належить до соціально вразливих верств населення (студент), має вік 20 років.

Встановлено, що на рахунки **Фізичної особи А** зараховано значні суми від **Групи невстановлених осіб** у вигляді P2P-переказів, поповнення картки та інших форм зарахування. У подальшому отримані кошти **Фізична особа А** переважно перераховувала третім особам, що має ознаки транзитних операцій без економічного змісту та законної мети. Частина коштів використовувалася для оплати товарів та послуг для власних потреб.

Таким чином, є підстави вважати, що рахунки **Фізичної особи А** використовуються як «дропа» в організованій схемі онлайн-шахрайства.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2025.4.7.8. Схема шахрайського заволодіння коштами фізичних осіб з використанням «фішингу»

Держфінмоніторингом, з урахуванням інформації, отриманої від ПФР іноземної країни, виявлено шахрайську схему заволодіння коштами фізичних осіб із використанням механізму «фішингу».

ПФР іноземної країни надано інформацію про підозрілі транзакції, отримані **Громадянами України** через систему електронних грошей цієї держави. Ними одночасно було отримано кошти на різні суми від одного і того ж **Іноземного громадянина**, а також від інших фізичних осіб із різних країн Європи. Отримані кошти здебільшого були перераховані на криптовалютну біржу, що має негативну репутацію серед фінансових контрагентів.

Адміністратором системи електронних грошей отримано повідомлення від **Іноземного громадянина**, у якому зазначалося, що жертва отримала на свою електронну поштову скриньку фішингові листи, нібито надіслані обслуговуючим банком, з інструкціями щодо оновлення персональних даних на платформі банку. Після переходу за посиланням у листі та введення особистих даних і паролів треті особи отримали доступ до банківського рахунку жертви та здійснили незаконні перекази.

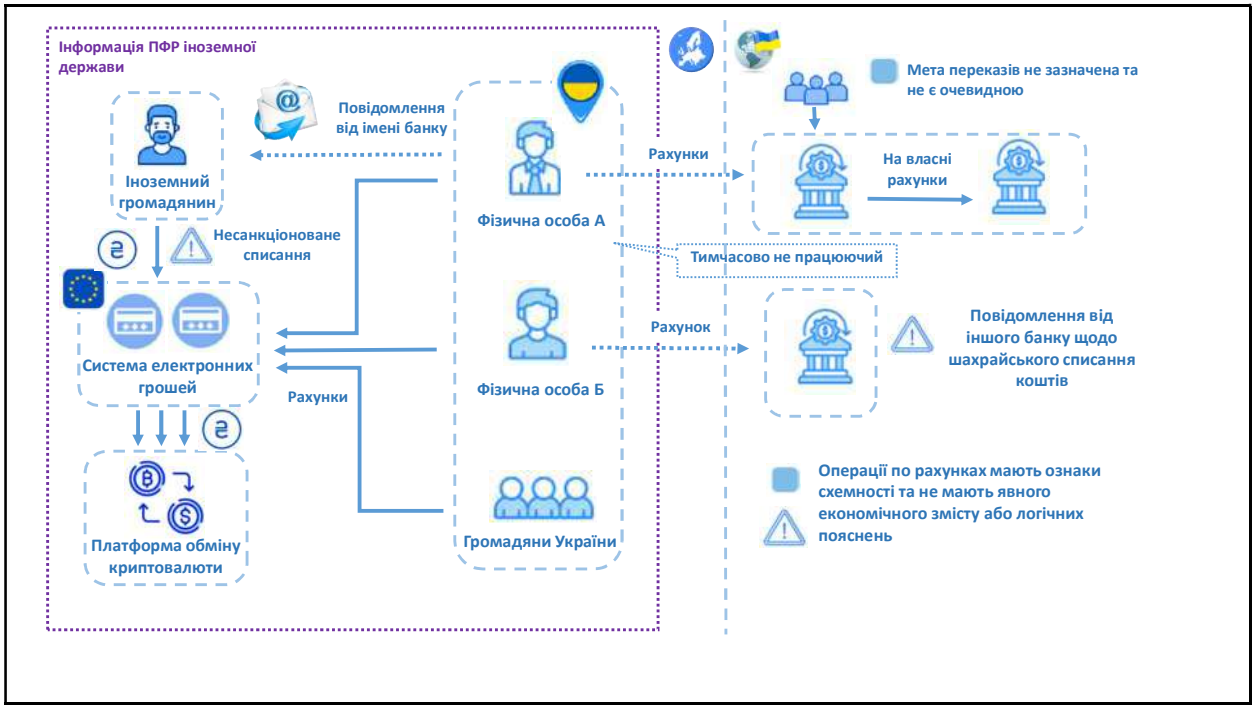
Встановлено, що стосовно окремих **Громадян України** наявні повідомлення про підозрілу діяльність за їх рахунками, яка має ознаки шахрайства, схемності та не має очевидного економічного змісту або логічного пояснення.

Так, за рахунком **Фізичної особи А** (соціальний статус – тимчасово не працює) виявлено зарахування значних сум від трьох фізичних осіб, а також внесення готівки. Надалі отримані кошти перераховувалися на власні карткові рахунки. Мета переказів не зазначалася та не є очевидною.

Стосовно **Фізичної особи Б** обслуговуючий банк отримав повідомлення від іншої банківської установи щодо шахрайського списання коштів з рахунку їх клієнта на рахунок **Фізичної особи Б**, із проханням заблокувати картку.

Враховуючи викладене, є підстави вважати, що рахунки **Громадян України**, відкриті в банківських установах України та іноземної держави, використовуються для заволодіння коштами у шахрайський спосіб із подальшою легалізацією, у тому числі через криптовалютні платформи.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2025.4.7.9. Кібератака на Укрзалізницю

У 2025 році зафіксовано інцидент кібератаки на систему продажу квитків, яка мала безпосередній вплив на надання послуг населенню. Атака була високотехнологічною та заздалегідь підготовленою – зловмисники використали спеціально розроблене шкідливе програмне забезпечення, адаптоване до специфіки інфраструктури цільового об'єкта.

За результатами технічного аналізу, фахівці CERT-UA ідентифікували використання тактик, технік та процедур, характерних для російських спецслужб. Це дозволяє припустити, що атака була скоєна з підтримкою на державному рівні й мала ознаки складної кампанії, спрямованої на дестабілізацію критичної цифрової інфраструктури.

Цей інцидент є прикладом застосування інструментів кібервійни в межах гібридної агресії проти України, де кіберпростір використовується для ураження соціально чутливих та стратегічно важливих об'єктів.

Приклад 2025.4.7.10. Кібератаки проти Нотаріату України

Починаючи з другої половини січня 2025 року Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA фіксується поновлення активності організованого злочинного угруповання UAC-0173 – так званих «чорних нотаріусів», які на замовлення та за грошову винагороду здійснюють кібератаки з метою отримання прихованого віддаленого доступу до комп'ютерів нотаріусів і подальшого внесення несанкціонованих змін до державних реєстрів.

РОЗДІЛ 4.8. ВІДМИВАННЯ ЗЛОЧИННИХ ДОХОДІВ ІЗ ВИКОРИСТАННЯМ ВІРТУАЛЬНИХ АКТИВІВ

З 2022 року суттєво зросла кількість злочинів із використанням віртуальних активів, які дедалі частіше застосовуються для обходу санкцій, відмивання коштів та фінансування незаконної діяльності через анонімні гаманці, децентралізовані біржі та псевдоінвестиційні платформи.

В частині фінансової цілісності, яка в першу чергу пов'язана з протидією ВК/ФТ, основним міжнародним стандартом є Рекомендація 15 FATF, яка визначає вимоги до віртуальних активів (VAs) та постачальників послуг, пов'язаних з віртуальними активами (VASPs). Її виконання включає оцінку ризиків ВК/ФТ, обов'язкову реєстрацію та ліцензування VASP, впровадження KYC, моніторинг транзакцій, дотримання TravelRule, а також обов'язок виявлення та повідомлення про підозрілі операції.

До найбільш поширених злочинів належать:

- легалізація доходів через віртуальні активи, що забезпечує швидке й анонімне переміщення коштів;
- кіберзлочини як інструмент відмивання, коли викрадені кошти конвертуються в віртуальну валюту для подальшої легалізації;

– зв'язок між корупцією та військовими витратами, що сприяє розкраданню коштів, призначених для оборонного сектору.

За даними Національної поліції України, злочини з використанням віртуальних активів сформували окрему сферу. Криптовалюти та децентралізовані фінансові платформи активно застосовуються для прихованого переміщення коштів, які згодом виводяться у фіатні валюти, що ускладнює їхнє відстеження та створює ризики легалізації.

За даними Державної податкової служби України, поширилася тенденція використання криптовалют для маскування походження коштів, отриманих унаслідок майнових правопорушень, а також для приховування осіб, причетних до їх скоєння.

Фінансовий сектор спостерігає активну участь підставних осіб «дропів» у проведенні транзакцій, пов'язаних із віртуальними активами.

Таким чином, використання віртуальних активів у схемах ВК/ФТ стало більш складним і технологічним.

Ключові тенденції:

1. Зростання використання стейблкоїнів.

Стейблкоїни (наприклад, USDT, USDC) дедалі частіше застосовуються для швидких, стабільних і менш помітних транзакцій. Вони стали популярними у схемах фінансування терористичних груп та обходу санкцій.

2. Активізація DeFi-платформ.

Децентралізовані фінансові сервіси (DeFi) використовуються для обміну, кредитування, зберігання активів без участі централізованих посередників. Це ускладнює ідентифікацію учасників та моніторинг транзакцій.

3. Використання нерозміщених гаманців (unhostedwallets).

Злочинці все частіше використовують гаманці без прив'язки до бірж або VASP, що дозволяє уникати контролю. Такі гаманці складно відстежити, особливо при транзакціях між юрисдикціями.

4. P2P-обмін та міксери.

Прямі перекази між користувачами без участі бірж – популярний спосіб приховати джерело коштів. Міксери (mixingservices) використовуються для розпорошення сліду транзакцій, що ускладнює фінансове розслідування.

Стратегії російської федерації щодо використання криптоінструментів для обходу міжнародних санкцій

Віртуальні активи стали одним із ключових інструментів, які російська федерація використовує для обходу фінансових санкцій та здійснення розрахунків поза традиційною системою міжнародних платежів. Зокрема, peer-to-peer операцій (P2P-перекази), стейблкоїнів (stablecoins), міксерів транзакцій (mixers), крос-чейн бриджів (cross-chainbridges) та децентралізованих фінансових сервісів (DeFi).

У відповідь міжнародна спільнота посилила санкційний тиск на криптоінфраструктуру, впровадили санкціонування адрес, жорсткіші KYC-вимоги та блокчейн-аналітику, що підвищило ефективність протидії.

Розвиток інструментів протидії ВК у сфері віртуальних активів. Посиленню виявлення незаконних операцій з віртуальними активами сприяло активне впровадження блокчейн-аналітики та жорсткіші KYC/AML-вимоги на криптобіржах. Це дало змогу ефективніше ідентифікувати підозрілі транзакції, розкривати складні схеми, заморожувати гаманці та блокувати ризикові сервіси.

Сучасні аналітичні платформи дозволяють у режимі, наближеному до реального часу, відстежувати потоки коштів, визначати ризикові адреси, а також виявляти міксери, тумблери, P2P-майданчики та інші потенційно небезпечні інструменти.

Використання ВА в схемах ВК/ФТ.

	Перевагами використання віртуальних активів залишаються висока анонімність, швидкість переказів у межах країни та за кордон, децентралізований характер платежів та обмежене регулювання в окремих юрисдикція. Згідно зі звітом Chainalysis про криптозлочинність, ці ж фактори роблять їх привабливим інструментом для незаконних фінансових операцій.

Узагальнені типові приклади відмивання злочинних доходів від із використанням віртуальних активів.

Приклад 2025.4.8.1. Отримання коштів невідомого походження від продажу криптовалюти через IBAN із використанням сервісу cryptofiat.finance[36]

Банком виявлено схему, у межах якої на рахунок клієнта надходили кошти від продажу криптовалюти, що переказувалися неповнолітніми особами віком 14 - 16 років. Усі вони мали відкриті рахунки в одному з українських банків.

Кошти надходили на рахунок клієнта Банку дробленими сумами через перекази за реквізитами IBAN. За інформацією клієнта, джерелом надходжень був криптообмінний сервіс cryptofiat.finance, який спеціалізується на конвертації віртуальних активів у фіатні валюти.

Країною походження значної частини коштів була Туреччина, зокрема покупцем віртуальних активів клієнта виступав резидент Туреччини.

Банком встановлено такі індикатори підозрілості фінансових операцій:

- невідоме або непідтверджене джерело походження коштів контрагентів клієнта, у тому числі неповнолітніх осіб;
- проведення ризикових операцій з криптоактивами через звичайні поточні рахунки, не призначені для такої діяльності;
- ускладнена схема конвертації криптовалюти у гривню з використанням стороннього сервісу обміну, що маскує реальних учасників операцій.

З огляду на виявлені ознаки, операції були кваліфіковані Банком як підозрілі.

[36] За даними НБУ

Приклад 2025.4.8.2. Фінансові операції групи фізичних осіб з коштами, отриманими від кібератак

Держфінмоніторингом, з урахуванням інформації, отриманої від суб'єктів первинного фінансового моніторингу та правоохоронного органу, виявлено схему, пов'язану зі здійсненням фінансових операцій **Групою фізичних осіб** з коштами, що попередньо були отримані внаслідок кібератак на **Компанії-нерезиденти**.

Правоохоронним органом встановлено, що **Група компаній-нерезидентів** зазнала кібератаки із використанням шкідливого програмного забезпечення, що призвело до блокування частини даних та ускладнення роботи компаній. Для відновлення доступу зловмисники висунули вимогу сплатити викуп у віртуальних активах. Кошти у формі криптовалюти були перераховані на віртуальний гаманець, наданий злочинцями. Відомо, що серед учасників цієї схеми є громадянин України – **Фізична особа А**.

Виявлено, що фінансові операції **Фізичної особи А**, здійснені на значні суми, не відповідають її офіційно задекларованим доходам. На рахунки **Фізичної особи А** надходили кошти:

- перекази від **Групи фізичних осіб Б**;
- перекази від юридичних осіб у вигляді «повернення фінансової допомоги» (за відсутності будь-яких операцій з надання такої допомоги);
- поповнення власних рахунків безготівковим та готівковим шляхом;
- інші транзакції невідомої економічної природи.

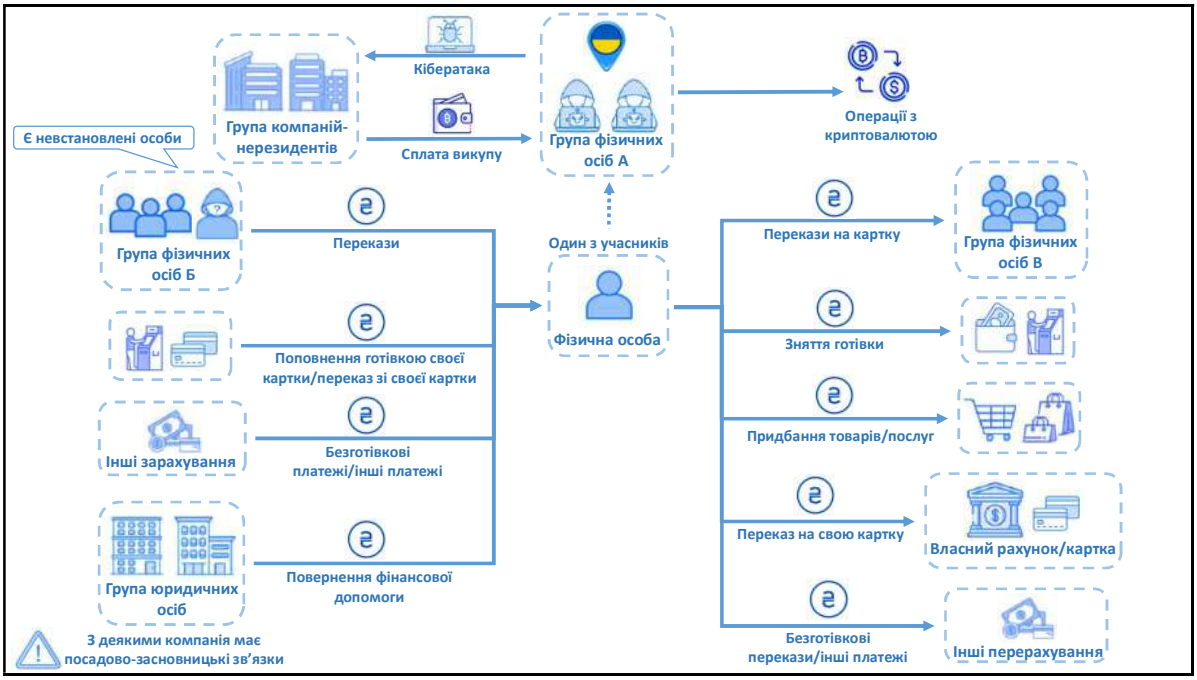
Серед юридичних осіб, що здійснювали перерахування, є компанії, пов'язані з **Фізичною особою А** посадово-засновницькими зв'язками.

Надалі **Фізична особа А** перераховувала отримані кошти іншій **Групі фізичних осіб В**, здійснювала перекази на власні рахунки, знімала готівку, витрачала кошти на придбання товарів і послуг та проводила інші транзакції.

Додатково встановлено, що, на ім'я **Фізичної особи А** зареєстровано криптовалютний гаманець, який використовується як «депозитна адреса» для отримання криптовалюти з інших платформ чи гаманців на власний обліковий запис.

Враховуючи зазначені факти, є підстави вважати, що діяльність **Фізичної особи А** спрямована на легалізацію (відмивання) доходів, одержаних злочинним шляхом унаслідок участі у шахрайських кібератаках.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2025.4.8.3. Шахрайське заволодіння коштами фізичних осіб шляхом організації неіснуючих проєктів із «криптотрейдингу»

Держфінмоніторингом, з урахуванням інформації, отриманої від суб'єктів первинного фінансового моніторингу, ПФР іноземної країни та правоохоронного органу, виявлено схему, пов'язану з шахрайським заволодінням коштів громадян України та іноземців шляхом інвестування у неіснуючі проєкти з «криптотрейдингу», що фактично є елементом фінансової піраміди.

Встановлено, що за рахунком **Фізичної особи А** здійснено фінансові операції на суми, які не відповідають її офіційно задекларованим доходам. На рахунки **Фізичної особи А** надходили кошти від великої кількості фізичних осіб, а також здійснювалися поповнення рахунку готівкою та безготівковим шляхом. Крім того, на рахунок надходила заробітна плата. Надалі **Фізична особа А** перераховувала кошти іншій групі фізичних осіб, на інший власний рахунок, а також здійснювала оплату товарів і послуг на користь юридичних осіб. Операції мали «транзитний» характер.

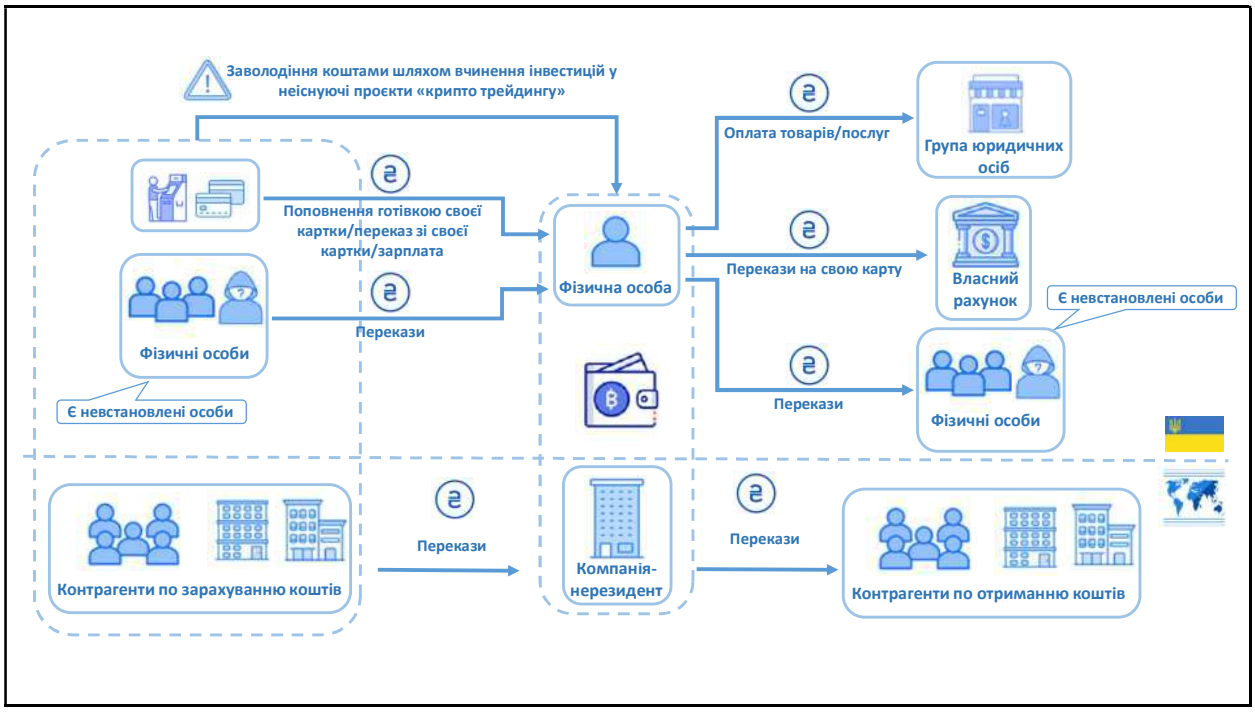
Правоохоронним органом встановлено, що **Фізична особа А** є одним з організаторів фінансової піраміди у сфері криптовалюти, яка позиціонувалася як «надприбуткові інвестиційні проєкти». Організаторами створено низку **Компаній-нерезидентів**, розроблено відповідні інвестиційні продукти та проведено ряд маркетингових заходів (презентацій, прес-конференцій) для формування хибної громадської думки щодо легальності та прибутковості цих проєктів.

Насправді діяльність таких проєктів полягала виключно у залученні коштів громадян України та іноземців без наміру здійснювати реальні інвестиції та виплачувати обіцяний дохід. Встановлено, що більшість організаторів та учасників схеми володіють значними обсягами рухомого та нерухомого майна, вартість якого суттєво перевищує їх офіційні доходи.

Однією **з компаній-нерезидентів**, через яку здійснювали залучення коштів громадян для подальшого їх виведення у тіньовий (криптовалютний) обіг, є **Компанія А**, стосовно якої ПФР іноземної країни надала інформацію про підозрілу транзитну діяльність, що має ознаки відмивання коштів.

За результатами аналізу криптогаманців, які могли використовуватися у протиправній діяльності, встановлено «транзитний характер» операцій: перекази однаковими сумами, здійснені за короткий проміжок часу, із нульовими залишками після їх проведення. Це свідчить про намір приховати джерело походження активів, подальший рух коштів, а також особи їх відправників і отримувачів.

Правоохоронним органом здійснюється досудове розслідування.



РОЗДІЛ 4.9. ВІДМИВАННЯ ЗЛОЧИННИХ ДОХОДІВ ЧЕРЕЗ ГРАЛЬНИЙ БІЗНЕС

Гральний бізнес залишається вразливим сектором до використання з метою легалізації злочинних доходів.

Нелегальні онлайн-казино, «live-студії», а також підставні гральні майданчики дедалі частіше стають частиною складних фінансових схем, де використовуються фіктивні компанії, транзитні рахунки, підставні особи («дропи») та криптовалюти.

Як саме використовуються підставні особи («дропи»):

- **реєстрація акаунтів** на гральних платформах на ім'я підставних осіб («дропів») часто без їх реальної участі або з мінімальним залученням (наприклад, за гроші, паспортні дані або копії документів).
- **внесення коштів** у вигляді ставок через криптовалюту або банківські картки, що прив'язані до «дропів».
- **виведення коштів** як «виграшу» або «прибутку», що нібито отриманий легально.
- **подальше переказування грошей -** знову ж таки через низку транзитних рахунків, часто за допомогою обмінників, P2P - платформ або офшорних структур.

Підставна особа («дроп») у схемі відмивання коштів – це буфер між реальною особою/організатором та грошовим слідом. Багато «дропів» – це соціально вразливі групи: студенти, пенсіонери, безробітні.

В Україні зафіксовано низку масштабних розслідувань, у яких з'ясувалося, що через подібні платформи щороку обертаються мільярди гривень із сумнівним походженням.

Одним із ключових трендів стало поєднання грального бізнесу з криптовалютними інструментами для ускладнення відстеження грошових потоків. Гравці або підставні особи («дропи») заводять крипту на платформу, роблять мінімальні ставки, а потім виводять кошти як «виграші», що створює видимість законного доходу. Цей механізм активно використовується в схемах, де важливо «очистити» походження грошей перед виведенням у реальний бізнес чи купівлею активів.

Схеми стають дедалі складнішими, і без ефективного контролю над цифровими активами та онлайн–гемблінгом існує ризик, що гральний сектор перетвориться на основний канал відмивання «брудних» коштів у майбутньому.

Узагальнені типові приклади відмивання злочинних доходів через гральний бізнес наведено нижче.

Приклад 2025.4.9.1. Відмивання доходів через онлайн-ресурси з реалізації ігрових предметів[37]

Виявлено схему відмивання доходів із використанням онлайн-ресурсів, що спеціалізуються на продажі ігрових предметів (відеоігор).

Встановлено, що **Фізичні особи** здійснювали перекази коштів на сотні мільйонів гривень з використанням платіжних карток, емітованих іноземними банками, у тому числі банками, зареєстрованими в рф, на користь **Підприємства А**, яке має ознаки фіктивності. Перекази здійснювалися нібито як оплата вартості ігрових предметів (відеоігор).

Платежі ініціювалися на сайті небанківської фінансової установи за відсутності належних заходів моніторингу ділових відносин та фінансових операцій клієнтів. Прийняті платежі були перераховані цією установою на банківський рахунок **Підприємства А**, як оплата за ігрові предмети.

Привертає увагу, що: відсутні документи щодо реалізації/купівлі/продажу ігрових предметів; на задекларованих онлайн-ресурсах немає будь-якої інформації про **Підприємство А**, що вказує на штучність торгівельної діяльності.

Надалі отримані кошти (сотні мільйонів гривень) Підприємство А переказувало в межах договору з Банком з метою здійснення виплат на електронні платіжні засоби фізичних осіб, які могли надалі:

- знімати ці кошти у готівковій формі;
- використовувати їх у будь-який інший спосіб.

Приклад 2025.4.9.2. Виведення коштів із онлайн-казино на фізичну особу з їх подальшим обготівковуванням[38]

Виявлено схему відмивання доходів із використанням онлайн-казино, з подальшим обготівкуванням виграшу.

Компанія А, яка є онлайн-казино в Україні та має відповідну ліцензію, здійснює неодноразову виплату виграшу фізичній особі. Виплати починаються із **незначної суми та у наступному зростають**. Загальна сума виграшу сягає мільйони гривень. Виплата виграшу здійснюється в безготівковій формі шляхом перерахування коштів на рахунки фізичної особи в банках. Для підтвердження виграшу Компанія А надає фізичній особі довідки про факт виграшу.

В подальшому фізична особа **знімає кошти готівкою** та перераховує на свої рахунки в інших банках (теж з метою зняття готівки). Як правило, фізична особа має рахунки у 5-6 банках.

При цьому, фізичні особи, через яких виводяться та обготівковуються кошти, як правило, не мають доходів або мають незначні доходи, і водночас **не мають негативних факторів** ділової репутації, таких як борги або судові справи.

[37] За даними НБУ
[38] За даними НБУ

Таким чином, схема забезпечує легалізацію коштів шляхом обрання осіб без негативної ділової історії та **використання великої кількості банківських рахунків для обготівковування** значних сум.

Приклад 2025.4.9.3. Схема маскування діяльності онлайн-казино з використанням електронного терміналу

Держфінмоніторингом, з урахуванням інформації суб'єктів первинного фінансового моніторингу, виявлено **підозрілі фінансові операції,** проведені по рахунку компанії з використанням електронного термінала, встановленого юридичною особою згідно з договором еквайрингу.

Банком зафіксовано **нетипову активність** після запуску електронного термінала на рахунку клієнта – **Компанії А**, що не відповідає задекларованому основному виду діяльності (роздрібна торгівля, що здійснюється фірмами поштового замовлення або через мережу Інтернет).

Встановлено, що **Компанією А** створено сайт для приймання платежів від платників. Проте цей сайт створено виключно для імітації діяльності:

- відсутність будь-якої активності й реклами в мережі Інтернет;
- сторінка оплати генерується не з вказаного сайту, а з іншого ресурсу;
- відсутність обов'язкового поля «вид товару»;
- контактний телефон, зазначений як «підтримка 24/7», вимкнений;
- електронна адреса, що не існує.

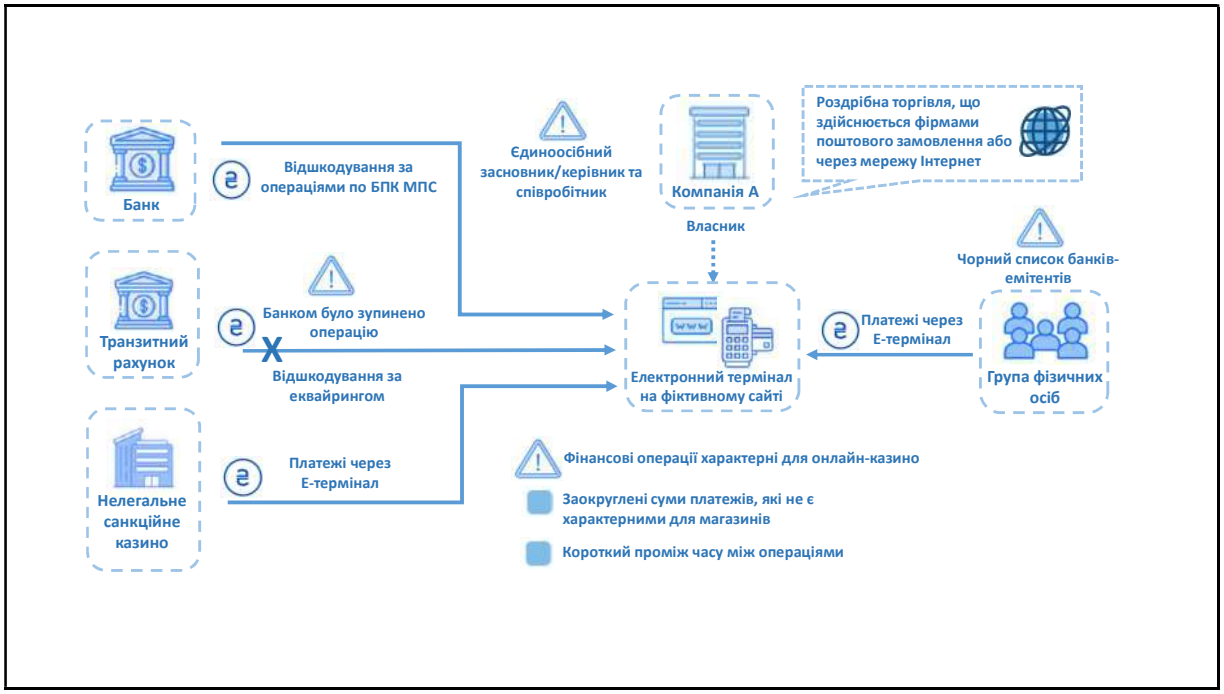
Це свідчить, що сайт не має ознак реального інтернет-магазину та може використовуватися виключно для проведення **платежів, характерних для незаконної азартної діяльності** (заокруглені суми, короткі інтервали між транзакціями).

Додатково встановлено, що **Група фізичних осіб**, яка здійснювала платежі через електронний термінал, перебуває у «чорному списку» банків-емітентів через підозри їхньої причетності до протиправних схем, зокрема **незаконної організації або проведення азартних ігор та лотерей**.

Окремо встановлено, що частина коштів на рахунок **Компанії А** надходила безпосередньо через електронний термінал, який був **розміщений на сайті нелегального санкційного онлайн-казино**.

З огляду на наведені обставини існують обґрунтовані підозри, що створення **Компанії А** та здійснені нею фінансові операції мають на меті **забезпечення діяльності з незаконної організації чи проведення азартних ігор та лотерей**, у тому числі через **маскування під інтернет-магазин**.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2025.4.9.4. Легалізація коштів, отриманих від організації та проведення азартних ігор/казино у мережі інтернет

Держфінмоніторингом, з урахуванням інформації, отриманої від суб'єктів первинного фінансового моніторингу та правоохоронного органу, виявлено схему, спрямовану на отримання прихованого прибутку від організації та проведення азартних ігор/онлайн-казино, із використанням механізмів зменшення бази оподаткування, обготівковування та виведення коштів за кордон.

Встановлено, що на рахунки **Групи юридичних осіб А**, основна діяльність яких пов'язана з організуванням азартних ігор, надходила частина коштів від **Фінансових компаній** та **Групи юридичних осіб Б**, діяльність яких також пов'язана зі сферою грального бізнесу.

Платежі здійснювалися під виглядом:

- фінансової допомоги/позик;
- фінансових послуг;
- розміщення вкладів/депозитів;
- інших ризикових фінансових інструментів;
- переведення безготівкових коштів у готівку;
- формування податкового кредиту без фактичного постачання товару.

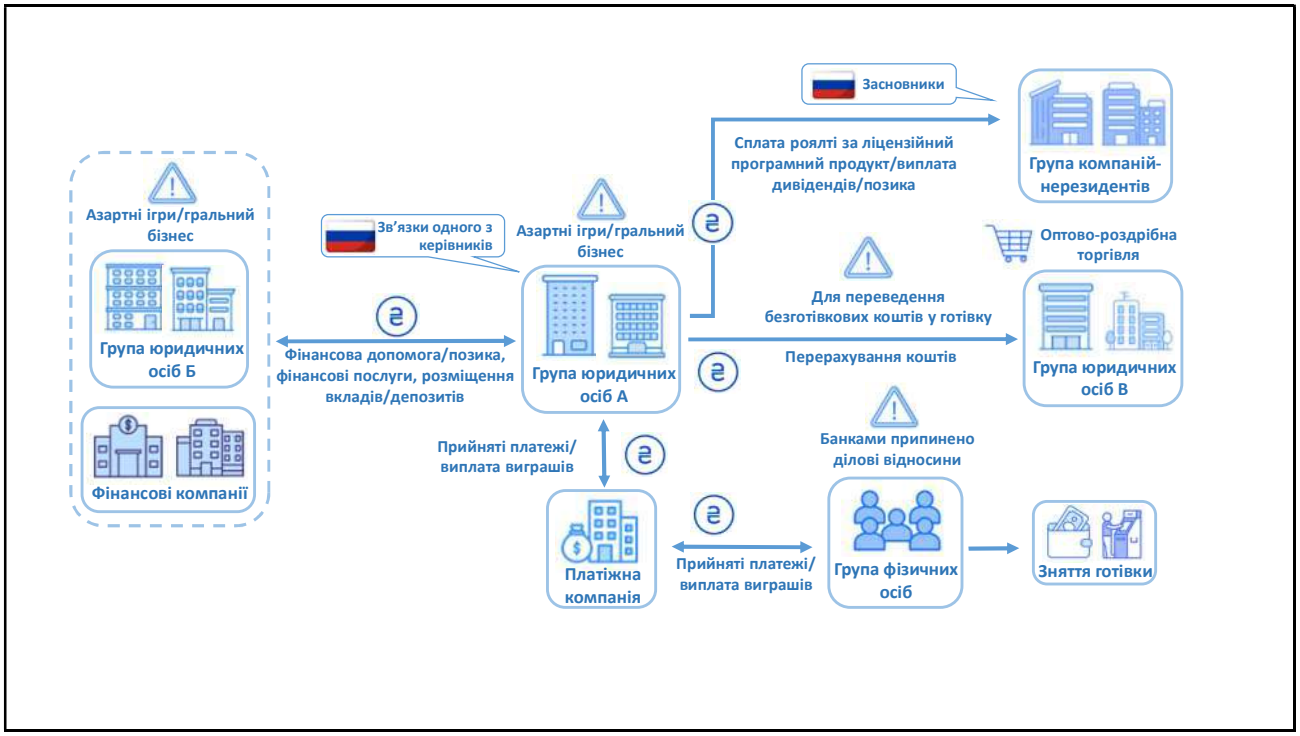
Також встановлено перекази коштів **Групою юридичних осіб А** на користь **Групи компаній-нерезидентів**, до складу засновників яких входять **громадяни росії,** під виглядом:

- сплати роялті за «ліцензійний програмний продукт»;
- виплати дивідендів;
- надання фінансової допомоги/позики тощо.

Додатково виявлено **бізнес-зв'язки** одного з керівників **Групи юридичних осіб А** з громадянином росії, що посилює ризики причетності до іноземних організованих структур грального бізнесу.

У результаті встановлено, що учасники схеми забезпечують функціонування незаконного онлайн-казино на території України, а отриманий прибуток виводиться на користь фактичних бенефіціарних власників у росії та надалі оприбутковується до бюджету держави-агресора, що становить загрозу економічній та національній безпеці України.

Правоохоронним органом здійснюється досудове розслідування.



РОЗДІЛ 4.10. ВІДМИВАННЯ ДОХОДІВ ВІД ТОРГІВЛІ ЗБРОЄЮ

У 2022-2025 роках в Україні формується тренд зростання ризиків, пов'язаних з незаконним обігом зброї та подальшим відмиванням доходів від цієї діяльності.

Фіксується збільшення кількості виявлених правопорушень, вилученої стрілецької зброї, боєприпасів і вибухових речовин, що прямо пов'язується з умовами повномасштабної війни, ротацією військових підрозділів та активним переміщенням озброєння.

Узагальнені типові приклади відмивання злочинних доходів від торгівлі зброєю наведено нижче.

Приклад 2025.4.10.1. Транскордонне відмивання незаконних доходів від продажу зброї та акцій оборонної компанії (Франція - Україна - Монако)[39]

Триваюче розслідування у трьох країнах призвело до арешту українського підприємця, підозрюваного у відмиванні незаконних коштів через нерухомість у Франції та Монако. Французька, українська та монакська влади співпрацюють над викриттям масштабної схеми відмивання грошей, пов'язаної з прибутками від незаконного продажу зброї та акцій оборонної компанії.

Підозрюваний є сином відомого підприємця в Україні, який володів оборонною компанією. Після російського вторгнення прибутки почали знижуватися, а власників підозрюють у незаконному продажу свого контрольного пакета акцій представникам іноземної держави.

Щоб приховати незаконний прибуток від продажу, син власника придбав нерухомість у кількох країнах, зокрема у Франції та Монако. Вважається, що згодом він відмив сотні мільйонів євро прибутку.

Лише у Франції його підозрюють у відмиванні понад 57 мільйонів євро. Він також відмивав прибутки від незаконного продажу зброї своїм батьком, власником оборонної компанії. Невдовзі після початку розслідування щодо відмивання грошей французька влада заморозила активи підозрюваних на суму 57 мільйонів євро.

Розслідування продовжувалися в рамках спільної слідчої групи, створеної при Агентстві Європейського Союзу з питань співробітництва у сфері кримінального правосуддя, що сприяє судовій співпраці між трьома країнами.

[39] https://www.eurojust.europa.eu/news/international-operation-uncovers-large-scale-scheme-laundering-hundreds-millions-euros

Завдяки співпраці правоохоронних органів сина було заарештовано в Монако. Під час операції в Монако було виявлено кілька цінних для розслідування документів. Власник оборонної компанії вже перебуває під судом в Україні за злочини проти національної безпеки, а тепер його також підозрюють у відмиванні грошей.

Приклад 2025.4.10.2. Незаконний збут вогнепальної зброї та боєприпасів організованою групою на території України[40]

Національна поліція спільно зі Службою безпеки України викрила групу торгівців зброєю, які незаконно продавали зброю та вибухівку криміналітету.

Угруповання діяло на території двох областей, однак зловмисники намагалися налагодити збут вогнепальної зброї та боєприпасів на території всієї України. Поліцейські оголосили фігурантам про підозри, збройний арсенал вилучено.

Ініціатор злочинної групи залучив трьох знайомих, які здійснювали пошук та доставку зброї. Оперативники кримінальної поліції отримали інформацію, що вказані особи підшукують шляхи збуту зброї на території України та запобігли потраплянню чотирьох збройових арсеналів до рук терористів чи криміналітету.

Правоохоронці провели 10 обшуків у домівках, гаражах та автомобілях фігурантів, під час яких вилучили значний арсенал: артилерійський снаряд, 13 пістолетів, 5 автоматів, гвинтівку, підствольні гранатомети з пострілами, 24 гранати із запалами, близько 3 000 набоїв та обладнання для виготовлення патронів. Найдорожчий набір коштував 260 000 гривень, загальна вартість - понад 1 млн гривень.

Слідчі національної поліції зібрали достатньо доказів та оголосили підозри у вчиненні злочину, передбаченого ч. 1 ст. 263 КК України (незаконне поводження з вогнепальною зброєю, бойовими припасами або вибуховими речовинами). Санкція статті передбачає до 7 років позбавлення волі.

[40] https://npu.gov.ua/news/natspolitsiia-spilno-z-sbu-vykryla-hrupu-torhivtsiv-zbroieiu-iaki-nezakonno-prodavaly-zbroiu-ta-vybukhivku-kryminalitetu?utm_source=chatgpt.com

РОЗДІЛ 4.11. ВІДМИВАННЯ ДОХОДІВ ВІД ТОРГІВЛІ ЛЮДЬМИ

У 2022 - 2025 роках торгівля людьми набула нових форм та інтенсивності, поєднуючи традиційні схеми експлуатації з цифровими інструментами вербування та фінансових розрахунків. Масштабне переміщення населення, економічна вразливість, онлайн-вербування та зростання попиту на трудову й сексуальну експлуатацію створили умови для розширення кримінальних мереж.

Злочинці дедалі частіше використовують соціальні мережі, месенджери та фіктивні платформи працевлаштування для залучення жертв, а отримані доходи маскують через підставних осіб («дропів»), електронні гаманці, криптовалютні перекази, транзитні рахунки, фіктивні ФОПи та мікроплатежі.

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

Приклад 2025.4.11.1. Легалізація незаконних доходів, отриманих від онлайн-трансляцій матеріалів порнографічного характеру

Держфінмоніторингом, з урахуванням інформації, отриманої від суб'єктів первинного фінансового моніторингу та правоохоронного органу, виявлено **підозрілі фінансові операції на рахунках фізичних осіб**, які можуть бути причетними до **створення та розповсюдження матеріалів порнографічного характеру**.

Правоохоронним органом повідомлено, що **двома фізичними особами – Подружжям** було облаштовано студію з використанням комп'ютерного обладнання, засобів фото- та відеозйомки, а також іншої техніки для забезпечення онлайн-трансляцій порнографічного характеру. Контент призначався для перегляду широким колом осіб через мережу Інтернет.

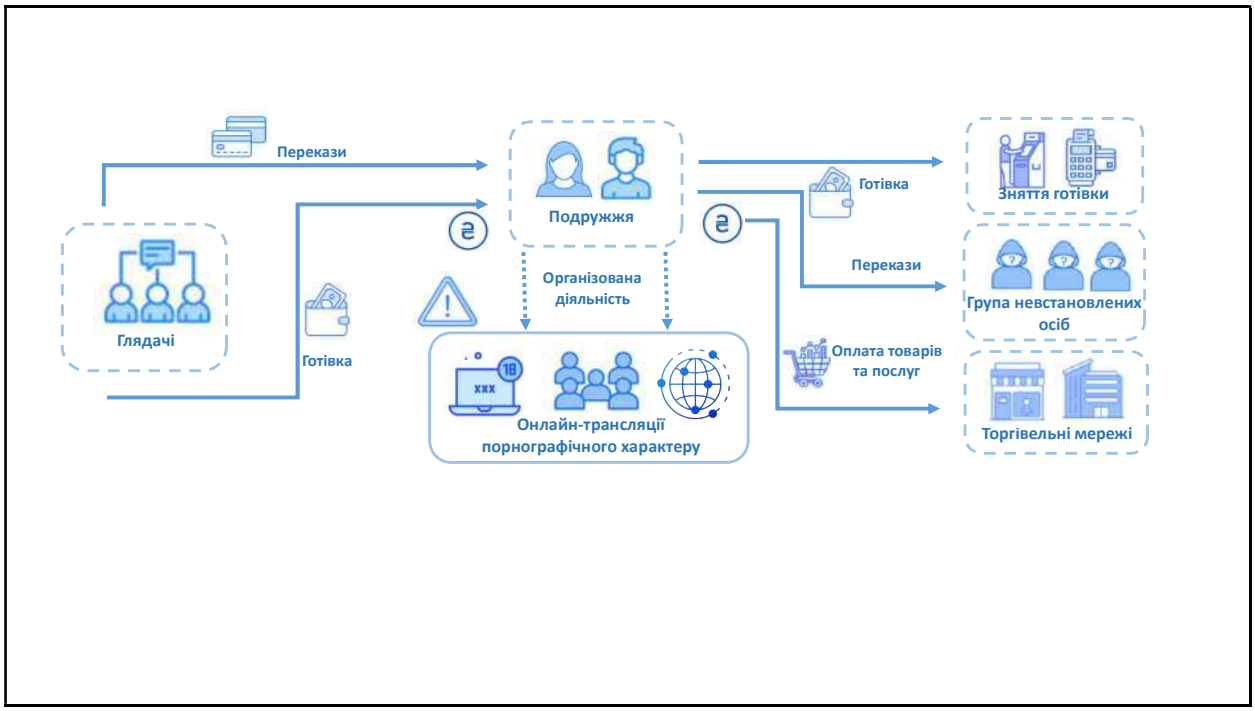
На рахунках **Подружжя** акумулювалися кошти, що надходили від **Групи фізичних осіб**, а також у готівковій та безготівковій формі через обслуговуючі банківські установи. У подальшому ці кошти:

- перераховувалися **Групі невстановлених осіб**;
- **знімалися готівкою**;
- використовувалися для **розрахунків у торговельних мережах** за товари та послуги.

Привертає увагу, що **сукупний офіційний дохід Подружжя значно менший,** ніж загальні суми здійснених ними фінансових операцій, що свідчить про можливе використання коштів **незаконного походження.**

Таким чином, є підстави вважати, що фінансові операції, проведені зазначеними фізичними особами, **мають ознаки приховування джерел походження коштів,** у тому числі отриманих від **незаконної діяльності,** пов'язаної зі створенням та розповсюдженням порнографічного контенту.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 2025.4.11.2. Легалізація незаконних доходів, одержаних від торгівлі людьми

Держфінмоніторингом, з урахуванням інформації, отриманої від суб'єктів первинного фінансового моніторингу та ПФР іноземної держави, виявлено **схему легалізації незаконних доходів**, одержаних фізичною особою від **торгівлі людьми.**

ПФР іноземної держави поінформовано про причетність громадянки України – **Фізичної особи А**, яка перебуває під вартою в іноземній країні, до **керівної структури міжнародної злочинної мережі,** що спеціалізувалася на організованому сутенерстві, торгівлі людьми та відмиванні коштів. Установлено, що ця мережа забезпечувала проституцію великої кількості жінок, їхнє залучення до надання сексуальних послуг та незаконне перевезення через кордони кількох держав.

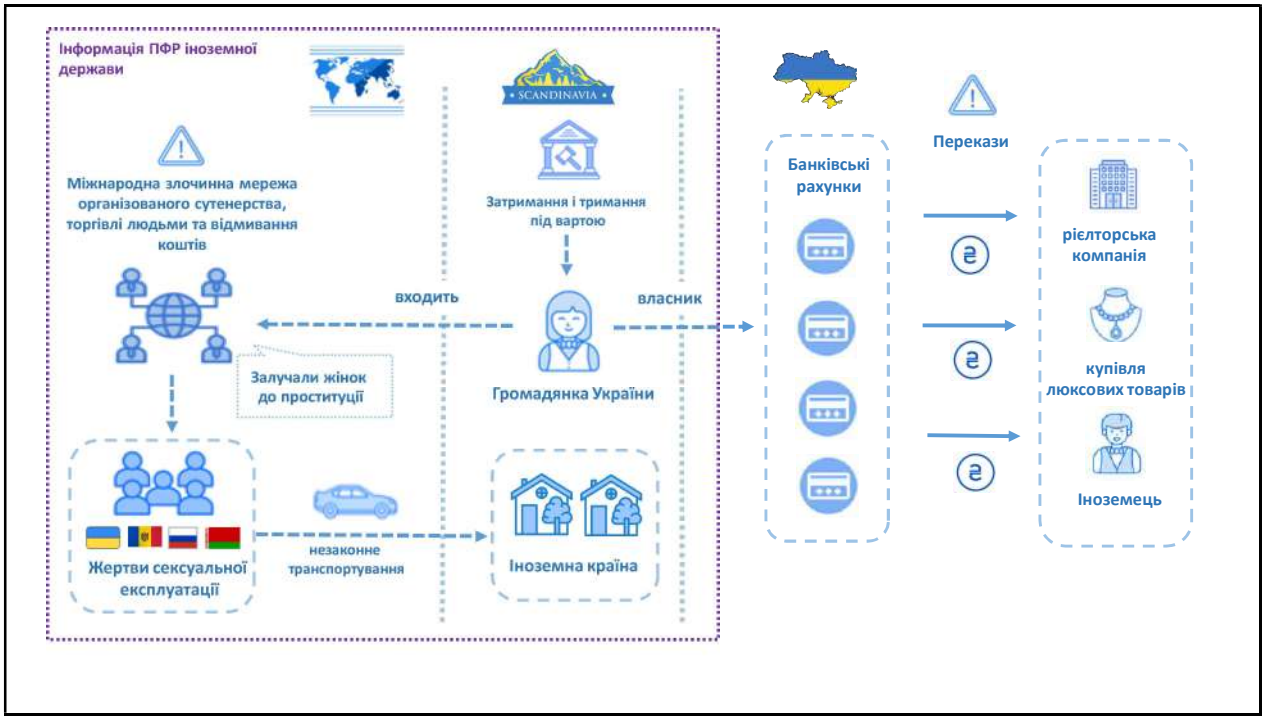
Встановлено, що **Фізична особа А** має рахунки, відкриті в банківських установах України. Проаналізовані фінансові операції, здійснені за межами України по цих рахунках, пов'язані з:

- купівлею **люксових товарів;**
- оплатою **нерухомості** на користь іноземної рієлторської компанії;
- переказами коштів іноземному громадянину, вказаному як **родич**.

Суми відповідних операцій значно перевищують офіційно задекларовані доходи **Фізичної особи А**.

Враховуючи ризики, що кошти на рахунках **Фізичної особи А** можуть мати злочинне походження, Держфінмоніторингом прийнято рішення про **зупинення видаткових операцій** та **блокування залишків коштів.**

Правоохоронним органом здійснюється досудове розслідування.


Інформація ПФР іноземної держави
SCANDINAVIA
Міжнародна злочинна мережа організованого сутенерства, торгівлі людьми та відмивання коштів
Затримання і тримання під вартою
входить
власник
Залучали жінок до проституції
Громадянка України
Банківські рахунки
Перекази
рієлторська компанія
купівля люксових товарів
Іноземець
Жертви сексуальної експлуатації
незаконне транспортування
Іноземна країна

РОЗДІЛ 4.12. ВІДМИВАННЯ ДОХОДІВ ВІД ТОРГІВЛІ НАРКОТИЧНИМИ ЗАСОБАМИ

У 2023–2025 роках незаконний обіг наркотичних засобів суттєво трансформувався, змістившись у бік синтетичних наркотиків, онлайн-торгівлі та транскордонних схем.

Військові умови та економічна нестабільність посилили вразливість населення, сприяли зростанню збутових мереж та активізації кримінальних груп, які використовують цифрову інфраструктуру для анонімного продажу та логістики наркотиків.

Поширеними є моделі збуту через даркнет, зашифровані месенджери, «закладки» та малопомітні кур'єрські канали, що ускладнює ідентифікацію учасників та потоків.

Фінансові схеми у цій сфері базуються на криптовалютах, електронних гаманцях, P2P-переказах, мікротранзакціях, змішувачах та використанні підставних осіб «дропів».

Ринок незаконного обігу наркотичних засобів стає більш децентралізованим, мобільним та технологічно вдосконаленим, що посилює ризики для фінансової системи України.

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

Приклад 2025.4.12.1. Підозрілі фінансові операції на рахунках групи фізичних осіб, які причетні до збуту наркотичних речовин

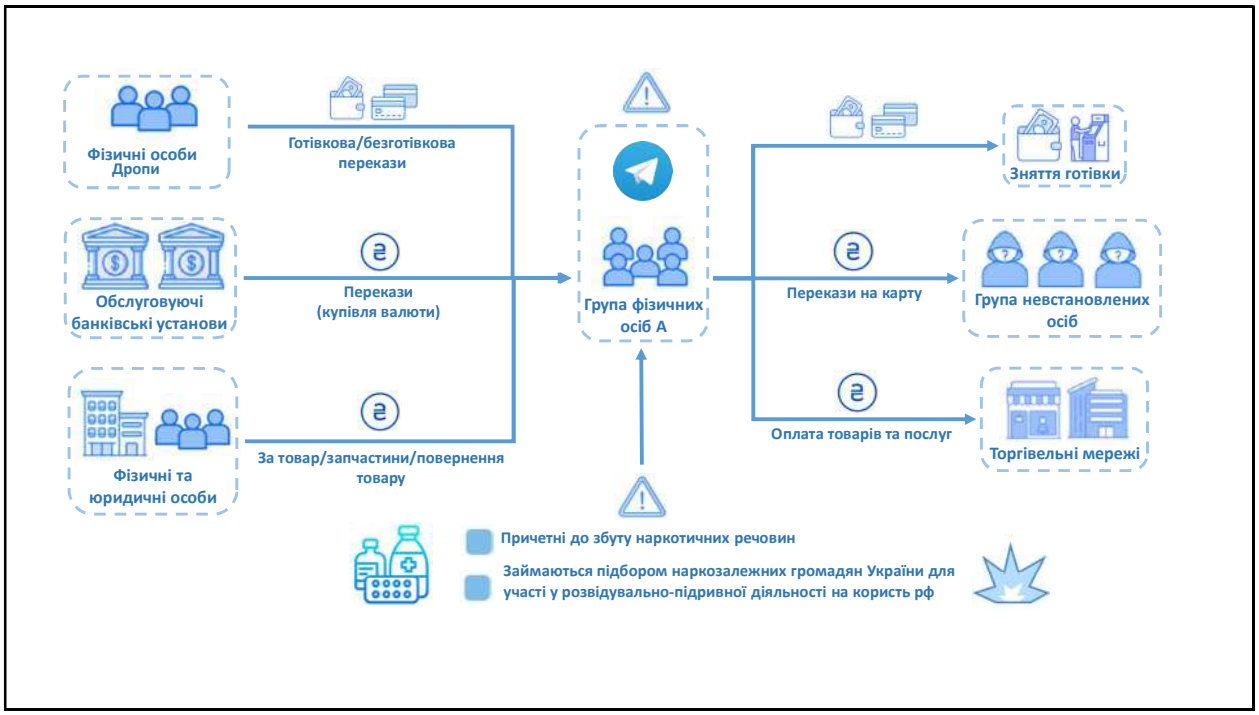
Держфінмоніторингом, з урахуванням інформації, отриманої від суб'єктів первинного фінансового моніторингу та правоохоронного органу, виявлено підозрілі фінансові операції на рахунках групи фізичних осіб, які підозрюються у збуті наркотичних речовин та підбору громадян України для участі у розвідувально-підривній діяльності на користь росії.

Правоохоронним органом надано інформацію, що спецслужбами рф через Телеграм-канал залучаються наркозалежні особи (громадяни України), які за винагороду здійснюють диверсії та інші протиправні дії на території України. Для цього залучаються треті особи, так звані «дропи», через яких здійснюють грошові перерахунки за виконану роботу. Виявлено, що до організації злочинної схеми причетна **Група фізичних осіб А**.

Встановлено, що на рахунках **Групи фізичних осіб А** акумулювались кошти з різних джерел: готівкові та безготівкові зарахування від фізичних і юридичних осіб за товари, запчастини, повернення товару, а також банківські перекази, зокрема – для купівлі валюти. У подальшому кошти були переміщені іншим фізичним особам, зняті готівкою або використані у якості розрахунків у торгівельних мережах за товари та послуги.

Характер проведених фінансових операцій та профіль їх учасників свідчить про ймовірність використання **Групою фізичних осіб А** «дропів» для переміщення коштів невідомого походження, у тому числі від збуту наркотичних речовин, які можуть використовуватись для фінансування протиправної діяльності.

Правоохоронним органом здійснюється досудове розслідування.



РОЗДІЛ 4.13. ВИКОРИСТАННЯ СТРАХОВОГО РИНКУ ТА НЕБАНКІВСЬКИХ ФІНАНСОВИХ УСТАНОВ У СХЕМАХ ВІДМИВАННЯ ДОХОДІВ, ОДЕРЖАНИХ ЗЛОЧИННИМ ШЛЯХОМ

Страховий ринок і небанківські фінансові установи також можуть бути залучені до схем відмивання доходів через зростання обсягів їхніх продуктів, активізацію ломбардів, мікрофінансових і факторингових компаній, що привертає увагу фінансових злочинців.

Багато продуктів страхування не є достатньо гнучкими, щоб бути першим інструментом вибору для відмивачів коштів. Однак, як і у випадку з іншими продуктами фінансових послуг, існує ризик того, що кошти, використані для придбання страхування, можуть бути доходами від злочинної діяльності.

По-перше, **розширення спектру страхових продуктів**, особливо у сегменті ризикового страхування (non-life), сприяє формуванню каналів для легалізації коштів. Зокрема, страхові премії можуть маскувати незаконне походження коштів, а виплати за договорами страхування – виконувати функцію «очищення» активів.

По-друге, **небанківські фінансові установи**, зокрема ломбарди, мікрофінансові компанії, факторингові установи, демонструють зростаючу активність на фінансовому ринку, але при цьому залишаються менш регульованими порівняно з банківським сектором. Це створює можливості для використання таких установ у схемах ВК/ФТ.

Крім того, **недостатній контроль за джерелами коштів**, обмежений моніторинг транзакцій та наявність компаній з фіктивною або частково легальною діяльністю створюють ризики використання страхових компаній і небанківських фінансових установ як проміжної ланки у багатоступеневих схемах ВК/ФТ.

У деяких випадках ці сегменти можуть використовуватись як **«транзитні зони»**: кошти реального сектору сплачувались за страховими договорами, переказувались далі як агентські винагороди або позики – без подальшого повернення, з ознаками фіктивності або підконтрольності бенефіціарів.

Узагальнені типові приклади відмивання злочинних доходів страховий ринок та небанківські фінансові установи наведено нижче.

Приклад 2025.4.13.1. Відмивання доходів із використанням страхової компанії та небанківської фінансової установи[41]

Виявлено схему відмивання доходів із використанням страхової компанії та небанківської фінансової установи.

Суб'єкти господарювання реального сектору економіки, у ролі клієнтів **Страхової компанії** (фігуранта кримінальних проваджень, ліцензії анульовані, перебуває у процесі припинення), перераховують їй страхові платежі (премії). Після цього **Страхова компанія** перераховує кошти **Небанківській фінансовій установі**, що має ліцензії на надання фінансових послуг (кредитування, факторинг), у вигляді винагороди як страховому агенту.

Надалі отримані кошти перераховуються у формі кредитів та позик іншим суб'єктам господарювання та небанківським фінансовим установам (які також мають ліцензії на провадження діяльності з надання фінансових послуг).

При цьому **відсутні будь-які розрахунки** за виданими кредитами та позиками.

Наведені факти можуть свідчити про участь **Страхової компанії** у схемі виведення прибутку суб'єктами господарювання реального сектору економіки шляхом:

– сплати коштів за договорами страхування;

– подальшого перерахування коштів **Небанківській фінансовій установі** під виглядом агентських винагород;

– скеровування коштів до підконтрольних організаторам схеми небанківських фінансових установ та юридичних осіб під виглядом кредитів і позик, які не повертаються.

Приклад 2025.4.13.2. Відмивання доходів із використанням підприємств з ознаками фіктивності[42]

Виявлено схему відмивання доходів, до якої залучені підприємства з ознаками фіктивності та небанківська фінансова установа.

Фізичні особи, використовуючи платіжні картки та послуги небанківської фінансової установи, ініціювали перекази на користь **Кредитної організації –** клієнта цієї небанківської установи **–** нібито з метою «погашення кредиту». Обсяги таких операцій становили **сотні мільйонів гривень за короткий період (близько 3 місяців)**.

Надалі зазначені кошти через банківські установи зараховувались **на платіжні картки інших фізичних осіб**, що свідчить про транзитний характер фінансових потоків без економічного сенсу.

За інформацією банків, які здійснювали еквайринг таких операцій, списання коштів з карток фізичних осіб фактично проводилось **за призначенням платежу «розваги»**, що не відповідає заявленій меті – «погашення кредиту».

[41] За інформацією НБУ
[42] За інформацією НБУ

Встановлено, що **Кредитна організація фактично не здійснювала видачу кредитів** (позик, позичок). Після певного періоду активної діяльності організація подала заяву на анулювання ліцензій, які було анульовано.

У діяльності **Кредитної організації** виявлено ознаки «фіктивності», зокрема:

- місцезнаходження збігається з адресою масової реєстрації;
- фактичне розташування в промисловій зоні, що нетипово для кредитних установ;
- вебсайт зареєстровано в день здійснення першої операції з «погашення кредиту».

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

Розуміння основних інструментів, індикаторів та способів вчинення злочинів є ключовим для ефективної протидії ВК та ФТ.

Виявлення операцій високого ризику, аналіз підозрілих фінансових транзакцій та діяльності учасників дозволяють своєчасно ідентифікувати нелегальну діяльність на ранніх етапах, встановлювати коло учасників, джерела походження нелегальних доходів і їх подальше використання.

В сучасних умовах протидія ВК та ФТ вимагає ретельного моніторингу фінансових операцій та впровадження передових технологій. Використання штучного інтелекту, big data-аналітики та автоматизованих систем виявлення аномалій дозволить швидко ідентифікувати підозрілі операції та поведінкові відхилення клієнтів.

У 2025 році інноваційні технології та ризик-орієнтований аналіз стають ключовими інструментами підвищення ефективності фінансового моніторингу.

Систематизація способів злочинної діяльності та виділення ключових елементів схем ВК/ФТ є основою ефективної протидії.

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

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

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

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

5.1. Основні інструменти у виявлених схемах ВК та ФТ

За результатами дослідження встановлено, що у типових схемах відмивання коштів та фінансування тероризму використовувались різні інструменти, які можливо згрупувати за тематичними напрямами..

Згрупування за принципом «Група інструментів» (Tool Group, скорочено TG) є доцільним для підвищення наочності та кращого розуміння механізмів використання відповідних інструментів у протиправній діяльності.

Представлена класифікація інструментів (TG) побудована на аналізі матеріалів Держфінмоніторингу, а також міжнародної практики.

Реєстраційні маніпуляції (TG)

Необґрунтовані реєстраційні дії

- створення юридичних осіб, що не обґрунтовано реальною економічною доцільністю;
- створення пов’язаних юридичних осіб із циклічними змінами директорів та бенефіціарів;
- створення юридичних осіб з мінімальними або відсутніми ознаками реальної діяльності;
- використання «підставних» осіб для реєстрації юридичних осіб та фізичних осіб-підприємців;

Фіктивні суб’єкти господарювання

- використання фіктивних суб’єктів господарювання та компаній-нерезидентів;
- використання підроблених реєстраційних документів;

Маніпуляції структурою власності та управління

- залучення підставних осіб, номінальних власників та використання складної структури власності;
- використання номінальних директорів;
- адреса юридичної особи не відповідає реальному місцезнаходженню бізнесу, відсутні ознаки фактичної діяльності;
- використання низки посередників з різних юрисдикцій для встановлення реальних КБВ;

Регіональний ризик

- реєстрація юридичних осіб у юрисдикціях із низьким рівнем прозорості бенефіціарів;
- створення юридичних осіб у країнах, що не підтримують санкційні режими;
- перереєстрація компаній за «законодавством» окупаційної влади;

Маскування діяльності

- застосування механізмів ребрендингу юридичної особи без об'єктивної економічної необхідності;
- маскування фактичної діяльності юридичної особи (створення хибного уявлення про характер або масштаби діяльності; приховування справжніх напрямів функціонування);
- зміна назви юридичної особи без економічної доцільності, у тому числі одразу після появи ризикових ознак чи негативних зв'язків;
- необґрунтована зміна виду економічної діяльності (КВЕД) (часта або різка зміна, що не відповідає операційній моделі);
- необґрунтована зміна доменного імені або цифрової ідентичності компанії;

Маніпуляції інформаційним середовищем

- використання компаній та організацій, залучених до інформаційних, пропагандистських або підривних операцій;

Використання фізичних осіб (TG)

Використання вразливих соціальних груп

- використання осіб з вразливих соціальних груп (безробітних, громадян похилого віку студентів, ВПО, громадян інших країн) для відкриття рахунків і здійснення транзитних операцій;

Використання кеш-кур'єрів

- використання «кеш-кур'єрів» для обготівкування та транспортування готівки;

Використання новітніх технологій (віртуальні активи)

- залучення фізичних осіб для отримання та конвертації віртуальних активів;

Використання підставних осіб, афілійованих компаній та дроблення бізнесу (TG)

- використання підставних осіб («дропів») для відкриття рахунків і проведення транзитних операцій;
- застосування дропів для обготівкування коштів через банкомати, P2P-перекази або криптовалютні біржі;
- вербування дропів через соціальні мережі, месенджери та оголошення про «швидкий заробіток»;
- спеціалізоване залучення дропів у шахрайські схеми, зокрема фішинг, діяльність кол-центрів та криптотранзит;

- реєстрація фізичних осіб – підприємців на підставних осіб («дропів») з подальшим використанням їхніх рахунків у схемах відмивання коштів та фінансування тероризму;
- організоване використання широкого кола фізичних осіб (номіналів, «дропів», транзитерів) для проведення фінансових операцій;
- використання пов'язаних фізичних осіб – підприємців та юридичних осіб для штучного розподілу фінансових потоків (дроблення бізнесу);
- залучення підконтрольних суб'єктів господарювання зі спільними власниками або директорами;
- використання афілійованих компаній у різних юрисдикціях для переміщення коштів;
- наявність ймовірних родинних або неформальних зв'язків між учасниками незаконних схем;
- централізоване управління рахунками, що формально належать різним фізичним та юридичним особам;

Маніпуляції з товаром (TG)

Маніпуляції з постачанням та номенклатурою товарів

- відсутність постачання товарів при 100% передоплаті;
- підміна (заміна) номенклатури товарів;
- фіктивне документальне оформлення без фактичного постачання товару;
- невідповідність задекларованих та фактичних обсягів/якості товарів;

Маніпуляції з характеристиками та ідентифікацією товарів

- змішування сировини різних виробників;
- зміна упаковки, маркування чи кодів УКТ ЗЕД для маскування походження;
- маскування товарів подвійного призначення під цивільні поставки;

Фіскальні та документарні схеми

- використання «скруток» та «зустрічних потоків»;

Логістика і транзит (TG)

Транскордонні маршрути обходу санкцій

- транспортування санкційних товарів через лояльні юрисдикції до країни агресора;
- перенаправлення товарів після перетину кордону (re-routing) – зміна фактичного маршруту або кінцевого отримувача товару вже після ввезення його до проміжної країни з метою приховування справжнього напрямку поставки або обходу санкційних обмежень;

- використання багатоступеневих логістичних маршрутів для маскування ланцюга постачання;

Використання транзитних компаній і логістичних посередників

- здійснення транзитних операцій із залученням компаній-транзитерів;
- використання компаній-посередників без реальної логістичної інфраструктури;
- створення фіктивних (віртуальних) логістичних маршрутів у документах;

Вартісні маніпуляції (TG)

Маніпуляції з ціною та вартісними показниками

- умисне завищення або заниження контрактної ціни товарів, робіт чи послуг порівняно з їх реальною ринковою вартістю;
- заниження або завищення задекларованих обсягів чи якості товарів;

Альтернативні канали розрахунків

- розрахунки у віртуальних активах за товарні операції;
- розрахунки через офшори для маскування справжньої вартості;
- використання третіх країн для розрахунків із рф/рб;

Фінансові маніпуляції (TG)

- оплата через ланцюг компаній без економічної доцільності;
- використання псевдокредитних та факторингових договорів для маскування руху коштів;
- використання рахунків, фактично контрольованих третіми особами;
- здійснення платежів через агрегатори або платіжні сервіси, що приховують реального отримувача коштів, у тому числі використання підставних інтернет-платіжних акаунтів/рахунків продавців, оформлених на фіктивних або непричетних осіб;
- розрахунки через офшорні рахунки, що не пов’язані з реальною господарською діяльністю;
- використання значної кількості рахунків одним клієнтом без економічної доцільності;
- проведення операцій на нетипово великі суми, що не відповідають ризик-профілю клієнта;
- різкі непритаманні зміни фінансової активності клієнта;
- дроблення платежів;
- використання підсанкційних або високоризикових платіжних систем;
- поповнення передплатних карток та інших інструментів із високим ризиком анонімності;

- дроблення платежів;

Маніпуляції з інвестиціями та цінними паперами (TG)

- псевдоінвестування та використання фіктивних інвестиційних продуктів;
- купівля-продаж неліквідних або «сміттєвих» цінних паперів для створення штучних збитків/прибутків;
- трансфер цінних паперів між пов'язаними особами за неринковими цінами;
- використання інвестиційних фондів або трастів для приховування походження активів;
- маніпуляції ринковою активністю (здійснення штучних або узгоджених торговельних операцій);
- використання криптоінвестиційних схем та фіктивних токенів для залучення коштів і маскування їх незаконного походження через створення штучних або неіснуючих цифрових активів;

Санкційні ризики (TG)

Обхід санкцій через треті країни

- використання третіх країн-посередників для обходу санкційних обмежень щодо рф/рб;
- приховування або свідоме викривлення інформації про кінцевого користувача та фактичну країну призначення товарів у контрактах, інвойсах, сертифікатах походження та митних документах;
- використання фінансових або торговельно-економічних операцій, пов'язаних із країнами, що віднесені міжнародними стандартами та національним законодавством до юрисдикцій з підвищеним чи високим ризиком ВК/ФТ/ФРЗМЗ, у тому числі через посередників або компанії, зареєстровані у третіх країнах, з метою приховування реального походження коштів, товарів або кінцевого бенефіціара;

Використання юридичних осіб для забезпечення поставок санкційних товарів

- використання юридичних осіб з метою імпорту на територію країни-агресора виробничого обладнання, яке може бути використано для виробництва військових товарів або товарів подвійного призначення;
- реєстрація юридичних осіб у юрисдикціях, що неналежно дотримуються санкційних режимів, з метою обслуговування операцій із підсанкційними суб'єктами;

Маскування власності та контролю над підсанкційними структурами

- заміна реальних кінцевих бенефіціарних власників або керівників підсанкційних юридичних осіб на номінальних осіб;
- створення нових компаній-«правонаступників» для продовження діяльності підсанкційних структур (ребрендинг, передача активів);
- приховування справжнього контролю через багаторівневі корпоративні структури у ризикових юрисдикціях;

Фінансовий обхід санкцій і альтернативні канали розрахунків

- використання банків, фінансових посередників та платіжних сервісів у країнах, які не приєдналися до санкцій, для проведення розрахунків із підсанкційними контрагентами;
- проведення розрахунків у віртуальних активах (у тому числі стейблкоїнах) для обходу санкційних та комплаєнс-обмежень традиційної фінансової системи;
- використання фінансових операцій у юрисдикціях підвищеного ризику для приховування реального походження коштів або бенефіціара;

Фінансові операції та зв'язки з територіями, де тривають військові дії (TG)

- отримання та відправлення переказів до/з територій, де ведуться бойові дії або діють незаконні збройні формування;
- регулярні транзакції з юридичними особами чи фізичними особами, що перебувають на тимчасово окупованих територіях або мають там операційну діяльність;
- співпраця з особами, афілійованими з релігійними чи іншими організаціями, які підтримують агресію росії або окупаційні адміністрації;
- маскування операцій через треті країни з метою приховування їхнього зв'язку з територіями військових дій;
- використання віртуальних валют для переказу коштів у зони військових дій;
- використання неофіційних систем розрахунків та готівкового переміщення коштів у регіонах з обмеженим контролем.

Операції з криптовалютами (TG)

- надання послуг з переведення криптовалюти у готівку, у тому числі через обмінники на тимчасово окупованих територіях;
- використання P2P-переказів, неліцензованих обмінників та інших платформ, що працюють поза регуляторним полем;
- співпраця з підсанкційними або високоризиковими криптобіржами;
- використання криптоміксерів, міжланцюгових мостів (сервісів, що дозволяють переводити активи між різними блокчейнами), а також приватних криптовалют для приховування реального походження коштів та ускладнення їх відстеження;
- використання фізичних осіб як «крипто-мулів» для отримання та конвертації криптовалют;
- здійснення транзакцій через високоризикові юрисдикції або платформи без KYC;
- використання криптовалют у шахрайських схемах та схемах фінансування тероризму та ніших незаконних схемах;
- використання фіктивних криптопроєктів для залучення коштів;

Цифрові маніпуляції та кіберзагрози (TG)

- створення фейкових акаунтів, підроблених та дубльованих веб-сайтів у різних юрисдикціях;
- використання шкідливих програм (включно з програмами-вимагачами) для викрадення даних та доступу до фінансових сервісів;
- викрадення цифрових даних, злом акаунтів користувачів та компрометація платіжних інструментів;
- несанкціоноване втручання в роботу електронних банківських систем;
- проведення фішингових атак, соціальної інженерії та застосування deepfake-технологій для обходу KYC;
- використання VPN, проксі та анонімізуючих інструментів для приховування цифрової ідентичності;

Маніпуляції інформацією та шахрайство (TG)

- використання ботоферм і фейкових акаунтів для викривлення інформації та імітації легітимних сервісів;
- проведення атак з використанням соціальної інженерії – шахрайських листів (фішинг), обманних телефонних дзвінків (bishing), шахрайських SMS-повідомлень (smishing) та маскування під легітимні номери чи адреси (spoofing) – з метою отримання доступів, паролів, кодів підтвердження та фінансової інформації клієнтів;
- перехоплення електронної кореспонденції та підміна реквізитів у рахунках (BEC-схеми — перехоплення корпоративної пошти для зміни платіжних даних);

- використання deepfake-технологій для обходу KYC та введення в оману контрагентів;

Незаконна діяльність (TG)

- здійснення незаконних правочинів, включаючи фіктивні договори та операції;
- використання гуманітарної допомоги для продажу або інших нелегальних фінансових вигод.

Узагальнений аналіз показує, що інструменти ВК/ФТ рідко застосовуються ізольовано – переважно вони комбінуються у складні багаторівневі моделі. Класифікація за TG дозволяє систематизувати ці прояви, виокремити типовий шаблон незаконної діяльності та забезпечити підґрунтя для формування індикаторів підозрілості й профілів ризику.

Таким чином, TG-класифікація є ключовим елементом дослідження схем ВК/ФТ у сучасних умовах та важливим інструментом для підвищення ефективності виявлення й запобігання протиправним фінансовим операціям.

5.2. Операційні інструменти та канали руху коштів, що використовуються у схемах ВК/ФТ

У процесі здійснення незаконних фінансових операцій правопорушники застосовують широкий спектр операційних інструментів та каналів руху коштів.

На відміну від кластерів «Груп інструментів» (TG), які відображають системні механізми та моделі побудови схем, операційні інструменти (Operational Instruments, OI) виконують функцію безпосереднього проведення фінансових транзакцій.

Операційні інструменти (OI) є універсальними та застосовуються у широкому спектрі незаконних фінансових схем, незалежно від їх структури, складності чи способу організації.

У більшості випадків такі інструменти не використовуються ізольовано. Злочинці комбінують їх із більш складними TG-інструментами, зокрема: залученням підставних осіб та транзитерів, використанням фіктивних компаній або НПО, застосуванням криптовалютної інфраструктури, побудовою транскордонних ланцюгів переміщення коштів, маніпуляціями з документами та цифровими ідентичностями тощо.

Такі поєднання дозволяють створювати багаторівневі незаконні схеми, які ускладнюють виявлення реальних бенефіціарів, джерел походження активів та кінцевого призначення фінансових потоків.

Використання операційних інструментів (OI) формує операційну основу більшості схем ВК/ФТ та значною мірою визначає їхню динаміку та спосіб реалізації.

Згрупування інструментів за принципом «Операційні інструменти» (Operational Instruments, OI) є логічним та доцільним для підвищення наочності і кращого розуміння того, яким саме чином здійснюється рух коштів у межах протиправних фінансових схем.

Представлена класифікація операційних інструментів (OI) побудована на аналізі матеріалів Держфінмоніторингу, правоохоронних органів, а також міжнародної практики.

Нижче наведено найбільш розповсюджені операційні інструменти у схемах ВК/ФТ:

Класичні фінансові інструменти

Інструменти введення коштів у фінансову систему (ОІ)

- використання платіжних терміналів та банкоматів;
- зарахування коштів на карткові рахунки через провайдерів електронних грошей;
- внесення готівки через каси банків;
- поповнення електронних гаманців;
- внесення коштів на рахунки через сторонніх осіб (транзитери, підставні особи «дропи»);

Готівкові операції та інструменти швидкого обігу готівки (ОІ)

- використання готівки;
- обмін готівкової валюти у легальних та нелегальних пунктах;
- використання кеш-кур'єрів;
- передача коштів готівкою через кордон;
- використання неформальних систем розрахунків (аналог hawala, Telegram-обмінники);

Інструменти транзиту та переміщення коштів (ОІ)

- використання послуг інтернет-еквайрингу та анонімізованих платіжних сервісів;
- P2P-перекази через банки та мобільні сервіси;
- транзит через рахунки третіх осіб («мулів»);
- використання великої кількості карткових рахунків для дроблення операцій;
- перекази через системи міжнародних платежів;

Інструменти маскування економічної суті операцій (ОІ)

- надання або повернення фінансової допомоги/позик;
- надання благодійної допомоги;
- використання неприбуткових організацій (НПО);
- виплата дивідендів;
- передача коштів у формі подарунків родичам;
- купівля-продаж майнових прав та інших нематеріальних активів;
- здійснення інвестицій та їх повернення;

Інструменти інтеграції коштів у легальну економіку (OI)

- придбання елітних автомобілів та дороговартісних активів;
- інвестиції у нерухомість, включно з псевдодолевою участю;
- використання фінансових компаній (ломбарди, факторинг, мікрофінансування);

Сучасні цифрові та онлайн-інструменти

Інструменти цифрової ідентичності та обходу KYC (OI)

- використання deepfake-технологій для проходження дистанційної верифікації;
- використання викрадених акаунтів банкінгу/FinTech;
- перевипуск SIM-карти клієнта шахраями з метою отримання контролю над його номером телефону та перехоплення SMS-кодів і одноразових паролів для входу в онлайн-банкінг та проведення фінансових операцій;
- купівля номерів телефонів, що раніше належали клієнтам фінансових установ з метою отримання одноразових паролів для відновлення доступу до онлайн-банкінгу від імені клієнтів, проведення фінансових операцій та оформлення кредитів;
- використання VPN/Proxy/TOR для анонімізації IP-адрес та геолокації;
- створення «чистих» акаунтів у неукраїнських фінтех-сервісах для подальших транзакцій;

Цифрові та криптовалютні інструменти (OI)

- операції з криптовалютами (віртуальними активами), включаючи P2P-платформи;
- використання криптобірж або P2P-платформ, що обслуговують російських користувачів або перебувають під санкціями;
- використання неліцензованих криптообмінників;
- використання криптоміксерів та міжланцюгових мостів;
- використання подарункових карток як інструмента анонімізації;
- купівля та продаж NFT і цифрових токенів (унікальних цифрових об’єктів та криптографічних активів, що підтверджують право власності в блокчейні);
- використання електронних маркетплейсів для фіктивних продажів;

Інструменти електронної комерції (ОІ)

- фіктивні інтернет-магазини;
- використання платформ дропшипінгу;
- прийом платежів через соцмережі та месенджери;
- використання маркетплейсів для фіктивних продажів/повернень;
- платформи для краудфандингу – фіктивні збори;

Інструменти грального бізнесу (ОІ)

- використання неліцензованих онлайн-казино;
- виплата «виграшів» як спосіб легалізації коштів (включно з псевдо виграшами в онлайн-іграх).

5.3. Індикатори підозрілості учасників (PI)

У процесі аналізу виявлених схем встановлено, що ключовим чинником їх реалізації є характеристики самих учасників – їхні поведінкові, структурні та цифрові ознаки, які відхиляються від типової або економічно обґрунтованої моделі діяльності.

Саме такі відхилення визначаються як **індикатори підозрілості учасників** (Participant Indicators, PI), що дозволяють ідентифікувати ризикових клієнтів, виявляти приховані зв'язки та встановлювати потенційну причетність до схем ВК/ФТ.

Індикатори PI застосовуються як елементи первинної та поглибленої аналітичної оцінки та не є самостійним доказом протиправної діяльності.

На відміну від інструментів і механізмів схем ВК/ФТ (TG та OI), які описують, що саме використовується у незаконних операціях, індикатори PI відображають, хто саме бере участь у схемі та які характерні поведінкові або структурні відхилення спостерігаються в учасників.

Індикатори підозрілості учасників є ключовим елементом ризик-орієнтованого аналізу та застосовуються для:

- оперативної ідентифікації ризикових учасників фінансових операцій;
- виявлення неочевидних зв'язків і повторюваних патернів поведінки;
- оцінки ступеня аномальності профілю клієнта;
- підсилення алгоритмів автоматизованого ризик-скорингу та AML-моделей;
- підвищення точності виявлення схем ВК/ФТ на ранніх стадіях.

З метою підвищення аналітичної ефективності індикатори підозрілості учасників (PI) згруповано за тематичними напрямами, що відображають найбільш поширені поведінкові, структурні та цифрові аномалії учасників у межах типових схем ВК/ФТ.

Представлена класифікація побудована на основі матеріалів Держфінмоніторингу, а також міжнародної практики.

Нижче наведено систематизований перелік ключових індикаторів підозрілості учасників (PI), що найчастіше фіксувалися у виявлених та досліджених схемах ВК/ФТ.

Класифікація індикаторів підозрілості учасників

Категорія	Група індикаторів підозрілості учасників
Геополітичні та санкційні ризики (Geopolitical and Sanctions Risks – GEO)	• WF – Фінансування війни. SA – Санкції. PP – Політичні партії.
Державні кошти (Governmental and Budgetary Risks – GOV)	• BGCR – Бюджет/корупція.
Комерційні зловживання та податкові порушення (Business and Tax Abuse & Evasion Risks – BUS)	• BA – Діяльність учасника. BO – Кінцеві бенефіціари та посадові особи. • TE – Ухилення від сплати податків. PII – Професійні посередники.
Технологічні та кіберризики – Technological and Cyber Risks (TECH)	• DI – Зловживання цифровою ідентичністю.
Кримінальні ризики – Criminal Risks (CRIME)	• CIN – Кримінальна причетність особи. • CYB – Кіберзлочинність. • FR – Шахрайство.
Соціальні та гуманітарні ризики (Social and Humanitarian Risks – SOC)	• NP – Неприбуткові організації. RO – Релігійні організації.
Поведінкові та загальні ризики (Behavioral and General Risk Factors – GEN)	• GN – Загальні індикатори. DC – Документи.

Індикатори підозрілості учасників не є самостійною підставою для висновку про протиправну діяльність, а застосовуються у сукупності з іншими індикаторами, результатами транзакційного аналізу та професійним судженням аналітика відповідно до ризик-орієнтованого підходу.

Рівень ризику за індикаторами PI має визначатися з урахуванням кількості індикаторів, їх повторюваності, контексту діяльності клієнта та результатів додаткової перевірки.

Уніфікована система кодування індикаторів підозрілості учасників. До індикаторів підозрілості учасників додано уніфіковані коди з метою ідентичності, можливої автоматизації та подальшої інтеграції у внутрішні аналітичні системи суб'єктів фінансового моніторингу (зокрема модулі ризик-скоринг-платформ).

Для кожного індикатора застосовується стандартизований кодовий формат, який забезпечує можливість автоматичного групування, пошуку та оновлення індикаторів за категоріями. Наведено можливі алгоритми виявлення, що сприяють ефективному аналізу та обробці даних.

Така система кодування є першим кроком до побудови сучасної ризик-орієнтованої аналітичної інфраструктури та дозволяє ефективно інтегрувати індикатори підозрілості учасників у бази даних, алгоритми машинного навчання й аналітичні дашборди, підвищуючи точність виявлення суб'єктів, потенційно причетних до підозрілої діяльності, та одночасно знижуючи вплив людського фактора в процесі прийняття аналітичних рішень.

Група: GEO; Категорія: фінансування війни – war financing (WF)

Код індикатора	Назва індикатора	Можливі джерела інформації (для автоматизації; перелік не обмежує використання інших джерел)	Можливі алгоритми виявлення
PI-WF-001	Особа, пов'язана з незаконним збройним формуванням або окупаційними адміністраціями.	Санкційні списки; база розшуку МВС; дані СБУ; відкриті судові рішення; OSINT.	Виявлено збіг особи з санкційними списками, даними МВС/СБУ або судовими рішеннями.
PI-WF-002	Особа, яка фігурує у кримінальних провадженнях щодо державної зради, колабораційної діяльності, тероризму, диверсій або інших злочинів проти основ національної безпеки України.	Судові рішення; санкційні списки; інформаційні повідомлення державних, правоохоронних або розвідувальних органів; OSINT.	Виявлення кримінальних проваджень або офіційних повідомлень щодо державної зради, колабораційної діяльності чи тероризму.
PI-WF-003	Реєстрація ФОП або юридичних осіб на тимчасово окупованих територіях.	ЄДР (місце реєстрації); IP - та геолокаційні дані; дані операторів POS-терміналів; інформаційні повідомлення державних, правоохоронних або розвідувальних органів.	Виявлено ФОП/юридичних осіб зареєстрованих на ТОТ.
PI-WF-004	Використання виробничих потужностей, розташованих на тимчасово окупованих територіях або під контролем рф.	Перелік територій, на яких ведуться бойові дії або які тимчасово окуповані.	Виявлено використання виробничих потужностей на ТОТ або під контролем рф.
PI-WF-005	Причетність до благодійних/ релігійних/громадських організацій, що підтримують тероризм, екстремізм чи військову агресію рф.	Санкційні списки; матеріали правоохоронних органів; OSINT.	Виявлено зв'язок особи з благодійною, релігійною або громадською організацією, що підтримує тероризм чи агресію рф.
PI-WF-006	Причетність до логістичних компаній або «перевалочних» вузлів, що обслуговують товарні потоки рф з	Інформаційні повідомлення державних, правоохоронних або розвідувальних органів.	Встановлено причетність до логістичних компаній або «перевалочних» вузлів, задіяних в обслуговуванні санкційних потоків

	метою обходу санкцій.		рф.
PI-WF-007	Наявність у клієнта або його пов'язаних осіб (посадові особи, бенефіціари) активів (для ведення бізнесу) на тимчасово окупованих територіях.	KYC-дані клієнта; інформаційні повідомлення державних, правоохоронних або розвідувальних органів; OSINT.	У клієнта або пов'язаних осіб виявлено активи для бізнесу на ТОТ.
PI-WF-008	Зв'язки з юридичними особами або структурами, що перебувають у санкційних списках.	Санкційні списки; OSINT.	Виявлено зв'язки з юридичними особами зі санкційних списків.
PI-WF-009	Причетність учасника до псевдогуманітарних фондів або «волонтерських» структур, які фігурують у схемах фінансування агресії рф.	Санкційні списки; інформаційні повідомлення державних, правоохоронних або розвідувальних органів; OSINT.	Виявлено зв'язок учасника з псевдогуманітарними чи «волонтерськими» структурами, залученими до фінансування агресії рф.
PI-WF-010	Взаємодія учасника з посередниками з юрисдикцій, що активно використовуються рф для обходу санкцій.	Аналітика ризикових контрагентів; OSINT.	Зафіксовано взаємодію з посередниками з юрисдикцій обходу санкцій рф (ризикова географія).
PI-WF-011	Клієнт або керівники/бенефіціари мають зв'язки з бізнес-структурами, що забезпечують потреби військово-промислового комплексу рф.	Санкційні списки; інформаційні повідомлення державних, правоохоронних або розвідувальних органів; OSINT.	Клієнт/бенефіціари пов'язані з бізнесами, що забезпечують ВПК рф.
PI-WF-012	Публічна діяльність учасника, що демонструє підтримку військових дій рф/рб чи ідеологічних структур агресії.	OSINT.	Виявлена публічна підтримка військових дій рф/рб або ідеології агресії.

Група: GEO; Категорія: санкції – sanctions (SA)

Код індикатора	Назва індикатора	Можливі джерела інформації (для автоматизації; перелік не обмежує використання інших джерел)	Можливі алгоритми виявлення
PI-SA-001	Щодо учасника застосовано національні або міжнародні санкції.	Санкційні списки.	Автоматизована перевірка учасника за національними та міжнародними санкційними списками.
PI-SA-002	Учасник має ознаки сприяння обходу санкційних обмежень (через посередників, альтернативні юрисдикції, мережі пов’язаних осіб).	Санкційні списки; комерційні бази; аналітика ризикових контрагентів; OSINT.	Виявлення опосередкованих зв’язків учасника з підсанкційними особами через посередників або альтернативні юрисдикції із застосуванням граф-аналізу та аналітики контрагентів.
PI-SA-003	Наявна публічна або офіційна інформація про співпрацю учасника з підсанкційними суб’єктами, фінансовими установами або платформами.	Санкційні списки; офіційні публічні повідомлення державних/правоохоронних органів; OSINT.	Автоматизований моніторинг відкритих та офіційних джерел із використанням пошуку за ключовими словами для виявлення інформації про співпрацю з підсанкційними суб’єктами.
PI-SA-004	Учасник пов’язаний із юридичними особами, створеними або перереєстрованими з метою обходу санкцій.	ЄДР; комерційні бази; OSINT.	Аналіз реєстраційних даних юридичних осіб з метою виявлення компаній, створених або перереєстрованих після запровадження санкцій та пов’язаних із підсанкційними особами через бенефіціарів, керівників або контактні дані.

PI-SA-005	Наявність мережі пов’язаних осіб/компаній, що маскує контроль або бенефіціарів підсанкційних активів.	Комерційні бази; OSINT.	Застосування мережевого аналізу для виявлення складних або циклічних структур володіння, номінальних учасників та інших ознак приховування фактичного контролю над підсанкційними активами.
PI-SA-006	Учасник здійснює діяльність у юрисдикціях підвищеного ризику обходу санкцій без очевидної економічної доцільності.	Санкційні списки; переліки високоризикових юрисдикцій; комерційні аналітичні платформи; OSINT.	Автоматизований аналіз географії діяльності та фінансових операцій учасника з фокусом на юрисдикції підвищеного ризику.
PI-SA-007	Керівники, бенефіціари або пов’язані особи учасника перебувають під санкціями.	Санкційні списки; комерційні аналітичні платформи.	Автоматична перевірка керівників, кінцевих бенефіціарних власників та пов’язаних осіб учасника за санкційними списками.

Група: GEO; Категорія: політичні партії – political parties (PP)

Код індикатора	Назва індикатора	Можливі джерела інформації (для автоматизації; перелік не обмежує використання інших джерел)	Можливі алгоритми виявлення
PI-PP-001	Причетність учасника до політичної партії, забороненої в Україні через просування проросійських наративів.	Судові рішення; повідомлення Мін’юсту України; санкційні списки РНБО; офіційні повідомлення правоохоронних органів; OSINT.	Автоматична перевірка учасника за переліками заборонених в Україні політичних партій і санкційними списками.
PI-PP-002	Афілійованість учасника із забороненою політичною партією через пов’язані юридичні особи.	ЄДР; судові рішення; офіційні повідомлення правоохоронних органів; OSINT.	Автоматизований аналіз реєстраційних даних і пов’язаних осіб (бенефіціарів, керівників, засновників).

PI-PP-003	Публічна діяльність учасника, яка, відповідно до судових рішень та/або офіційно оприлюдненої інформації державних чи правоохоронних органів, свідчить про системне просування інтересів політичної партії або пов'язаних із нею структур, діяльність яких заборонена в Україні.	Судові рішення; повідомлення державних чи правоохоронних органів.	Автоматизований моніторинг відкритих джерел і офіційних повідомлень із застосуванням пошуку за ключовими словами та аналізу згадок учасника.

Група: GOV; Категорія: бюджет/корупція – budget-corruption (BGCR)

Код індикатора	Назва індикатора	Можливі джерела інформації (для автоматизації; перелік не обмежує використання інших джерел)	Можливі алгоритми виявлення
PI-BGCR-001	Наявність негативної інформації щодо клієнта — учасника публічних закупівель для потреб держави або територіальних громад.	Портали публічних закупівель; Судові рішення; комерційні аналітичні платформи з аналізу закупівель; OSINT.	Автоматичне зіставлення даних клієнта з інформацією з реєстрів судових рішень та порталів публічних закупівель для виявлення фактів участі та наявності негативної інформації..
PI-BGCR-002	Відсутність у учасника, який визначений переможцем бюджетної закупівлі, реальної бізнес-інфраструктури (офісу, персоналу, матеріально-технічної бази), необхідної для виконання умов договору.	KYC/EDD-дані; OSINT.	Автоматизоване зіставлення даних про переможця закупівлі з KYC/EDD-профілем (офіс, персонал, активи).

PI-BGCR-003	Отримання чи виявлення інформації щодо особи, яка причетна до розкрадання бюджетних коштів та/або вчинення корупційних діянь.	KYC/EDD-дані; OSINT.	Автоматичний моніторинг судових рішень, офіційних повідомлень та відкритих джерел на предмет згадування клієнта у корупційних або розкрадання бюджетних коштів.
PI-BGCR-004	Клієнт має ознаки повторюваних перемог у процедурах публічних закупівель з обмеженою кількістю учасників, серед яких виявляються пов’язані між собою особи, у тому числі з самим клієнтом.	Портали публічних закупівель; комерційні аналітичні платформи з аналізу закупівель; KYC/EDD-дані; OSINT.	Автоматичний аналіз історії участі клієнта у закупівлях.
PI-BGCR-005	Регулярне залучення учасником посередників або третіх осіб для отримання платежів за договорами, укладеними з розпорядниками бюджетних коштів.	Портали публічних закупівель; комерційні аналітичні платформи з аналізу закупівель; KYC/EDD-дані; OSINT.	Аналіз платіжних потоків за бюджетними договорами.
PI-BGCR-006	Наявність підтвердженої інформації про фігурування учасника у журналістських розслідуваннях щодо розкрадання бюджетних коштів, хабарництва або інших корупційних правопорушень.	Журналістські розслідування; повідомлення правоохоронних органів; судові рішення; OSINT.	Автоматизований моніторинг відкритих джерел та медіа.
PI-BGCR-007	Наявність інформації про участь учасника у кримінальних	Судові рішення; офіційні публічні повідомлення правоохоронних органів; OSINT.	Автоматична перевірка клієнта за судовими реєстрами та

	провадженнях за корупційними статтями Кримінального кодексу України.		офіційними повідомленнями.
PI-BGCR-008	Політично значуща особа (PEP) або пов'язана з нею особа фігурує у кримінальних провадженнях або судових справах за корупційними статтями Кримінального кодексу України.	Судові рішення; офіційні публічні повідомлення правоохоронних органів; OSINT.	Автоматизоване виявлення корупційних справ.

Група: BUS; Категорія: діяльність учасника – business activity (BA)

Код індикатора	Назва індикатора	Можливі джерела інформації (для автоматизації; перелік не обмежує використання інших джерел)	Можливі алгоритми виявлення
PI-BA-001	Учасник є новостворeним суб'єктом господарювання.	ЄДР.	Автоматичне визначення дати реєстрації. У разі строку діяльності менше встановленого порогу.
PI-BA-002	Незначний розмір статутного капіталу, що не відповідає заявленим масштабам діяльності.	ЄДР; KYC/EDD.	Зіставлення розміру статутного капіталу з заявленими оборотами або видами діяльності.
PI-BA-003	Відсутність або незначна кількість найманих працівників, що не відповідає характеру та обсягам заявленої діяльності.	ЄДР; податкові дані (у межах доступу); KYC/EDD; OSINT.	Автоматичне порівняння кількості працівників із заявленими обсягами діяльності.
PI-BA-004	Часті зміни назви юридичної особи, керівників або засновників без обґрунтованих бізнес-причин.	ЄДР; комерційні реєстри.	Фіксація кількості змін реєстраційних даних за визначений період.
PI-BA-005	Часті зміни місцезнаходження, адреси реєстрації або основних видів	ЄДР; комерційні реєстри; KYC/EDD.	Автоматичний аналіз історії змін адреси або видів діяльності.

	діяльності.		
PI-BA-006	Відсутність основних засобів, виробничих потужностей, складських приміщень або іншої матеріально-технічної бази, необхідної для діяльності.	KYC/EDD; OSINT.	Зіставлення заявленої діяльності з наявністю основних засобів.
PI-BA-007	Припинення або ліквідація суб'єкта господарювання невдовзі після здійснення фінансових операцій на значні суми.	ЄДР; OSINT.	Припинення діяльності невдовзі після проведення фінансових операцій на значні суми.
PI-BA-008	Учасник не є виробником товарів, але декларує значні обсяги торгівлі або експорту.	ЄДР; податкові чи митні дані (публічні); KYC/EDD.	Порівняння статусу учасника з обсягами торгівлі або експорту.
PI-BA-009	Відсутність ліцензій або дозволів на види діяльності, що підлягають обов'язковому ліцензуванню.	Ліцензійні реєстри; ЄДР; KYC/EDD.	Автоматична перевірка наявності ліцензій для відповідних КВЕД.
PI-BA-010	Відсутність витрат на оренду або утримання приміщень за відсутності підтвердження використання власних або інших площ.	KYC/EDD; OSINT.	Аналіз фінансових витрат на утримання приміщень.
PI-BA-011	Реєстрація за адресою масової реєстрації юридичних осіб.	ЄДР; комерційні реєстри; OSINT.	Автоматичне зіставлення адреси з переліками масової реєстрації.
PI-BA-012	Наявність значної кількості рахунків у різних банківських установах без зрозумілої бізнес-логіки.	KYC/EDD; внутрішні банківські дані.	Аналіз кількості відкритих рахунків.
PI-BA-013	Залучення надмірної кількості посередників або номінальних контрагентів без економічної доцільності.	KYC/EDD; аналітика контрагентів; OSINT .	Виявлення ланцюгів посередників без економічної доцільності.

PI-BA-014	Відсутність належної деталізації в договорах або торгових угодах (опис товарів/послуг, ціноутворення, обсяги).	Договори (контрагенти); KYC/EDD.	Перевірка договорів на наявність ключових умов.
PI-BA-015	Ознаки номінального характеру діяльності: мінімальна операційна активність при значних фінансових оборотах.	KYC/EDD.	Зіставлення фінансових оборотів із реальною операційною активністю.
PI-BA-016	Відсутність або формальна цифрова присутність (вебсайт, контактні дані, ділова комунікація) при заявленій активній діяльності.	OSINT; KYC/EDD.	Аналіз наявності вебсайту, контактів та ділової комунікації.
PI-BA-017	Невідповідність між задекларованими видами діяльності (КВЕД) та фактичним характером діяльності.	ЄДР; KYC/EDD.	Порівняння задекларованих КВЕД з фактичними операціями клієнта.

Група: BUS; Категорія: кінцеві бенефіціарні власники та посадові особи – beneficial owners and officials (BO)

Код індикатора	Назва індикатора	Можливі джерела інформації (для автоматизації; перелік не обмежує використання інших джерел)	Можливі алгоритми виявлення
PI-BO-001	Наявність ознак розбіжностей між відомостями про КБВ та структурою власності юридичної особи.	ЄДР; KYC/EDD; комерційні аналітичні платформи; OSINT.	Автоматичне зіставлення КБВ з ЄДР та KYC-профілем; виявлення різних осіб/часток; flag при зміні КБВ без оновлення KYC.
PI-BO-002	Ознаки використання номінальних посадових осіб або номінальних КБВ.	KYC/EDD; ЄДР; OSINT; аналітика зв’язків.	Графовий аналіз: одна особа та десятки компаній; відсутність доходів/активів у КБВ.
PI-BO-003	Фізична особа є КБВ або входить до органів управління	ЄДР; комерційні аналітичні платформи;	Порогове правило: >N компаній за X місяців;

	значної кількості юридичних осіб без економічної логіки.	OSINT.	мережевий показник «multi-director» (надмірна концентрація керівних/бенефіціарних ролей однієї особи).
PI-BO-004	КБВ/керівник з ознаками соціальної або економічної вразливості.	KYC/EDD; ЄДР; OSINT.	Вік фізичної особи <20 або 75<. Відсутність доходів та роль фізичної особи в юридичній особі. Офіційні доходи та обороти юридичної особи.
PI-BO-005	Короткий період існування юридичних осіб та часті зміни засновників/керівників.	ЄДР; KYC/EDD.	«age-risk score» компанії; Правило: >2 змін за 12 міс.
PI-BO-006	Негативна інформація щодо КБВ/керівника.	Судові рішення; повідомлення державних органів та правоохоронних органів; OSINT.	Автоматизований пошук у судових документах; контрольний список слів/фраз для автоматичного пошуку.
PI-BO-007	Одноосібний посадово-засновницький склад.	ЄДР; KYC/EDD.	Поєднання одноосібного керівництва та бенефіціарного володіння з високими фінансовими оборотами — тригер підвищеного ризику.
PI-BO-008	Непрозора або надмірно ускладнена структура власності.	ЄДР; KYC/EDD; аналітичні платформи; OSINT.	Надмірно ускладнена багаторівнева структура власності, у тому числі із залученням іноземних юридичних осіб без зрозумілої економічної мети.

PI-BO-009	КБВ/керівник проживає або зареєстрований на ТОТ.	ЄДР; KYC/EDD; переліки ТОТ; OSINT.	Гео-фільтр адрес; перетин із переліком ТОТ.
PI-BO-010	Опосередкований контроль з боку громадян рф/рб над юридичною особою через третіх осіб.	Аналітика зв'язків; санкційні списки; KYC/EDD; OSINT.	Graph-path detection (RF → intermediary → client) – автоматизоване виявлення ланцюгів фінансових або контрольних зв'язків між суб'єктами через посередників (від джерела ризику до кінцевого клієнта). Ownership-chain – аналіз ланцюга володіння та контролю з метою встановлення кінцевих бенефіціарних власників і прихованих зв'язків між компаніями та фізичними особами.
PI-BO-011	Невідповідність фінансового стану КБВ масштабам діяльності ЮО.	KYC/EDD; OSINT; фінансова аналітика.	Wealth vs turnover mismatch – невідповідність між задекларованим (або очікуваним) рівнем добробуту клієнта та обсягами фінансових оборотів за рахунками. ML-feature «wealth_gap» – аналітичний показник (ознака для моделей машинного навчання), що кількісно відображає розрив між фінансовими оборотами та підтвердженими

			доходами/активами клієнта.
PI-BO-012	Часті зміни КБВ або керівників юридичної особи.	ЄДР; KYC/EDD.	Моніторинг даних ЄДР та KYC/EDD для фіксації частих змін кінцевих бенефіціарних власників або керівників юридичної особи протягом визначеного періоду.

Група: BUS; Категорія: ухилення від сплати податків- tax evasion (TE)

Код індикатора	Назва індикатора	Можливі джерела інформації (для автоматизації; перелік не обмежує використання інших джерел)	Можливі алгоритми виявлення
PI-TE-001	Наявність податкового боргу у клієнта за даними ДПС України за умови суттєвих або непропорційно високих фінансових оборотів за рахунками, що не відповідають податковому статусу та фінансовому профілю клієнта.	ДПС України (податковий борг); KYC/EDD; фінансова звітність.	Перевірка наявності податкового боргу за даними ДПС.
PI-TE-002	Наявність судових рішень щодо клієнта за ст. 212 КК України (ухилення від сплати податків).	судові реєстри.	Моніторинг судових реєстрів на наявність рішень за ст. 212 КК України (ухилення від сплати податків) щодо клієнт.
PI-TE-003	Відсутність нарахування та виплати заробітної плати працівникам за наявності ознак господарської діяльності.	KYC/EDD.	Зіставлення даних про наявність обов’язкових платежів та сплачених податків.
PI-TE-004	Відсутність задекларованих доходів та/або сплачених податків	ДПС (декларації, податки); фінансова звітність; банківські обороти;	Порівняння обсягів банківських оборотів із задекларованими

	за наявності значних фінансових оборотів.	KYC/EDD.	доходами. Якщо обороти суттєво перевищують задекларовані доходи або доходи відсутні.

Група: BUS; Категорія: професійні посередники – Professional Intermediaries (PII)

Код індикатора	Назва індикатора	Можливі джерела інформації (для автоматизації; перелік не обмежує використання інших джерел)	Можливі алгоритми виявлення
PI-PII-001	Аудитор, бухгалтер або податковий консультант системно залучений до обслуговування значної кількості клієнтів із підвищеним рівнем ризику ВК/ФТ.	KYC/EDD клієнтів; реєстри аудиторів/бухгалтерів; комерційні аналітичні платформи; OSINT.	Виявлення професійного посередника, який повторюється у ризикових кейсах (STR/SAR, високий risk-score клієнтів) протягом визначеного періоду.
PI-PII-002	Адвокатське бюро або адвокатське об'єднання використовується як сервісний вузол для управління активами, номінального володіння або транзиту коштів.	KYC/EDD; договори з клієнтами; судові реєстри; OSINT.	Виявлення ролі адвокатського утворення як бенефіціарного/контрольного вузла без очевидної правової необхідності.

Група: TECH; Категорія: зловживання цифровою ідентичністю – digital identity misuse (DI)

Код індикатора	Назва індикатора	Можливі джерела інформації (для автоматизації; перелік не обмежує використання інших джерел)	Можливі алгоритми виявлення
PI-DI-001	Відкриття рахунку за результатами дистанційної (відео) ідентифікації з ознаками використання AI-підробки або deepfake.	Системи відеоідентифікації; AI-liveness detection; biometric score; KYC/EDD; журнали ідентифікації.	Аналіз результатів liveness-перевірки та AI-детекції. У разі фіксації низького рівня живості, ознак синтетичного обличчя або маніпуляцій із

			відеопотоком система формує високий ризик зловживання цифровою ідентичністю.
PI-DI-002	Збіг фото-, біометричних або поведінкових даних (обличчя, підпис, голос) у кількох клієнтів.	Біометричні бази банку; біометричне зіставлення обличчя або голосу (face/voice matching); аналіз поведінкових характеристик користувача (behavioral biometrics); міжбанківський обмін.	Виявлення збігу біометричних шаблонів між різними клієнтськими профілями понад встановлений поріг схожості – автоматичне формування ризик-маркера повторного використання ідентичності.
PI-DI-003	Ознаки крадіжки або захоплення цифрової ідентичності клієнта.	Звернення клієнтів; fraud-кейси; поведінкова аналітика; device/IP-логи; повідомлення інших банків.	Різка зміна поведінкових і технічних параметрів доступу (пристрої, IP, геолокація) у поєднанні зі зверненням клієнта або зовнішнім повідомленням – високий ризик зловживання цифровою ідентичністю.
PI-DI-004	Багаторазові спроби проходження дистанційної ідентифікації з різних пристроїв або IP-адрес.	Логи ідентифікації; device fingerprinting; IP-аналіз; системи antifraud.	Фіксація багаторазових спроб проходження дистанційної ідентифікації протягом короткого проміжку часу з різних пристроїв або IP-адрес.
PI-DI-005	Спроби входу, ідентифікації або верифікації з території держав, що здійснюють військову агресію проти України.	GeoIP-бази; санкційні списки; SOC.	Виявлення доступу або спроб ідентифікації з високоризикових юрисдикцій.

Група: CRIME; Категорія: кримінальна причетність особи – criminal involvement (CIN)

Код індикатора	Назва індикатора	Можливі джерела інформації (для автоматизації; перелік не обмежує використання інших джерел)	Можливі алгоритми виявлення
PI-CIN-001	Участь або фігурування особи у кримінальних провадженнях (за виключенням випадків згадування банківських установ та фінансових компаній).	Повідомлення правоохоронних органів; судові реєстри.	Виявлення згадки особи у кримінальному провадженні.
PI-CIN-002	Родинні зв'язки з особами, причетними до злочинної діяльності.	Повідомлення правоохоронних органів; судові реєстри; KYC/EDD; граф-аналіз.	Встановлення підтверджених родинних зв'язків із фігурантами кримінальних справ.
PI-CIN-003	Пов'язаність з організованими злочинними групами.	Повідомлення правоохоронних органів; OSINT.	Виявлення зв'язків із ОЗГ за офіційними або підтвердженими джерелами.
PI-CIN-004	Причетність до корупційних злочинів.	Судові рішення; НАЗК; Повідомлення правоохоронних органів.	Фіксація корупційних правопорушень або проваджень.
PI-CIN-005	Причетність особи до легалізації (відмивання) майна, одержаного злочинним шляхом, відповідно до статті 209 Кримінального кодексу України.	Судові рішення; Повідомлення правоохоронних органів.	Виявлення кримінальних проваджень або судових справ щодо особи.
PI-CIN-006	Причетність до кримінальних правопорушень проти основ національної безпеки України (Розділ I КК України).	Повідомлення правоохоронних органів; судові реєстри; OSINT.	Виявлення кримінальних проваджень або судових справ за статтями відповідного розділу КК України щодо особи.

PI-CIN-007	Причетність до кримінальних правопорушень проти життя та здоров'я особи (Розділ II КК України).	Повідомлення правоохоронних органів; судові реєстри; OSINT.	Виявлення кримінальних проваджень або судових справ за статтями відповідного розділу КК України щодо особи.
PI-CIN-008	Причетність до кримінальних правопорушень проти волі, честі та гідності особи (Розділ III КК України).	Повідомлення правоохоронних органів; судові реєстри; OSINT.	Виявлення кримінальних проваджень або судових справ за статтями відповідного розділу КК України щодо особи.
PI-CIN-009	Причетність до кримінальних правопорушень проти статевої свободи та статевої недоторканості особи (Розділ IV КК України).	Повідомлення правоохоронних органів; судові реєстри; OSINT.	Виявлення кримінальних проваджень або судових справ за статтями відповідного розділу КК України щодо особи.
PI-CIN-010	Причетність до кримінальних правопорушень проти виборчих, трудових та інших прав і свобод людини і громадянина (Розділ V КК України).	Повідомлення правоохоронних органів; судові реєстри; OSINT.	Виявлення кримінальних проваджень або судових справ за статтями відповідного розділу КК України щодо особи.
PI-CIN-011	Причетність до кримінальних правопорушень проти власності (Розділ VI КК України).	Повідомлення правоохоронних органів; судові реєстри; OSINT.	Виявлення кримінальних проваджень або судових справ за статтями відповідного розділу КК України щодо особи.
PI-CIN-012	Підозра у вчиненні економічних злочинів (кримінальні правопорушення, передбачені Розділом VII КК України — у сфері господарської діяльності).	Повідомлення правоохоронних органів; судові реєстри; OSINT.	Виявлення кримінальних проваджень або судових справ за статтями відповідного розділу КК України щодо особи.
PI-CIN-013	Причетність до кримінальних правопорушень проти довкілля (Розділ VIII	Повідомлення правоохоронних органів; судові реєстри; OSINT.	Виявлення кримінальних проваджень або судових справ за

	КК України).		статтями відповідного розділу КК України щодо особи.
PI-CIN-014	Причетність до кримінальних правопорушень проти громадської безпеки (Розділ IX КК України).	Повідомлення правоохоронних органів; судові реєстри; OSINT.	Виявлення кримінальних проваджень або судових справ за статтями відповідного розділу КК України щодо особи.
PI-CIN-015	Причетність до кримінальних правопорушень проти безпеки виробництва (Розділ X КК України).	Повідомлення правоохоронних органів; судові реєстри; OSINT.	Виявлення кримінальних проваджень або судових справ за статтями відповідного розділу КК України щодо особи.
PI-CIN-016	Причетність до кримінальних правопорушень проти громадського порядку та моральності (Розділ XII КК України).	Повідомлення правоохоронних органів; судові реєстри; OSINT.	Виявлення кримінальних проваджень або судових справ за статтями відповідного розділу КК України щодо особи.
PI-CIN-017	Причетність до кримінальних правопорушень у сфері обігу наркотичних засобів, психотропних речовин та проти здоров'я населення (Розділ XIII КК України).	Повідомлення правоохоронних органів; судові реєстри; OSINT.	Виявлення кримінальних проваджень або судових справ за статтями відповідного розділу КК України щодо особи.
PI-CIN-018	Причетність до кримінальних правопорушень у сфері охорони державної таємниці, недоторканності державних кордонів та мобілізації (Розділ XIV КК України).	Повідомлення правоохоронних органів; судові реєстри; OSINT.	Виявлення кримінальних проваджень або судових справ за статтями відповідного розділу КК України щодо особи.
PI-CIN-019	Причетність до кримінальних правопорушень проти авторитету органів державної влади,	Повідомлення правоохоронних органів; судові реєстри; OSINT.	Виявлення кримінальних проваджень або судових справ за статтями

	органів місцевого самоврядування та журналістів (Розділ XV КК України).		відповідного розділу КК України щодо особи.
PI-CIN-020	Причетність до кримінальних правопорушень у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж (Розділ XVI КК України).	Повідомлення правоохоронних органів; судові реєстри; OSINT.	Виявлення кримінальних проваджень або судових справ за статтями відповідного розділу КК України щодо особи.
PI-CIN-021	Причетність до кримінальних правопорушень у сфері службової діяльності та професійної діяльності, пов'язаної з наданням публічних послуг (Розділ XVII КК України).	Повідомлення правоохоронних органів; судові реєстри; OSINT.	Виявлення кримінальних проваджень або судових справ за статтями відповідного розділу КК України щодо особи.
PI-CIN-022	Причетність до кримінальних правопорушень проти правосуддя (Розділ XVIII КК України).	Повідомлення правоохоронних органів; судові реєстри; OSINT.	Виявлення кримінальних проваджень або судових справ за статтями відповідного розділу КК України щодо особи.
PI-CIN-023	Причетність до військових кримінальних правопорушень (Розділ XIX КК України).	Повідомлення правоохоронних органів; судові реєстри; OSINT.	Виявлення кримінальних проваджень або судових справ за статтями відповідного розділу КК України щодо особи.
PI-CIN-024	Причетність до кримінальних правопорушень проти миру, безпеки людства та міжнародного правопорядку (Розділ XX КК України).	Повідомлення правоохоронних органів; судові реєстри; OSINT.	Виявлення кримінальних проваджень або судових справ за статтями відповідного розділу КК України щодо особи.

Застереження. В Єдиному державному реєстрі судових рішень можуть міститися численні згадки про банківські установи та фінансові компанії, однак їхня поява у судових матеріалах здебільшого має довідковий характер. Такі суб'єкти можуть фігурувати у різних процесуальних статусах – як учасники цивільних спорів, сторони господарських проваджень, заявники чи треті особи, що не завжди пов'язано з ризиками ВК/ФТ.

Під час аналізу таких згадок Аналітичні системи повинні враховувати специфічний статус суб'єктів, піднаглядних Національному банку України, та інтерпретувати дані з урахуванням повного контексту. Сам факт фігурування фінансового посередника в судових документах не може автоматично підвищувати рівень ризику без оцінки змісту рішення, характеру справи та відповідних індикаторів.

Група: CRIME; Категорія: Кіберзлочинність – Cybercrime (CYB)

Код індикатора	Назва індикатора	Можливі джерела інформації (для автоматизації; перелік не обмежує використання інших джерел)	Можливі алгоритми виявлення
PI-CYB-001	Щодо особи наявна інформація про співпрацю з даркнет-майданчиками.	Повідомлення правоохоронних органів; судові рішення.	Виявлено згадку особи у матеріалах правоохоронних органів або судових рішеннях як пов'язаної з даркнет-майданчиками.
PI-CYB-002	Використання особою даркнет-платформ або прихованих сервісів для здійснення незаконної діяльності.	Повідомлення правоохоронних органів; судові рішення.	Зафіксовано використання особою даркнет-платформ або прихованих сервісів у кримінальних матеріалах.
PI-CYB-003	Наявна інформація про участь особи у кіберзлочинних форумах, маркетплейсах або закритих онлайн-спільнотах.	Повідомлення правоохоронних органів; судові рішення.	Особу ідентифіковано як учасника кіберзлочинних форумів або онлайн-спільнот.
PI-CYB-004	Кореляція особи з кіберінцидентами, витоками даних або поширенням шкідливого ПЗ.	Дані правоохоронних органів; судові рішення.	Встановлено зв'язок особи з кіберінцидентами, витоками даних або шкідливим ПЗ.

PI-CYB-005	Ознаки залучення особи до обігу викрадених даних, цифрових активів або незаконних онлайн-сервісів.	Повідомлення правоохоронних органів; судові рішення.	Наявна інформація про участь особи в обігу викрадених даних або цифрових активів.
PI-CYB-006	Згадки особи в OSINT або матеріалах правоохоронних органів як учасника кіберзлочинної діяльності.	Повідомлення правоохоронних органів; судові рішення; OSINT.	Підтверджена згадка особи в OSINT або матеріалах правоохоронних органів як кіберзлочинця.

Група: CRIME; Категорія: шахрайство – Fraud (FR)

Код індикатора	Назва індикатора	Можливі джерела інформації (для автоматизації; перелік не обмежує використання інших джерел)	Можливі алгоритми виявлення
PI-FR-001	Відмова клієнта надати документи або інформацію, що підтверджують джерело походження коштів та/або мету фінансових операцій.	KYC/EDD-анкети; запити банку до клієнта; внутрішні системи банку (облік взаємодії з клієнтом); журнал комунікацій з клієнтом (фіксація контактів і відповідей).	У разі, якщо банком направлено клієнту запит на надання документів або інформації для підтвердження джерела походження коштів та/або мети фінансових операцій, і клієнт відмовився від їх надання або не надав такі документи у встановлений банком строк, система автоматично формує ознаку підвищеного ризику шахрайських дій клієнта.
PI-FR-002	Встановлення фактів надання клієнтом власних рахунків у користування третім особам (ознаки «дропа», «мула»).	Транзакційні дані; поведінкова аналітика; device/IP-аналіз; дані банківського моніторингу; повідомлення інших банків.	Масові операції з непов’язаними контрагентами, швидкий вхід/вихід коштів і невідповідність технічних параметрів доступу

			– високий ризик шахрайства.
PI-FR-003	Наявність інформації про клієнта як учасника фінансових шахрайських схем у повідомленнях банків або повідомленнях державних чи правоохоронних органів.	Повідомлення інших банків; міжбанківський обмін; внутрішні blacklist/watchlist; OSINT; повідомлення правоохоронних органів.	У разі включення клієнта до переліку осіб, причетних до фінансових шахрайських схем, або отримання зовнішнього повідомлення від інших банків, платіжних систем чи уповноважених органів, система автоматично встановлює високий рівень ризику шахрайських дій клієнта.
PI-FR-004	Ознаки шахрайства із використанням соціальної інженерії (фішинг, вішинг, смішинг, BEC), у тому числі використання рахунку клієнта як транзитного.	Транзакційні дані; звернення клієнтів; повідомлення інших банків; платіжні системи; повідомлення правоохоронних органів.	Швидке надходження коштів від потерпілих осіб з подальшим оперативним перерахуванням, у поєднанні з повідомленнями про шахрайство.
PI-FR-005	Нетипова технічна поведінка доступу до рахунку клієнта (часті зміни пристроїв, IP-адрес).	Device fingerprinting; IP-логи; поведінкова аналітика.	Часті або різкі зміни пристроїв/геолокацій, нехарактерні для клієнта.
PI-FR-006	Невідповідність фінансової поведінки клієнта його віку, соціальному статусу або задекларованим доходам.	KYC/EDD-анкети; дані про доходи; транзакційна історія; OSINT.	Фінансова активність або залишки коштів, що істотно перевищують очікуваний рівень з урахуванням профілю клієнта.

PI-FR-007	Пов’язаність клієнта з іншими рахунками, за якими раніше фіксувалися шахрайські операції.	Граф-аналіз; міжбанківський обмін; внутрішні fraud-бази; аналітика пов’язаних осіб.	Виявлення фінансових, технічних або поведінкових зв’язків із рахунками, що використовувалися у шахрайських схемах.
PI-FR-008	Імітування офіційних вебсайтів або використання логотипів, назв і візуальної айдентики інших осіб (ознаки фішингу / шахрайства).	OSINT; реєстри ТМ та логотипів; соцмережі; скарги користувачів; дані правоохоронних органів.	Виявлення вебресурсу або сторінки в соцмережах, що імітує назву чи візуальну айдентику відомої особи/бренду.

Група: SOC; Категорія: неприбуткові організації – non-profit organizations (NP)

Код індикатора	Назва індикатора	Можливі джерела інформації (для автоматизації; перелік не обмежує використання інших джерел)	Можливі алгоритми виявлення
PI-NP-001	Відсутність у відкритих джерелах інформації про гуманітарні/благодійні проєкти та цілі зборів за відсутності обґрунтованих безпекових причин.	Офіційний сайт; соцмережі; OSINT.	Автоматичний OSINT-скан: відсутність згадок про проєкти або результати діяльності.
PI-NP-002	Небажання або відмова керівництва НПО надавати інформацію про учасників НПО, донорів або партнерів.	KYC/EDD.	Фіксація відмови або неповної відповіді на запит банку.
PI-NP-003	Концентрація управління НПО в однієї особи або пов’язаних осіб без належного внутрішнього контролю.	KYC; граф-аналіз.	Виявлення одноосібного контролю.
PI-NP-004	Інформація про зв’язки НПО або її керівників з терористичними, екстремістськими чи	Санкційні списки; повідомлення правоохоронних органів; OSINT.	Виявлення підтверджених фактів.

	злочинними угрупованнями.		
PI-NP-005	Пов’язаність НПО з особами або структурами під санкціями або у кримінальних провадженнях.	Санкційні списки; судові реєстри; міжвідомчий обмін.	Збіг із санкційними/кримінальними списками.
PI-NP-006	Співпраця НПО з юрисдикціями, які підтримують агресію проти України.	Переліки країн (юрисдикцій) підвищеного ризику; KYC.	Виявлення донорів або партнерів НПО, пов’язаних із юрисдикціями, що підтримують агресію проти України.

Група: SOC; Категорія: релігійні організації – religious organizations (RO)

Код індикатора	Назва індикатора	Можливі джерела інформації (для автоматизації; перелік не обмежує використання інших джерел)	Можливі алгоритми виявлення
PI-RO-001	Причетність релігійної організації до діяльності організації, забороненої в Україні, або пов’язаність з такою організацією.	Рішення судів; санкційні списки; повідомлення правоохоронних органів.	Виявлення релігійної організації або її керівних осіб у судових рішеннях, санкційних списках чи офіційних повідомленнях про заборону діяльності – автоматичне формування ризик-маркера з урахуванням підтвердженого статусу заборони.

Група: GEN; Категорія: загальні індикатори – general (GN)

Код індикатора	Назва індикатора	Можливі джерела інформації (для автоматизації; перелік не обмежує використання інших джерел)	Можливі алгоритми виявлення
PI-GN-001	Володіння фізичною особою значною кількістю банківських рахунків або платіжних карток без обґрунтованої потреби.	KYC/EDD; внутрішні банківські системи; перелік рахунків.	Виявлення кількості рахунків/карток понад встановлений поріг без поясненого призначення.
PI-GN-002	Невідповідність соціального статусу або віку особи обсягам і характеру фінансових операцій. Особи, які належать до соціально вразливих верств населення (студенти, пенсіонери) або отримують соціальну допомогу тощо. Особи зі спеціальним статусом (малозабезпечені, жебраки), або молодого (до 20 років), або похилого (після 75 років) віку.	KYC/EDD; дані про доходи; транзакційна історія.	Порівняння профілю клієнта (вік, статус, доходи) з фінансовою активністю.
PI-GN-003	Проживання фізичної особи на тимчасово окупованих територіях України.	KYC; адресні дані; офіційні переліки ТОТ.	Зіставлення адреси проживання з переліком ТОТ.
PI-GN-004	Розміщення виробничих або господарських потужностей на тимчасово окупованих територіях.	Реєстраційні дані; KYC ЮО; OSINT.	Виявлення локації активів/потужностей на ТОТ → підвищення рівня ризику.
PI-GN-005	Володіння або розпорядження активами, джерела набуття яких не підтверджені.	KYC/EDD; дані про доходи; транзакційна історія.	Відсутність підтверджених джерел походження активів при значних обсягах.
PI-GN-006	Зазначення виграшів як джерела походження коштів без належного підтвердження.	KYC.	Виявлення надходжень із посиланням на виграші без підтверджуючих

			документів.
PI-GN-007	Залучення неповнолітніх осіб до незаконної діяльності.	KYC/EDD; дані про доходи; транзакційна історія.	Порівняння профілю клієнта (вік, статус, доходи) з фінансовою активністю.
PI-GN-08	Участь в операціях клієнта значної кількості фізичних осіб - контрагентів.	KYC/EDD-профіль учасника (тип клієнта, заявлена діяльність, очікувана модель поведінки); Транзакційні журнали за рахунками (картками) учасника; Внутрішні AML-системи; Результати мережевого (графового) аналізу зв'язків учасника з іншими фізичними особами; Дані платіжних систем та P2P-переказів; OSINT (за потреби — для виявлення публічної діяльності, зборів коштів, «волонтерських» ініціатив без офіційного статусу).	Визначення учасника, який протягом встановленого періоду (наприклад, 30 днів) здійснює фінансові операції з ≥ X унікальними фізичними особами, що не відповідає його заявленому профілю або статусу.

Група: GEN; Категорія: документи – documents (DC)

Код індикатора	Назва індикатора	Можливі джерела інформації (для автоматизації; перелік не обмежує використання інших джерел)	Можливі алгоритми виявлення
PI-DC-001	Подані клієнтом документи містять суттєві помилки, суперечності або ознаки підробки чи маніпуляцій.	KYC/EDD-дані; судові рішення.	Виявлено невідповідності або ознаки підробки в документах клієнта під час KYC/EDD або наявні згадки у судових рішеннях.
PI-DC-002	Клієнт не надає або безпідставно відмовляється надати первинні документи, що пояснюють економічний зміст фінансових операцій.	KYC/EDD-дані; запити СПФМ.	Клієнт не надав запитані первинні документи у встановлений строк або без обґрунтованих причин.
PI-DC-003	Подання клієнтом сумнівних, неповних або неперевірюваних	KYC/EDD-дані.	Неможливо підтвердити походження коштів

	документів щодо походження подарунків, допомоги або коштів від родичів чи третіх осіб.		за наданими документами щодо подарунків або допомоги від родичів/третіх осіб.

5.4. Індикатори підозрілості фінансових операцій (діяльності) (ІО)

За результатами проведеного дослідження визначено основні індикатори підозрілості фінансових операцій (діяльності) (Indicators of Operations – IO), які застосовувалися у типових схемах легалізації (відмивання) злочинних доходів та фінансування тероризму.

З метою забезпечення системності та підвищення ефективності аналітичного опрацювання зазначені індикатори згруповано за тематичними напрямами, що відображають природу та характер ризиків ВК/ФТ. Також до кожного індикатора додано можливий алгоритм виявлення, що дозволяє автоматизувати процес їхнього застосування.

Запроваджена система групування дає змогу оперативно ідентифікувати ключові сфери ризику, виявляти типові моделі зловживань, а також підвищувати точність ризик-скорингу під час автоматизованого аналізу фінансових операцій.

Для уніфікації, автоматизації та подальшої інтеграції індикаторів підозрілості у внутрішні аналітичні системи суб’єктів фінансового моніторингу, зокрема у модулі ризик-скоринг-платформ, для кожного індикатора застосовується стандартизований кодовий формат. Такий підхід забезпечує можливість автоматичного групування, пошуку та актуалізації індикаторів за категоріями ризику.

Стандартизована система кодування дозволяє ефективно інтегрувати індикатори до баз даних, алгоритмів машинного навчання, аналітичних дашбордів і форматів звітності, що сприяє підвищенню точності виявлення підозрілих фінансових операцій та оперативності реагування суб’єктів фінансового моніторингу.

Класифікація індикаторів підозрілості фінансових операцій

Категорія	Група індикаторів підозрілості фінансових операцій
Геополітичні та санкційні ризики (Geopolitical and Sanctions Risks – GEO)	• WF – Фінансування війни. • SA – Санкції. • FC – ФО з фіктивними іноземними компаніями.
Державні кошти (Governmental and Budgetary Risks – GOV)	• BGCR – Бюджет/корупція.
Комерційні зловживання та податкові порушення (Business and Tax Abuse & Evasion Risks – BUS)	• TE – Ухилення від сплати податків. • FA – ФО з фіктивними учасниками. • RP – ФО пов'язаних осіб. • NM – Невідповідність фінансових операцій. • TO – Транзитні операції. • CO – Готівкові операції.
Кримінальні ризики – Criminal Risks (CRIME)	• FR – Шахрайство. • GB – Гральний бізнес (нелегальний/тіньовий). • CIN – Кримінальна причетність особи. • DC – Документи з ознаками підробки.
Соціальні та гуманітарні ризики (Social and Humanitarian Risks – SOC)	• NP – Неприбуткові організації. • MN – Неповнолітні особи.
Технологічні та кіберризики (Technological and Cyber Risks – TECH)	• CC – Криптовалюта. • AI – Використання штучного інтелекту та автоматизація.
Поведінкові та загальні ознаки підозрілості (General and Behavioral Indicators – GEN)	• GN – Загальні індикатори. • NC – Не співпрацює. • PD – Призначення платежу. • CB – Транскордонні операції.

На відміну від індикаторів підозрілості учасників, індикатори фінансових операцій фокусуються на динаміці руху коштів, їх економічній логіці, маршрутах, інструментах та поведінкових аномаліях, що дозволяє:

- виявляти приховані або замасковані схеми;
- здійснювати автоматизований ризик-скоринг операцій;
- зменшувати вплив людського фактора під час первинного відбору;
- забезпечувати своєчасне реагування суб'єктів фінансового моніторингу.

Індикатори ІО застосовуються як основа автоматизованого моніторингу, поєднуються між собою та з іншими категоріями індикаторів і формують єдину аналітичну модель виявлення ризиків ВК/ФТ/ФРЗМЗ.

Звертаємо увагу, що не всі індикатори (Red Flags) можуть бути автоматично ідентифіковані в інформаційних системах або за допомогою алгоритмів. Використання автоматизованих засобів виявлення ризиків має доповнюватися аналітичною роботою та експертною оцінкою з боку відповідальних підрозділів.

Обмеження автоматизованого виявлення індикаторів ризику:

Необхідність експертної оцінки

Деякі індикатори вимагають аналізу або професійного судження, яке не може бути автоматизованим (наприклад, оцінка економічної доцільності операції чи наявності реального бізнесу).

Відсутність необхідних даних у системах

У багатьох випадках інформація, необхідна для формування індикатора (зокрема, щодо структури власності, наявності персоналу, матеріально-технічної бази тощо), може бути недоступною, неструктурованою або відсутньою.

Нецифрова природа окремих критеріїв

Частина Red Flags ґрунтується на аналізі документів, умов контрактів, змісту переговорів чи інших нефінансових факторів, що потребують людського втручання.

Контекстуальність та складність формалізації

Деякі індикатори складно описати у вигляді чітких алгоритмів, оскільки їх наявність залежить від контексту, обставин здійснення операцій та поведінки контрагентів.

Водночас суб'єкти первинного фінансового моніторингу в межах власної системи управління ризиками мають можливість формувати, актуалізувати та застосовувати додаткові індикатори підозрілості й Red Flags з урахуванням специфіки своєї діяльності, профілю клієнтів і виявлених ризиків.

Група: GEO; Категорія: фінансування війни – war financing (WF)

Код індикатора	Назва індикатора	Можливі алгоритми виявлення
IO-WF-001	Фінансові операції, пов'язані з діяльністю незаконних збройних формувань або з суб'єктами країни-агресора.	1. Фінансова операція з контрагентом, пов'язаним із країною-агресором або ТОТ, щодо якого відсутні або неповні відомості в ЄДР. 2. Здійснення фінансової операції з контрагентом, щодо якого санкційний скринінг виявив прямий або опосередкований зв'язок із санкційним суб'єктом. 3. Здійснення транскордонної фінансової операції через транзитну юрисдикцію, нехарактерну для профілю клієнта та без очевидного економічного обґрунтування.
IO-WF-002	Здійснення операцій особами, які організовують, забезпечують та провокують військову агресію з боку росії.	1. Здійснення фінансової операції за участю особи, щодо якої за результатами OSINT-аналізу та/або офіційних джерел встановлено зв'язки з пропагандистськими або підконтрольними структурами, що залучені до організації, матеріального забезпечення або публічного сприяння військовій агресії рф.

IO-WF-003	Фінансові операцій на користь компаній-нерезидентів, які мають засновницькі або бізнесові зв'язки з суб'єктами росії, білорусі та інших агресорів.	1. Здійснення фінансової операції на користь компанії-нерезидента, щодо якої за результатами корпоративного та транзакційного аналізу встановлено наявність спільних кінцевих бенефіціарних власників або керівних осіб із суб'єктами рф, а також використання транзитних юрисдикцій без економічного обґрунтування.
IO-WF-004	Виведенням коштів через треті юрисдикції на рахунки компаній країни-агресора.	1. Здійснення фінансових операцій з виведення коштів через одну або кілька третіх (транзитних) юрисдикцій на рахунки компаній, зареєстрованих у країні-агресорі.
IO-WF-005	Транскордонні перекази до країни, про яку відомо, що вона підтримує (є нейтральною) збройну агресію росії.	1. Здійснення транскордонної фінансової операції на користь контрагента, розташованого в юрисдикції, яка відповідно до наявних оцінок ризиків використовується для підтримки або опосередкованого сприяння збройній агресії російської федерації, за відсутності очевидного економічного обґрунтування такої операції.
IO-WF-006	Еквайрингові операції на тимчасово окупованих територіях.	1. Здійснення еквайрингової операції з використанням платіжного термінала або торгової точки, геолокація яких відповідає тимчасово окупованим територіям України, незалежно від заявленого місця реєстрації суб'єкта господарювання.
IO-WF-007	Операції з ресурсами, що походять з тимчасово окупованих територій (корисні копалини, метали, руда, зерно тощо).	1. Здійснення фінансової операції за товарами з використанням товарних кодів підвищеного ризику (корисні копалини, метали, руда, зерно тощо), щодо яких виявлено невідповідність між заявленим походженням товару та фактичними ознаками його походження з тимчасово окупованих територій.
IO-WF-008	Поведінкові шаблони, характерні для фінансування диверсійних груп.	1. Здійснення клієнтом серії P2P-переказів у часовому проміжку з 22:00 до 07:00 (за місцевим часом) або у вихідні/святкові дні, за умови відсутності такої активності в історичному профілі клієнта.
IO-WF-009	Використання онлайн-казино для маскування фінансування війни.	1. Фінансові операції через онлайн-казино/беттінг за участю осіб, які фігурують у повідомленнях правоохоронних органів щодо причетності до фінансування війни.
IO-WF-010	Використання карткових рахунків «дропів» для фінансування війни.	1. Використання карткових рахунків «дропів» у фінансових операціях осіб, що фігурують у повідомленнях правоохоронних органів щодо фінансування війни.

Група: GEO; Категорія: санкції – Sanctions (SA)

Код індикатора	Назва індикатора	Можливі алгоритми виявлення
IO-SA-001	Використання банківських карток підсанкційних банків.	1. Ініціювання фінансової операції з використанням платіжної картки, емітованої банком, включеним до санкційних списків.

Група: GEO; Категорія: ФО з фіктивними іноземними компаніями – Fake Companies (Foreign) (FC)

Код індикатора	Назва індикатора	Можливі алгоритми виявлення
IO-FC-001	Проведення підозрілих фінансових операцій з іноземною компанією, що має ознаки фіктивності або компанії-клон.	1. Транзитні фінансові операції з іноземною компанією без очевидної економічної мети. 2. Багаторазові перекази значних сум за зовнішньоекономічними контрактами без фактичного руху товарів або надання послуг. 3. Платежі за нематеріальні послуги (консалтинг, маркетинг, IT, ліцензії) без підтверджуючих документів або з формальними описами. 4. Швидке зарахування та подальше виведення коштів. 5. Використання рахунків іноземної компанії виключно як транзитних. 6. Дроблення платежів або нетипова періодичність операцій для уникнення контролю. 7. Розрахунки з компанією, реквізити якої імітують відомого міжнародного контрагента.
IO-FC-002	Проведення підозрілих фінансових операцій між резидентом України та підконтрольною іноземною компанією, кінцевий бенефіціарний власник якої має негативну фінансово-економічну історію.	1. Регулярні перекази коштів між резидентом України та підконтрольною іноземною компанією без пояснення. 2. Фінансові операції з ознаками виведення капіталу або штучного формування витрат. 3. Перерахування коштів за фіктивними або формальними договорами ЗЕД. 4. Циклічні фінансові потоки між пов’язаними рахунками. 5. Перекази коштів, що не відповідають фінансовому стану або офіційним доходам КБВ. 6. Використання іноземної компанії для обходу обмежень, санкцій або контролю за рухом коштів.

Група: GOV; Категорія: бюджет/корупція – budget-corruption (BGCR)

Код індикатора	Назва індикатора	Можливі алгоритми виявлення
IO-BGCR-001	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.	1. Масові або багаторазові перекази бюджетних коштів на рахунки значної кількості контрагентів без очевидного економічного зв'язку з предметом договору. 2. Перерахування коштів на суб'єктів з ознаками фіктивності, транзитності або короткого строку діяльності. 3. Дроблення сум бюджетних платежів з подальшим швидким виведенням коштів; 4. Перекази на рахунки фізичних осіб або ФОП, не залучених до виконання договору (фінансування бюджет). 5. Подальший транзит коштів через ланцюг пов'язаних осіб або компаній. 6. Відсутність підтвердження фактичного виконання робіт або надання послуг при активному русі коштів.
IO-BGCR-002	Відсутність розрахунків за товар, який в подальшому має бути поставлений на державне підприємство.	1. Відсутність або затримка платежів за товар при наявності авансування з бюджету. 2. Спрямування отриманих коштів на інші цілі, не пов'язані з закупівлею товару. 3. Багаторазове переміщення коштів між рахунками без формування платежів постачальникам. 4. Використання коштів для фінансування сторонньої господарської діяльності. 5. Відсутність кореляції між фінансовими операціями та графіком поставок.
IO-BGCR-003	Здійснення фінансових операцій з дороговартісними активами членами сімей високопосадовців та/або афільованими з ними особами.	1. Придбання або відчуження дороговартісних активів (нерухомості, транспортних засобів, корпоративних прав, цінних паперів) без підтверджених джерел походження коштів. 2. Використання готівкових коштів або складних платіжних схем при розрахунках за активи. 3. Оплата активів через посередників, третіх осіб або пов'язані компанії. 4. Заниження або завищення вартості активів порівняно з ринковою. 5. Багатоетапні або транзитні фінансові операції перед або після придбання активів. 6. Швидкий перепродаж активів без економічної доцільності.
IO-BGCR-004	Отримання/надання членами сімей високопосадовців та/або афільованими з	1. Отримання або надання значних сум коштів за послуги, характер, обсяг або вартість яких складно перевірити. 2. Платежі за нематеріальні або консультаційні послуги.

	ними особами значних коштів за послуги.	3. Невідповідність суми винагороди ринковим цінам або профілю діяльності сторін. 4. Перерахування коштів через ланцюг посередників або пов'язаних осіб. 5. Регулярні або системні платежі без зрозумілої ділової мети. 6. Швидке зняття або подальший транзит коштів після їх зарахування.
IO-BGCR-005	Придбання активів членами сімей високопосадовців та/або афілійованими з ними особами за рахунок подарованих або успадкованих коштів.	1. Операція (або сукупність операцій за період) на значну суму, де як підтвердження джерел походження коштів або статків зазначено «подарунок/дарування» або «спадщина». 2. Повторюваність таких пояснень у різних операціях клієнта. 3. Невідповідність суми та/або частоти операцій фінансовому профілю клієнта або задекларованим доходам. 4. Порівняння сум операцій з доходами та податковою інформацією (за наявності), а також з історичною активністю рахунків.

Група: BUS; Категорія: ухилення від сплати податків- tax evasion (TE)

Код індикатора	Назва індикатора	Можливі алгоритми виявлення
IO-TE-001	Фінансові операції, що не відповідають задекларованому обсягу доходів або виду діяльності платника податків.	1. Обороти за рахунками суттєво перевищують задекларовані доходи. 2. Регулярні надходження/витрати, не характерні для заявленого КВЕД. 3. Різкі стрибки оборотів без сезонних або бізнес-пояснень. 4. Значні платежі за послуги/товари, які у подальшому відсутні у податковій звітності. 5. Розбіжності між податковими періодами та фактичним рухом коштів.
IO-TE-002	Здійснення господарської діяльності без реєстрації платником ПДВ, попри наявність обсягів постачання, що перевищують встановлений поріг.	1. Стабільні надходження/обсяги постачання, що відповідають або перевищують поріг ПДВ, без платежів ПДВ. 2. Відсутність ПДВ у призначеннях платежів. 3. Використання посередників для маскування реальних обсягів.
IO-TE-003	Перерахування коштів на рахунки пов'язаних осіб або ФОПів, які не мають необхідних трудових/виробничих ресурсів для надання послуг чи виконання	1. Перерахування коштів ФОП/пов'язаним особам за роботи/послуги без наявності операційних витрат у них. 2. Циклічні платежі між пов'язаними рахунками. 3. Формальні призначення платежів за нематеріальні послуги.

	робіт, з ознаками фіктивності.	4. Швидке виведення коштів після зарахування.
IO-TE-004	Значна кількість операцій клієнта з суб'єктами щодо яких наявна інформація про ухилення від сплати податків, зборів (обов'язкових платежів).	1. Масові або регулярні платежі контрагентам з наявними податковими ризиками. 2. Транзитні ланцюги учасників з наявними податковими ризиками. 3. Відсутність реальних поставок/послуг при активних розрахунках. 4. Концентрація оборотів на вузькому колі ризикових учасників.
IO-TE-005	Перерахування коштів на підставі первинних документів із ознаками підробки або недостовірності.	1. Оплата за інвойсами/актами з формальними або повторюваними описами. 2. Невідповідність реквізитів документів платіжним даним. 3. Дублювання номерів/дат документів. 4. Розбіжності сум у документах і платежах. 5. Відсутність підтвердження виконання робіт/поставок.
IO-TE-006	Обготівковування коштів через транзитні компанії з ознаками «скруток» або без фактичного надання товарів/послуг.	1. Перерахування коштів на транзитні компанії з подальшим зняттям готівки. 2. Швидкий рух коштів без операційних витрат. 3. Дроблення платежів і короткі часові інтервали. 4. Відсутність підтвердження товарообігу/послуг. 5. Використання ланцюгів посередників для маскування обготівковування.

Група: BUS; Категорія: ФО з фіктивними учасниками – Fake Actors (FA)

Код індикатора	Назва індикатора	Можливі алгоритми виявлення
IO-FA-001	Використання новостворених суб'єктів господарювання або суб'єктів господарювання з ознаками «фіктивності» (клони).	1. Значні або регулярні фінансові операції з новоствореними суб'єктами без підтвердженої операційної діяльності. 2. Транзитні перекази коштів через суб'єктів без наявності операційних витрат. 3. Швидке нарощування оборотів одразу після реєстрації. 4. Короткий життєвий цикл рахунків із повним виведенням коштів.
IO-FA-002	Коригування дій учасників фінансових операцій («фіктивних» учасників) з єдиного центру прийняття рішення.	1. Синхронні або однотипні фінансові операції між різними учасниками у короткі проміжки часу. 2. Використання однакових сценаріїв платежів різними учасниками (суми, призначення, періодичність). 3. Одночасне відкриття рахунків і початок активних операцій різними учасниками, які мають у подальшому схожу фінансову

		діяльність. 4. Централізований рух коштів до/з одного або декількох контрольних рахунків. 5. Циклічні фінансові потоки між пов'язаними рахунками учасника.
IO-FA-003	Переказ коштів з одних і тих самих джерел на рахунки різних фізичних осіб або ФОПів, які мають спільні ознаки (телефон, IP, адреса реєстрації, пристрій входу тощо).	1. Перекази коштів з одного або обмеженої кількості джерел на рахунки багатьох фізичних осіб/ФОПів. 2. Однакові або схожі суми та призначення платежів. 3. Швидке виведення коштів після зарахування. 4. Концентрація коштів на окремих рахунках. 5. Відсутність підтвердженої економічної ролі таких отримувачів у операціях.
IO-FA-004	Швидкий обіг значних сум коштів рахунками фізичних осіб або ФОПів із повним виведенням коштів з рахунку протягом доби без підтвердження економічної суті операцій чи джерела походження коштів (за винятком випадків документально підтвердженої господарської діяльності).	1. Повне або майже повне виведення коштів протягом 24 годин після зарахування. 2. Дроблення сум та багаторазові однотипні операції. 3. Відсутність документального підтвердження економічної суті операцій або джерел походження коштів (за винятком підтвердженої господарської діяльності).

Група: BUS; Категорія: ФО пов'язаних осіб - Related Parties (RP)

Код індикатора	Назва індикатора	Можливі алгоритми виявлення
IO-RP-001	Проведення сумнівних фінансових операцій між групою юридичних осіб, які розташовані за адресами масової реєстрації.	1. Регулярні або значні перекази коштів між юридичними особами з адресами масової реєстрації. 2. Транзитні фінансові операції без формування операційних витрат. 3. Циклічні або зворотні перекази між особами. 4. Використання однакових призначень платежів та сум. 5. Швидке виведення коштів з рахунку після зарахування.

IO-RP-002	Проведення сумнівних фінансових операцій між групою фізичних та/або юридичних осіб, які розташовані за спільними адресами чи мають інші спільні риси.	1. Регулярні або масові перекази коштів між фізичними та/або юридичними особами, що мають спільну адресу реєстрації / проживання, без очевидної економічної мети. 2. Однотипні фінансові операції (суми, призначення, періодичність) між учасниками зі спільними ідентифікаційними ознаками. 3. Циклічні перекази коштів між такими особами з мінімальними або нульовими залишками на рахунках. 4. Транзитний характер операцій: швидке зарахування коштів та їх подальше перерахування між пов'язаними учасниками. 5. Розпорошення коштів між групою осіб зі спільними ознаками з подальшою концентрацією на одному або кількох рахунках. 6. Перекази між різними особами зі спільними контактними даними (телефон, e-mail, пристрій доступу). 7. Невідповідність характеру операцій заявленій діяльності або фінансовому профілю учасників.
IO-RP-003	Фінансові операції, проведені між учасниками, які пов'язані між собою спільним посадово-засновницьким складом та метою їх операцій є маскування джерел походження коштів.	1. Багатоетапні або ланцюгові перекази між компаніями зі спільними директорами/засновниками. 2. Циклічні фінансові потоки (round-tripping). 3. Формальні або штучні підстави платежів. 4. Використання посередників без операційної необхідності. 5. Невідповідність характеру операцій профілю діяльності учасників.
IO-RP-004	Використання афілійованих банківських установ для розрахунків.	1. Концентрація розрахунків через обмежене коло афілійованих банків. 2. Нетипові маршрути платежів без економічної. доцільності. 3. Прискорений транзит коштів між рахунками у пов'язаних банках. 4. Обходження стандартних процедур фінансового. контролю. 5. Багаторазові операції з однаковими параметрами.

Група: BUS; Категорія: невідповідність ФО – Non-Matching (NM)

Код індикатора	Назва індикатора	Можливі алгоритми виявлення
IO-NM-001	Фінансові операції клієнта не відповідають ризик профілю клієнта.	1. Обороти, суми або частота операцій не корелюють із заявленим профілем. 2. Нетипові для клієнта інструменти/канали платежів. 3. Різкі зміни поведінки клієнта без бізнес-пояснень.
IO-NM-002	Структуровані платежі.	1. Дроблення сум на серії близьких за величиною операцій. 2. Повторювані платежі у короткі інтервали. 3. Обхід порогів контролю за сумою операції.
IO-NM-003	Платежі без найменування конкретного товару/послуги.	1. Формальні або загальні призначення («послуги», «оплата»). 2. Відсутність деталізації при регулярних платежах. 3. Розбіжності між призначенням і характером операцій.
IO-NM-004	Придбання високовартісних активів із непідтверджених джерел.	1. Оплата високовартісного активу без належного документального підтвердження джерел походження коштів. 2. Придбання активу, вартість якого не відповідає фінансовому профілю клієнта, за умови що джерелом коштів для розрахунку (повністю або переважно) є готівка, а через одну банківську установу здійснюється лише часткова оплата.
IO-NM-005	Проведення фінансових операцій, які не мають очевидної мети.	1. Фінансові операції без зрозумілої економічної логіки. 2. Циклічні фінансові потоки. 3. Відсутність зв’язку з діяльністю клієнта.
IO-NM-006	Проведення фінансових операцій зі значною кількістю контрагентів (невідповідність діяльності учасників операцій, розпорошення активів з метою приховування фінансових потоків).	1. Масові перекази коштів на користь значної кількості різних контрагентів протягом короткого проміжку часу без очевидної економічної мети. 2. Розпорошення коштів між великою кількістю контрагентів з подальшою концентрацією на окремих рахунках. 3. Однотипні або близькі за сумами платежі різним контрагентам із повторюваними або шаблонними призначеннями. 4. Невідповідність контрагентів заявленій діяльності клієнта (відсутність логічного зв’язку між видом діяльності та роллю отримувачів). 5. Швидкий подальший транзит коштів контрагентами після їх отримання (ознаки посередництва або дропів). 6. Різке збільшення кількості контрагентів без зміни бізнес-моделі або масштабів діяльності.

		7. Регулярні циклічні платежі між одними й тими самими групами контрагентів з мінімальними залишками на рахунках. 8. Залучення фізичних осіб або ФОПів у ролі отримувачів коштів без підтвердженої участі у господарській діяльності клієнта. 9. Дроблення платежів між багатьма контрагентами для уникнення порогів контролю.
IO-NM-007	Проведення необґрунтовано великої кількості операцій з використанням рахунків, у т.ч. карткових.	1. Надмірна кількість транзакцій за короткий час.
IO-NM-008	Здійснення операцій з переказу на картки великої кількості фізичних осіб без деталізації призначень платежів.	1. Перекази на картки багатьох ФО без деталізації (однакові суми/періодичність. швидке зняття або транзит).
IO-NM-009	Проведення необґрунтовано великої кількості операцій або на значні суми між фізичною особою та суб'єктами грального бізнесу.	1. Висока частота операцій між фізичною особою та гральними платформами протягом короткого періоду (доба/тиждень), що не відповідає фінансовому стану клієнта. 2. Значні сукупні суми переказів на користь грального бізнесу. 3. Циклічні операції «поповнення – виплата – повторне поповнення» без перерв, характерні для маскування транзиту коштів. 4. Дроблення платежів на серії невеликих сум на користь гральних платформ з метою уникнення контролю. 5. Використання кількох гральних операторів або платіжних посередників для здійснення однотипних операцій. 6. Швидке зарахування виграшів з подальшим негайним переказом або зняттям коштів. 7. Невідповідність між активністю в гральному бізнесі та відсутністю інших операційних витрат (зарплата, побут, податки). 8. Різкий сплеск гральних операцій після надходження коштів із сумнівних або транзитних джерел. 9. Використання рахунку як проміжного для подальшого перерозподілу коштів через гральні платформи.

IO-NM-010	Здійснення операцій з готівкою, обсяг яких не відповідає офіційно задекларованим доходам.	1. Значні зняття/внесення готівки. 2. Відсутність задекларованих доходів. 3. Дроблення готівкових операцій.
IO-NM-011	Фінансові операції не мають законних джерел походження коштів.	1. Надходження коштів без підтвердження джерел. 2. Транзит коштів одразу після зарахування. 3. Невідповідність сукупності фінансових операцій фінансовому стану клієнта.
IO-NM-012	Аномальний сплеск проведення фінансових операцій по рахунках.	1. Різке зростання оборотів/кількості. 2. Короткочасні «піки».
IO-NM-013	Проведення фінансових операцій пов'язаних з торгівлею корисними копалинами без наявності дозволів та ліцензій на їх видобуток або не підтвердження джерела таких копалин.	1. Платежі за корисні копалини (пісок, щебінь, глина, бурштин, руда тощо) без наявності підтверджених ліцензій/дозволів у платника або отримувача. 2. Регулярні або значні перекази коштів за сировину при відсутності документально підтвердженого походження корисних копалин. 3. Формальні або узагальнені призначення платежів («сировина», «матеріали», «продукція») без зазначення родовища, обсягу або виду копалин. 4. Невідповідність обсягів фінансових операцій заявленим виробничим потужностям або масштабам діяльності контрагентів. 5. Використання посередників або ланцюгів компаній для розрахунків за корисні копалини без економічної доцільності. 6. Транзитний характер операцій (швидке зарахування та подальше виведення коштів) при розрахунках за копалини. 7. Розрахунки з контрагентами з регіонів підвищеного ризику або територій, де поширений нелегальний видобуток. 8. Заниження або завищення вартості корисних копалин порівняно з ринковими цінами без обґрунтування. 9. Відсутність кореляції між фінансовими операціями та логістичними витратами (транспортування, зберігання, перевалка), притаманними торгівлі сировиною.

IO-NM-014	Мета переказів є неочевидною або носить незвичний характер.	1. Призначення платежу є розмитим, загальним або формальним («переказ коштів», «фінансова допомога», «розрахунки», «інші послуги») без розкриття економічної суті операції. 2. Часті зміни призначень платежів між однотипними фінансовими операціями без пояснення або логічного зв'язку. 3. Невідповідність між призначенням платежу та характером руху коштів (наприклад, «оплата послуг» із негайним транзитом або зняттям готівки). 4. Однакові або майже ідентичні призначення платежів при переказах між різними контрагентами без очевидної спільної мети. 5. Призначення платежів не відповідає профілю діяльності платника або отримувача (КВЕД, звичайна фінансова поведінка). 6 Застосування нетипових або незрозумілих формулювань, абревіатур, кодів, іноземних слів без пояснення. 7. Відсутність кореляції між вхідними та вихідними операціями за рахунком (на вході – одне призначення, на виході – інше, без логічного зв'язку). 9. Масові перекази з однаковою «неочевидною» метою протягом короткого періоду часу.
IO-NM-015	Отримання великої кількості платежів на свої рахунки від систем, що забезпечують проведення онлайн-платежів, за умови відсутності діяльності, пов'язаної з онлайн-маркетингом/аукціонами, або подібної діяльності.	1. Регулярні або масові надходження коштів від платіжних систем/еквайрингу за відсутності задекларованої онлайн-діяльності (маркетплейси, аукціони, e-commerce). 2. Висока частота дрібних або середніх платежів від великої кількості платників із однотипними або формальними призначеннями. 3. Невідповідність характеру надходжень заявленому виду діяльності (КВЕД) та відсутність витрат, притаманних онлайн-бізнесу (реклама, хостинг, логістика, повернення). 4. Швидкий транзит або обнулення коштів після зарахування з платіжних систем (ознаки посередництва/дроп-рахунку). 5. Раптовий початок або різкий сплеск надходжень від онлайн-платежів без запуску сайту/кабінету продавця чи маркетингової активності. 6. Використання кількох платіжних систем одночасно з ідентичними шаблонами надходжень (суми, час, призначення).

		7. Відсутність або мінімальна публічна присутність (сайт, сторінки продавця, оферта, політики), що корелює з активними онлайн-надходженнями. 8. Масові повернення/chargeback або повторні списання за схожими сценаріями. 9. Надходження з різних юрисдикцій без пояснення міжнародної онлайн-діяльності. 10. Подальша концентрація коштів на пов'язаних рахунках або виведення через готівку/віртуальні активи після зарахування від PSP.

Група: BUS; Категорія: транзит – Transit Operations (TO)

Код індикатора	Назва індикатора	Можливі алгоритми виявлення
IO-TO-001	Транзитне проходження безготівкових коштів за рахунком (протягом короткого проміжку часу). Вхідний та вихідний залишок після проходження коштів за рахунком є мінімальним та/або нульовим.	1. Зарахування коштів на рахунок клієнта та їх подальше перерахування протягом короткого часу (години/доба). 2. Мінімальний або нульовий залишок на рахунку після проведення операцій. 3. Відсутність операційних витрат (податки, оренда, зарплата). 4. Однотипні суми та призначення платежів. 5. Використання рахунку виключно як проміжної ланки.
IO-TO-002	Невідповідність отриманих доходів з обсягами проведених фінансових операцій.	1. Значні обороти при низькому або відсутньому задекларованому доході. 2. Розбіжності між надходженнями та фінансовим результатом. 3. Транзит коштів без відображення у звітності.
IO-TO-003	Спонтанні обороти по рахунках особи (значні за обсягами обороти або повна відсутність оборотів).	1. Раптове виникнення значних оборотів після тривалого періоду неактивності. 2. Різкі коливання обсягів операцій без сезонних або бізнес-пояснень. 3. Короткострокова активність із подальшим припиненням операцій. 4. Концентрація оборотів у вузьких часових інтервалах.
IO-TO-004	Великі щоденні обороти коштів з незначним сальдо на початок та кінець дня.	1. Щоденні значні надходження та списання при мінімальному початковому і кінцевому залишку. 2. Дроблення сум і багаторазові однотипні операції протягом дня. 3. Відсутність накопичення коштів, притаманного операційній діяльності.

Група: BUS; Категорія: готівка - Cash Operations (CO)

Код індикатора	Назва індикатора	Можливі алгоритми виявлення
IO-CO-001	Необґрунтоване в значних розмірах використання готівки для розрахунків.	1. Значні готівкові розрахунки при можливості безготівкових платежів. 2. Регулярні зняття/внесення готівки без економічного пояснення. 3. Дроблення готівкових сум для уникнення контролю. 4. Відсутність кореляції з операційними витратами клієнта.
IO-CO-002	Циклічний необґрунтований рух готівкових коштів за рахунком клієнта.	1. Повторювані цикли «зняття –внесення» у короткі строки. 2. Зарахування готівки на рахунок після транзиту через інших осіб. 3. Відсутність зміни фінансового результату при активному русі готівки. 4. Однакові суми та періодичність операцій.
IO-CO-003	Багаторазові зарахування готівкових коштів на карткові рахунки від невстановлених осіб.	1. Регулярні або масові зарахування готівки на картковий рахунок від різних невстановлених осіб протягом короткого періоду. 2. Однакові або близькі за розміром суми готівкових внесень, що повторюються з високою частотою. 3. Відсутність інформації про платників або неможливість ідентифікації осіб, які здійснюють готівкові внесення. 4. Швидке зняття готівки або подальший переказ коштів після їх зарахування на рахунок (ознаки транзитності). 5. Невідповідність обсягів готівкових надходжень фінансовому стану або задекларованим доходам власника рахунку. 6. Використання різних відділень банку / платіжних терміналів для внесення готівки без логічного пояснення. 7. Концентрація готівкових надходжень у певні дні або години, що може свідчити про організований характер операцій. 8. Відсутність цільового використання коштів (немає витрат на побут, зарплату, податки, послуги). 9. Поєднання готівкових внесень з іншими ризиковими ознаками (транзитні операції, дроблення). 10. Різке припинення готівкових надходжень після запитів банку/СПФМ або посилення контролю.

IO-CO-004	Внесення готівки з сумнівних джерел (не підтверджених).	1. Значні внесення готівки без підтверджених джерел походження. 2. Невідповідність сум задекларованим доходам. 3. Внесення готівки через різні відділення/термінали.
IO-CO-005	Проведення в значних обсягах фінансових операцій з готівкою, що не пов'язані з основним видом діяльності клієнта.	1. Готівкові обороти, не характерні для заявленої діяльності. 2. Концентрація готівкових операцій у короткі періоди. 3. Різка зміна структури розрахунків на користь готівки.
IO-CO-006	Фізичне переміщення готівки (кеш-кур'єри).	1. Часті внесення/зняття готівки у різних населених пунктах. 2. Короткі інтервали між операціями у віддалених локаціях. 3. Використання декількох рахунків/карток для готівкових операцій.
IO-CO-007	Зняття готівки або внесення на рахунки в різних країнах суб'єктами із зон конфліктів.	1. Готівкові операції у кількох країнах протягом короткого часу. 2. Нетипова географія готівкових операцій. 3. Швидкий транзит коштів після готівкових операцій.

Група: CRIME; Категорія: шахрайство – Fraud (FR)

Код індикатора	Назва індикатора	Можливі алгоритми виявлення
IO-FR-001	Множинні P2P-надходження з негайним транзитом/обготівковуванням, що не відповідають фінансовому профілю клієнта.	1. Надходження коштів від великої кількості фізичних осіб з подальшим швидким переказом або зняттям (ознаки масового шахрайства). 2. Масові однотипні платежі (суми, призначення, періодичність) від різних платників на один рахунок. 3. Раптовий сплеск активності за рахунком без зміни фінансового профілю клієнта. 4. Швидкий транзит коштів: зарахування – негайне перерахування третім особам або обготівковування. 5. Дроблення платежів для уникнення порогів фінансового контролю. 6. Нетипові або формальні призначення платежів, що часто змінюються та не мають економічної логіки. 7. Використання рахунку як проміжного (дроп-рахунку) без операційних витрат (зарплата, податки, побут). 8. Перекази коштів після зміни реквізитів доступу (телефон, e-mail, пароль, пристрій). 9. Географічні та часові аномалії (нетипові локації, нічні масові операції).

		10. Поєднання фінансових операцій із скаргами/зверненнями платників або блокуваннями з боку платіжних сервісів. 11. Подальша конвертація коштів у готівку, криптоактиви або перекази за кордон після масових надходжень.

Група: CRIME; Категорія: гральний бізнес (нелегальний / тіньовий) – Gambling (GB)

Код індикатора	Назва індикатора	Можливі алгоритми виявлення
IO-GB-001	Використання карток фізичних осіб для поповнення ігрових акаунтів незаконних казино в мережі Інтернет та інших неліцензованих платіжних сервісах.	1. Регулярні або масові карткові платежі (A2M/A2C) на користь відомих/ідентифікованих неліцензованих гральних платформ. 2. Дроблення сум і висока частота транзакцій у короткі проміжки часу. 3. Використання посередницьких платіжних сервісів/PSP для маскування призначення. 4. Швидкі зворотні виплати/виплати «виграшів» з подальшим транзитом або зняттям. 5. Географічні аномалії (еквайринг/мерчант за кордоном без пояснень). 6. Невідповідність обсягів операцій доходам платника.
IO-GB-002	Перерахування коштів на рахунки значної кількості суб'єктів господарювання, які працюють під нібито одним брендом онлайн казино (представники), у т.ч. за кордон.	1. Масові перекази на рахунки різних ЮО/ФОП, що декларують роботу під одним гральним брендом. 2. Однотипні призначення платежів та суми, регулярність. 3. Транзитні маршрути з подальшою концентрацією коштів. 4. Використання іноземних рахунків без економічного обґрунтування. 5. Відсутність кореляції між платежами та ліцензійним статусом отримувачів. 6. Швидке виведення коштів після зарахування.

Група: CRIME; Категорія: кримінальна причетність особи – criminal involvement (CIN)

Код індикатора	Назва індикатора	Можливі алгоритми виявлення
IO-CIN-001	Виявлення фінансових операцій, щодо яких наявна інформація про звернення постраждалих осіб до банківських установ та/або правоохоронних	1. Надходження до банку скарг клієнтів щодо несанкціонованих або спірних фінансових операцій. 2. Звернення постраждалих осіб до правоохоронних органів із зазначенням реквізитів конкретних рахунків або транзакцій.

	органів з повідомленнями про шахрайські дії, незаконне списання коштів, введення в оману або інше протиправне заволодіння коштами.	3. Численні звернення різних осіб щодо операцій з одними й тими самими контрагентами, рахунками або платіжними інструментами. 4. Оскарження клієнтами платежів, що мають ознаки шахрайства. 5. Здійснення операцій із використанням карток, рахунків або платіжних сервісів, щодо яких уже зафіксовані заяви постраждалих. 6. Невідповідність пояснень клієнта характеру та обсягу здійснених фінансових операцій після надходження скарги.
IO-CIN-002	Виявлення фінансових операцій, у яких однією зі сторін є фізична, щодо якої правоохоронним органом прийнято рішення про оголошення в розшук.	1. Фінансові операції після оголошення правоохоронним органом особи у розшук.
IO-CIN-003	Операції за участі суб’єктів із відкритими кримінальними провадженнями або судовими справами.	1. Здійснення фінансових операцій учасником, щодо якого відкрито кримінальне провадження або триває судове переслідування. 2. Проведення нетипових або підвищено ризикових фінансових операцій після дати відкриття кримінального провадження. 3. Транзитний характер операцій (швидке зарахування та подальше перерахування коштів) за участю особи, яка є фігурантом кримінального провадження. 4. Виведення активів (готівка, перекази на пов’язаних осіб, PSP, криптовалюта) на тлі слідчих або судових дій. 5. Використання посередників, підставних осіб або пов’язаних рахунків для здійснення фінансових операцій після появи інформації про кримінальне провадження. 6. Зміна структури фінансових потоків (нові рахунки, інші банки, інші платіжні інструменти) з метою ускладнення відстеження операцій.

Група: CRIME; Категорія: документи з ознаками підробки (DC)

Код індикатора	Назва індикатора	Можливі алгоритми виявлення
IO-DC-001	Наявність фактів щодо підробки або фальсифікації офіційних документів.	1. Перерахування коштів на підставі первинних документів (договорів, інвойсів, актів) з ознаками підробки або недостовірності. 2. Невідповідність реквізитів документів (дата, номер, сума, контрагент) даним платіжних операцій. 3. Дублювання номерів або шаблонів документів при різних фінансових операціях. 4. Використання формальних або однотипних документів для обґрунтування значних сум переказів. 5. Відсутність кореляції між документами та фактичним рухом товарів/наданням послуг. 6. Багаторазові платежі за документами, що не підтверджують реального економічного змісту операцій.

Група: SOC; Категорія: неприбуткові організації – non-profit organizations (NP)

Код індикатора	Назва індикатора	Можливі алгоритми виявлення
IO-NP-001	Подрібнення та структурування фінансових операцій, проведення фінансових операцій без належного пояснення суті таких операцій, проведення сумнівних фінансових операцій з використанням новітніх технологій (електронні гроші, криптоактиви).	1. Дроблення сум пожертв/переказів у короткі інтервали. 2. Структурування операцій без пояснення економічної мети. 3. Використання електронних грошей, криптоактивів без прозорої звітності. 4. Швидкий транзит коштів після зарахування. 5. Відсутність кореляції між надходженнями та заявленими програмами НПО.
IO-NP-002	Здійснення фінансової операції з виплати електронних переказів, у яких відсутня повна інформація про ініціатора або отримувача переказу.	1. Операції без повних даних про платника або отримувача. 2. Використання посередницьких платіжних сервісів для маскування сторін. 3. Повторювані платежі з мінімальними ідентифікаторами. 4. Подальший транзит або зняття коштів.
IO-NP-003	Необґрунтований переказ коштів на користь осіб, пов’язаних з НПО.	1. Регулярні перекази пов’язаним особам без підтвердженої ролі у проєктах. 2. Оплата послуг без результатів/звітів. 3. Завищені суми або циклічні платежі. 4. Швидке виведення коштів у готівку отримувачами.

IO-NP-004	Фінансові операції мають заплутаний характер.	1. Багатоетапні ланцюги переказів. 2. Часті зміни контрагентів/призначень. 3. Розпорошення коштів з подальшою концентрацією. 4. Відсутність прозорого зв'язку з цілями НПО.
IO-NP-005	Відсутність конкретизації платежів під час залучення коштів та при подальшому їх переказі.	1. Формальні призначення («допомога», «послуги»). 2. Відсутність деталізації як при зборі, так і при витрачанні коштів. 3. Невідповідність між описом збору та фактичними платежами. 4. Повторювані шаблонні формулювання.
IO-NP-006	Здійснення НПО фінансових операцій з призначенням платежів, що не стосуються благодійної діяльності.	1. Витрати на непрофільні послуги/товари. 2. Платежі, що не відповідають статутним цілям. 3. Регулярні непрофільні виплати без рішень/пояснень. 4. Виявлений транзит коштів через НПО.
IO-NP-007	Переказ коштів НПО на користь юридичних осіб, діяльність яких не відповідає суті фінансової операції (виду діяльності).	1. Платежі ЮО, КВЕД яких не відповідає суті операції. 2. Відсутність підтвердження виконання робіт/послуг. 3. Використання посередників без операційної необхідності. 4. Швидке виведення коштів отримувачем.
IO-NP-008	Здійснення переказів за послуги, вартість яких необґрунтована.	1. Завищені ціни порівняно з ринковими. 2. Відсутність конкурентних закупівель/обґрунтувань. 3. Формальні акти. 4. Повторювані виплати за однакові послуги.
IO-NP-009	Фінансові операції НПО не відповідають їх профілю діяльності.	1. Здійснення фінансових операцій, не пов'язаних зі статутною діяльністю НПО або заявленими програмами/проєктами. 2. Надходження або витрачання коштів без цільового призначення, передбаченого установчими документами. 3. Перерахування значних сум на користь фізичних осіб, ФОП або комерційних структур без обґрунтування та договорів. 4. Фінансування проєктів або контрагентів, інформація про які відсутня у відкритих джерелах або звітності НПО.

Група: SOC; Категорія: неповнолітні особи – Minor (MN)

Код індикатора	Назва індикатора	Можливі алгоритми виявлення
IO-MN-001	Наявність регулярних переказів великих сум, які перевищують звичайні потреби неповнолітньої особи. Часте поповнення рахунку неповнолітньої особи великими сумами, які не відповідають доходам родини та/або значно вищі за звичайні витрати на освіту, побут або дозвілля за віком особи.	1. Регулярні надходження великих сум, що перевищують типові витрати за віком. 2. Часте поповнення рахунку сумами, не корельованими з доходами родини. 3. Нетипові джерела надходжень або велика кількість платників.
IO-MN-002	Перекази, які проходять на значні суми через рахунок неповнолітнього та негайно пересилаються іншим одержувачам.	1. Швидке пересилання коштів на значні суми іншим одержувачам після зарахування. 2. Мінімальний або нульовий залишок після операцій. 3. Однотипні суми та призначення платежів. 4. Використання рахунку неповнолітнього як транзитного вузла. 5. Відсутність економічної або соціальної логіки операцій.

Група: TECH; Категорія: криптовалюта – crypto currency (CC)

Код індикатора	Назва індикатора	Можливі алгоритми виявлення
IO-CC-001	Здійснення розрахунків із використанням криптовалюти, особливо в рамках нетипових операцій або без очевидної доцільності.	1. Регулярна конвертація криптовалюти у фіатні кошти з подальшим швидким переказом або зняттям готівки. 2. Використання P2P-платформ, PSP або бірж для маскування призначення фінансових операцій. 3. Дроблення криптовалютних операцій на дрібні суми (structuring).
IO-CC-002	Транзитне перерахування криптовалютних активів між криптогаманцями, що не мають обґрунтування або супроводжуються дробленням.	1. Багатоетапні перекази між гаманцями у короткі проміжки часу. 2. Дроблення сум (peeling chains) з подальшою консолідацією. 3. Мінімальні залишки після транзакцій. 4. Відсутність економічної логіки маршрутів.

IO-CC-003	Фінансові операції клієнта з придбання криптовалюти за кошти сумнівного походження, зокрема за відсутності підтверджених джерел доходу.	1. Купівля криптовалюти за рахунок коштів без підтверджених джерел доходу. 2. Невідповідність обсягів купівлі фінансовому стану клієнта. 3. Попередні транзитні/готівкові операції перед купівлею. 4. Різкі піки купівель без пояснень.
IO-CC-004	Використання криптоплатформ, які не здійснюють належної ідентифікації користувачів (kyc) або перебувають у юрисдикціях із високим ризиком, а також транзакції через анонімні гаманці або «міксери».	1. Операції через платформи без KYC/AML або з високоризикових юрисдикцій. 2. Взаємодія з анонімними гаманцями, privacy-coins. 3. Використання міксерів/тумблерів, bridge-сервісів для маскування. 4. Повторні входи/виходи з однаковими патернами.
IO-CC-005	Операції з криптовалютними адресами, пов'язаними з даркнет-маркетплейсами.	1. Надходження/відправлення коштів на відомі даркнет-адреси. 2. Короткі цикли «купівля - переказ - обготівковування». 3. Дроблення та швидка зміна адрес. 4. Подальша конвертація у фіат або stablecoins.

Група: TECH; Категорія: використання ШІ та автоматизація - artificial intelligence (AI)

Код індикатора	Назва індикатора	Можливі алгоритми виявлення
IO-AI-001	Застосування автоматизованих фішингових атак, а також технологій deepfake для викрадення особистих даних або створення фальшивих цифрових ідентичностей.	1. Надходження коштів після скомпрометованої автентифікації або нетипових змін профілю. 2. Швидке виведення/переказ коштів після відновлення доступу або зміни реквізитів. 3. Операції, ініційовані після deepfake-ідентифікації (відео/аудіо) або масових фішингових кампаній. 4. Однотипні сценарії операцій, характерні для автоматизованих атак.
IO-AI-002	Аномальна або нестандартна поведінка клієнта під час проведення фінансових операцій, яка може свідчити про автоматизоване або несанкціоноване управління рахунком (наприклад, надто швидке введення даних,	1. Надто швидке введення даних та виконання команд. 2. Здійснення операцій у нетиповий для клієнта час (наприклад, уночі або у вихідні). 3. Одночасні дії з різних пристроїв/сесій. 4. Нетипова послідовність операцій без підтвердження користувачем.

	виконання нетипових команд).	
IO-AI-003	Раптова або систематична зміна геолокації проведення операцій, не характерна для історії активності клієнта, що може свідчити про використання VPN, бот-мереж або віддалений доступ.	1. Часті геострибки між країнами/регіонами у короткий час. 2. Невідповідність IP/гео історії клієнта. 3. Операції з високоризикових локацій. 4. Поєднання з швидкими транзитними переказами.
IO-AI-004	Масові одноманітні транзакції (від 10 і більше однотипних переказів) здійснені у короткий проміжок часу (до 1 хвилини). Наприклад, з використанням автоматичних скриптів / ботів.	1. ≥10 однотипних переказів протягом ≤1 хвилини. 2. Однакові суми та призначення платежів. 3. Повторювані ш «зарахування – переказ - обнулення». 4. Відсутність операційної логіки для такої інтенсивності.

Група: GEN; Категорія: загальні індикатори – General (GN)

Код індикатора	Назва індикатора	Можливі алгоритми виявлення
IO-GN-001	Значні суми перерахувань за надані послуги, вартість яких важко оцінити (агентські та рекламні послуги; послуги з підготовки документів, досліджень, з пошуку роботи тощо).	1. Значні платежі за агентські, рекламні, консалтингові, дослідницькі послуги. 2. Відсутність вимірюваного результату або підтвердження виконання. 3. Формальні або загальні призначення платежів. 4. Регулярність і повторюваність без бізнес-логіки.
IO-GN-002	Відсутність оплати за отримані від нерезидентів товари.	1. Імпорт товарів без відповідних платежів. 2. Тривалі розбіжності між поставками та розрахунками. 3. Нетипові схеми компенсації/заліків. 4. Використання посередників без економічної необхідності.
IO-GN-003	Відсутність операцій притаманних звичайній господарській діяльності (виплата заробітної плати, сплата податків і зборів, оренда плата тощо).	1. Відсутність або мінімальний обсяг обов’язкових регулярних платежів (оренда, комунальні послуги, податки, збори, заробітна плата) при наявності активних фінансових оборотів. 2. Здійснення значних надходжень і витрат без сплати податків або обов’язкових платежів у відповідних періодах. 3. Концентрація фінансових операцій на транзитних переказах без операційних

		витрат. 4. Систематичне перерахування коштів третім особам без формування витрат на забезпечення діяльності. 5. Різка зміна структури платежів із зникненням базових операційних витрат. 6. Невідповідність між масштабами фінансових операцій та фактичними витратами на ведення діяльності.
IO-GN-004	Значний обсяг фінансових операцій з надання / отримання фінансової допомоги.	1. Регулярні або великі суми «фінансової допомоги». 2. Відсутність договорів або умов повернення. 3. Циклічні або зворотні перекази. 4. Невідповідність фінансовому стану сторін.
IO-GN-005	Використання професійних мереж відмивання коштів для обходу санкцій.	1. Ланцюгові транзакції через посередників у різних юрисдикціях. 2. Повторювані маршрути платежів. 3. Швидка зміна контрагентів. 4. Розпорошення та подальша концентрація коштів.
IO-GN-006	Дроблення платежів між одними і тими ж учасниками фінансових операцій в один день.	1. Серії платежів із близькими сумами. 2. Короткі часові інтервали. 3. Обходження порогів контролю. 4. Відсутність операційної потреби.
IO-GN-007	Використання для доступу до он-лайн банкінгу різних осіб з одних і тих же IP-адрес.	1. Входи з одних IP/пристроїв до різних облікових записів. 2. Синхронні сесії. 3. Подальші транзитні операції. 4. Ознаки централізованого управління.
IO-GN-008	Відсутність або малоінформативність вебсайту.	1. Активні фінансові операції без публічної інформації про діяльність. 2. Сайт-«заглушка» або шаблонний контент. 3. Невідповідність між заявленими послугами і платежами.
IO-GN-009	Використання посередників в угодах.	1. Багатоетапні розрахунки через посередників. 2. Відсутність доданої вартості. 3. Збільшення вартості без пояснень. 4. Транзитний характер операцій.
IO-GN-010	Неодноразові фінансові операції за договорами відступлення прав вимоги (переведення боргу).	1. Часті переуступки/переведення боргу. 2. Використання як інструменту транзиту. 3. Відсутність економічної логіки. 4. Циклічність між пов’язаними особами.
IO-GN-011	Анонімне переміщення коштів.	1. Використання анонімних інструментів/посередників. 2. Мінімізація ідентифікаційних слідів. 3. Швидкі багаторівневі перекази. 4. Відсутність прозорого джерела/призначення.

Група: GEN; Категорія: не співпрацює - Non-Cooperation (NC)

Код індикатора	Назва індикатора	Можливі алгоритми виявлення
IO-NC-001	Учасник фінансової операції не надає пояснення щодо фінансових операцій та наявні ознаки щодо приховування джерел походження коштів.	1. Відмова або ухилення від надання пояснень щодо економічної мети операцій. 2. Ненадання або надання неповних/суперечливих документів. 3. Операції, не підтверджені джерелами походження коштів. 4. Транзитні або багатоетапні перекази без логічного обґрунтування. 5. Зміна поведінки клієнта після запитів СПФМ.
IO-NC-002	Після звернення СПФМ щодо надання документів та пояснень відкликав платіж та закрив рахунок.	1. Відкликання платежів або скасування операцій після звернення СПФМ. 2. Закриття рахунків одразу після запитів щодо документів/пояснень. 3. Спроби переміщення коштів на інші рахунки або до інших установ. 4. Різке припинення активності після періоду інтенсивних операцій.

Група: GEN; Категорія: призначення платежу - Payment Description (PD)

Код індикатора	Назва індикатора	Можливі алгоритми виявлення
IO-PD-001	Очевидна невідповідність призначень прибуткових та видаткових операцій за фінансовими операціями клієнта.	1. Різні за змістом призначення на вході та виході коштів без логічного зв’язку. 2. «Послуги» на вході – «фінансова допомога/повернення боргу» на виході. 3. Відсутність ланцюга економічної логіки між операціями. 4. Швидкий транзит після зарахування з іншим призначенням.
IO-PD-002	Зарахування та переказ коштів здійснюється з однаковим призначенням платежу із залученням широкого кола фізичних осіб без очевидної мети таких операцій.	1. Однакові призначення платежів від/на велику кількість ФО. 2. Однотипні суми та періодичність. 3. Відсутність очевидної мети або ролі фізичних осіб. 4. Подальше розпорошення або концентрація коштів.
IO-PD-003	Призначення платежу не відповідає звичній діяльності юридичної особи або фізичної особи-суб’єкта підприємницької діяльності.	1. Призначення, не характерні для заявленого виду діяльності (КВЕД). 2. Різка зміна типів призначень без бізнес-пояснень. 3. Поєднання непрофільних призначень із транзитними операціями. 4. Відсутність підтвердження виконання робіт/послуг за призначенням.

IO-PD-004	Нерозкриття інформації в призначенні платежу щодо підстав та мети переказу коштів.	1. Формальні або загальні формулювання («оплата», «послуги», «переказ коштів»). 2. Відсутність посилання на договір/контракт/інвойс/період/реквізити документів. 3. Повторювані шаблонні призначення при значних сумах.

Група: GEN; Категорія: транскордонні операції - Cross-Border Operations (CB)

Код індикатора	Назва індикатора	Можливі алгоритми виявлення
IO-CB-001	Цінові диспропорції у транскордонних операціях.	1. Здійснення транскордонної фінансової операції, за якою сума перерахованих за кордон коштів суттєво перевищує вартість фактично отриманих товарів, робіт або послуг.
IO-CB-002	Безпідставні регулярні транскордонні надходження.	1. Регулярне отримання або перерахування коштів з/за кордон без очевидної економічної мети та без зв'язку з основною діяльністю клієнта.
IO-CB-003	Операції з пов'язаними компаніями-нерезидентами.	1. Проведення транскордонних фінансових операцій за участю пов'язаних між собою компаній-нерезидентів з ознаками внутрішньогрупового або транзитного руху коштів.
IO-CB-004	Транзитні схеми через країни підвищеного ризику.	1. Здійснення міжнародних постачань або транскордонних платежів із транзитним переміщенням товарів чи коштів через країни підвищеного ризику без логістичного або економічного обґрунтування.
IO-CB-005	Операції з офшорними компаніями.	1. Перерахування коштів на рахунки офшорних компаній-нерезидентів без підтвердження реальної господарської діяльності або ділової мети операції.
IO-CB-006	Відсутність оплати або затримка оплати за імпортні поставки.	1. Відсутність або систематична несвоєчасність оплати за товари, роботи або послуги, фактично отримані від нерезидентів, за наявності договірних зобов'язань.
IO-CB-007	Операції з нерезидентами без економічної спроможності.	1. Перерахування коштів на користь нерезидентів, які не мають достатніх ресурсів (персоналу, приміщень, обладнання) для виконання умов укладених контрактів.
IO-CB-008	Переуступка боргу у транскордонних операціях.	1. Здійснення міжнародних постачань або фінансових операцій із подальшою переуступкою боргу чи прав вимоги на користь нерезидентів з інших юрисдикцій без економічної доцільності.

ІО-СВ-009	Псевдоінвестиційні та корпоративні операції.	1. Здійснення або повернення інвестицій, виплата дивідендів, купівля-продаж майнових прав чи відступлення прав вимоги з ознаками використання таких операцій для незаконного виведення коштів за кордон.

5.5. Найпоширеніші способи легалізації (відмивання) злочинних доходів

Результати дослідження Держфінмоніторингу засвідчують, що схеми легалізації злочинних доходів постійно змінюються, охоплюють різні сектори економіки та поєднують традиційні й цифрові фінансові інструменти.

Виявлені способи відмивання згруповано за типовими сценаріями та сферами ризику, що дає змогу чітко визначати характерні патерни поведінки та підсилювати ефективність протидії таким загрозам.

Нижче подано їх у згрупованому за тематикою вигляді:

Корупційні злочини та схеми відмивання злочинних доходів

- перерахування коштів з бюджетної установи на користь підприємства, яке підконтрольне політично значущій особі (PEP), шляхом оплати за послуги, вартість яких значно перевищує ринкову;
- отримання PEP коштів за фактично відсутні або штучно створені послуги з подальшим перерахуванням пов'язаним особам для придбання високовартісних товарів або обготівкування;
- часткове привласнення державних коштів компаніями-нерезидентами через ряд підконтрольних суб'єктів господарювання, що мають ознаки фіктивності, з подальшим придбанням нерухомості;
- виведення коштів з державного підприємства, шляхом оплати за товар, наявність якого підтверджено підробленими документами, на користь пов'язаних осіб, з подальшим придбанням активів;
- заволодіння бюджетними коштами територіальної громади шляхом продажу неліквідного нерухомого майна для соціально незахищених верств населення за завищеною вартістю. В подальшому кошти перераховуються на депозитний рахунок та на користь суб'єктів господарювання з ознаками фіктивності для придбання активів і обготівковування;
- перерахування бюджетних коштів юридичній особі з подальшим транзитом через власні рахунки або прямим переказом на користь групи суб'єктів господарювання з ознаками підозрілої діяльності;
- виведення коштів з державного підприємства шляхом придбання через посередника у компанії-нерезидента продукції за значно завищеною ціною з подальшим розпорошенням різниці між реальною та контрактною вартістю, зокрема на користь суб'єктів господарювання та компаній-нерезидентів, шляхом укладення умисно невигідних контрактів;
- отримання бюджетних коштів групою юридичних осіб, які в подальшому використовували їх не за цільовим призначенням шляхом перерахування на власні рахунки, депозитні рахунки, на користь суб'єктів господарювання, які мають ознаки «транзитності» та ризиковості;

- перерахування бюджетних коштів за товари, роботи та послуги на користь юридичних осіб та фізичних осіб-підприємців з подальшим перерахуванням на їх власні рахунки та на користь суб'єктів господарювання з сумнівною репутацією, та діяльність яких не відповідає предмету закупівлі товарів, робіт та послуг державними установами;
- привласнення бюджетних коштів шляхом перерахування на користь суб'єкта господарювання, пов'язаного з посадовою особою бюджетної установи з подальшим перерахуванням їх на власні рахунки та на рахунки осіб, пов'язаних родинними зв'язками;
- легалізація доходів РЕР отриманих від привласнення інвестиційних внесків фізичних осіб;
- отримання посадовою особою неправомірної вигоди з метою придбання нею та/або членами її родини дороговартісного рухомого та нерухомого майна;
- придбання елітного нерухомого та рухомого майна пов'язаними з РЕР особами за рахунок коштів з невстановлених джерел;
- внесення готівкових коштів на рахунок РЕР з непідтверджених джерел та отримання на рахунок РЕР дивідендів шляхом штучного формування прибутків юридичних осіб, кінцевими бенефіціарними власниками яких є інші РЕР.

Використання НПО у незаконній діяльності та незаконне заволодіння і привласнення благодійної допомоги

- завищення кошторисної вартості та обсягів робіт під час реалізації проєкту з будівництва житла для внутрішньо переміщених осіб коштом іноземних благодійників, з подальшим виведенням на пов'язаних фізичних осіб-суб'єктів підприємницької діяльності;
- перерахування коштів Благодійним фондом на користь фізичних осіб-суб'єктів підприємницької діяльності, з подальшим виведенням на рахунки осіб з ознаками фіктивності (так званих «дропів»);
- збір Громадською організацією добровільних пожертв з метою надання гуманітарної допомоги військовим, з подальшим використанням на власні потреби (погашення кредиту пов'язаної з Громадською організацією особи);
- нецільове використання добровільних пожертв Громадською організацією;
- шахрайське заволодіння коштами громадян шляхом розміщення оголошень у соціальних мережах, з подальшим використанням на власні потреби.

Транскордонне ВК

- виведення коштів з України під виглядом придбання прав на ліцензійне програмне забезпечення;
- придбання групою українських компаній (у т.ч. сільськогосподарських) програмного забезпечення на значну суму у компанії-нерезидента, яка уклала договір на розповсюдження цього ПЗ з іншою компанією, що має ознаки компанії-оболонки;
- експорт сільськогосподарської продукції підприємствами з ознаками фіктивності без повернення валютної виручки;
- зустрічний експорт (нелегальний експорт продукції супроводжується імпортом фруктів та овочів на територію України з метою їх подальшої реалізації за готівку);
- отримання групою юридичних осіб позик від фінансових компаній з подальшим переказом на користь групи компаній-нерезидентів за товари, які в подальшому не були поставлені;
- ухилення від сплати податків шляхом формування незаконного податкового кредиту при імпорті вживаних автомобілів та здійснення прихованої конвертації;
- заволодіння кредитними коштами державного банку з використанням зовнішньоекономічних операцій та залученням пов'язаних компаній-нерезидентів з метою подальшої легалізації злочинних доходів за межами України;
- укладення генерального кредитного договору з українським державним банком щодо формування покриття за акредитивами для закупівлі природного газу за кордоном за умов його подальшої реалізації на території України, який так і не було поставлено на територію України.

Податкові злочини та схеми ухилення від оподаткування

- проведення валютних операцій з придбання вибухонебезпечних речовин юридичною особою, пов'язаною з рф, за відсутності підтвердження державного замовлення на даний товар;
- використання рахунку фізичної особи, яка має ознаки «дропа», для проведення транзитних операцій з безготіковими коштами групи осіб та готівковим коштами невідомого походження;
- прихована конвертація безготівкових коштів у готівкові із застосуванням механізму «скрутки» та фіктивного продажу товару з метою відшкодування імпортного ПДВ;
- використання готівкових коштів для розрахунків за правочинами за заниженою вартістю з метою приховування джерел походження коштів та уникнення сплати відповідних податків;
- використання підконтрольних груп фізичних осіб – підприємців, в тому числі з ознаками «дропів», в схемах «дроблення бізнесу», спрямованих на зменшення податкового навантаження та обготівковування коштів;

- конвертація в готівку безготівкових коштів, отриманих від продажу металобрухту, через рахунки юридичних осіб, фізичних осіб та фізичних осіб – підприємців з метою ухилення від сплати податків та виведення коштів у тіньовий сектор;
- «прихована конвертація» безготівкових коштів у готівку з використанням механізму «зустрічних потоків» із залученням реально діючих оптових та роздрібних торгівців, які можуть мати необліковану готівку.

Відмивання доходів, отриманих від шахрайських дій та кіберзлочинів

- використання технологій штучного інтелекту (ШІ) з метою незаконного проходження дистанційної ідентифікації та отримання доступу до рахунку клієнта;
- умисна підробка документів щодо внесення коштів на депозит для шахрайського заволодіння грошовими коштами банківської установи;
- шахрайський продаж фізичною особою об'єктів комерційної нерухомості, до будівництва яких вона не мала законного відношення, за готівкові кошти;
- шахрайське заволодіння готівковими та безготівковими коштами громадян під виглядом збору коштів на потреби Збройних сил України;
- заволодіння коштами фізичних осіб шляхом обману або зловживання довірою (продаж неіснуючих товарів через соціальні мережі) з подальшим виведенням коштів на криптовалютну біржу;
- використання підробленого вебсайту державного органу, для доступу до особистих даних та банківських рахунків з метою незаконного списання коштів;
- використання фішингових листів для отримання доступу до банківського рахунку жертви та здійснення незаконних переказів.

Відмивання злочинних доходів із використанням віртуальних активів

- проведення операцій з криптоактивами, з використанням стороннього сервісу обміну, через звичайні поточні рахунки, не призначені для такої діяльності, із залученням неповнолітніх осіб та іноземних громадян;
- використання віртуальних активів як викупу за розблокування роботи компаній-нерезидентів, які постраждали внаслідок кібератак;
- використання фейкових проєктів з «криптотрейдингу», що фактично є елементом фінансової піраміди, з метою шахрайського заволодіння коштами громадян України та іноземців.

Відмивання злочинних доходів через гральний бізнес

- відмивання доходів із використанням онлайн-ресурсів, що спеціалізуються на продажі ігрових предметів (відеоігор);
- виведення коштів з онлайн-казино через неодноразові виплати виграшів на користь фізичних осіб без негативної ділової історії з використанням великої кількості банківських рахунків для обготівковування;

- використанням електронного термінала для здійснення фінансових операцій, які мають на меті забезпечення діяльності з незаконної організації чи проведення азартних ігор та лотерей, у тому числі через маскування під інтернет-магазин;
- отримання прихованого прибутку від організації та проведення азартних ігор/онлайн-казино, із використанням механізмів зменшення бази оподаткування, обготівковування та виведення коштів за кордон.

Торгівля зброєю

- відмивання коштів від незаконного продажу зброї та акцій оборонної компанії шляхом інвестування у закордонну нерухомість.

Торгівля людьми

- готівкові та безготівкові зарахування на рахунки фізичних осіб, які причетні до незаконної діяльності, пов’язаної зі створенням та розповсюдженням порнографічного контенту, з подальшим транзитом коштів іншим особам, переведенням в готівку та придбанням товарів/послуг;
- фінансові операції, проведені фізичною особою, яка входить до керівної структури міжнародної злочинної мережі, що спеціалізується на організованому сутенерстві, торгівлі людьми, пов’язані з веденням розкішного життя, при декларуванні незначних офіційних доходів можуть мати злочинне походження.

Торгівля наркотичними засобами

- використання групою фізичних осіб «дропів» для переміщення коштів невідомого походження, у тому числі від збуту наркотичних речовин, які можуть використовуватись для фінансування протиправної діяльності

5.6. Найпоширеніші способи фінансування війни та тероризму

Сучасна практика фінансування збройної агресії та терористичної діяльності охоплює широкий спектр способів, які використовуються як державними структурами країни-агресора, так і пов'язаними з нею приватними особами, підприємствами, псевдо благодійними організаціями та колаборантами.

У контексті збройної агресії російської федерації проти України спостерігається активне застосування комплексних схем переміщення коштів, приховання бенефіціарної власності, обходу санкцій, використання криптовалют, грального бізнесу, а також залучення вразливих категорій населення до фінансово-підривної діяльності.

Систематизовано найпоширеніші моделі, що застосовуються для фінансування війни, тероризму та підтримки режиму окупації, у межах яких виокремлено основні групи схем, що охоплюють ключові канали, інструменти та учасників, залучених до реалізації таких дій, а саме:

ФТ та ВК як частина фінансування війни

- Використання спецслужбами рф криптогаманців для переказу коштів на карткові рахунки громадян України з метою вербування для вчинення терористичних актів та інших злочинів на території України;
- Використання рахунків фізичної особи, яка зареєстрована та фактично перебуває на тимчасово окупованій території для фінансування та організації терористичних і диверсійних актів в Україні;
- зарахування на рахунки українських ІТ-працівників коштів від урядових організацій країни, що знаходиться у списку держав-терористів, з подальшим зняттям їх готівкою, для фінансування діючого режиму підсанкційної та терористичної держави;
- перерахування криптовалюти фізичною особою, яка є громадянином України, на криптогаманці, розміщені у російських та проросійських Telegram-каналах, які здійснюють збір коштів для закупівлі збройними формуваннями рф безпілотних літальних апаратів, обладнання, техніки тощо;
- зарахування на рахунки ФОП безготівкових платежів за товари, закупівлю яких не можливо підтвердити, з подальшим спрямуванням коштів на користь групи фізичних осіб, які підозрюються в участі у терористично-диверсійній діяльності на території України в інтересах країни-агресора;
- внесення готівкових коштів, які були отримані через агентів (кур'єрів) спецслужб рф, громадянами України – переважно особами літнього віку, на рахунки суб'єктів господарської діяльності, підконтрольних представникам країни-агресора.

Обхід санкцій та фінансових обмежень

- залучення компанії-посередника в Україні, розрахунки з якою проводяться шляхом зарахування зустрічних однорідних вимог, для експорту продукції компаніям-посередникам в інших країнах, з метою подальшого постачання продукції до рф в обхід санкцій РНБО України;
- здійснення платежів на компанії, що приховують реальних власників – резидентів/громадян рф, з метою уникнення санкцій;
- здійснення транскордонних переказів з використанням криптовалюти, створеної компанією, що належить російському державному банку;
- залучення підставних фірм, підконтрольних Компанії, включеній до санкційного списку OFAC, для постачання, в обхід санкцій, електронних компонентів, у тому числі мікроелектроніки подвійного призначення, до групи російських компаній, що входять до складу ВПК рф;
- залучення нерезидентів-посередників з метою імпорту товарів російського походження в обхід санкцій;
- виведення та легалізація коштів з підприємства, підконтрольного особі, стосовно якої застосовано санкції, шляхом залучення ряду підставних юридичних осіб із використанням удаваних договорів позики та переуступок прав вимоги;
- проведення фінансових операцій з придбання нерухомості, що належить фізичній особі, яка перебуває під санкціями, пов’язаною компанією, з метою збереження контролю над об’єктом нерухомості всупереч запровадженим санкціям.

ВИСНОВОК

Проведене типологічне дослідження підтверджує, що збройна агресія російської федерації стала системним каталізатором трансформації ризиків у сфері ВК/ФТ/ФРЗМЗ. Військові дії, тимчасова окупація частини територій України, масова міграція населення, руйнування об'єктів критичної, енергетичної, транспортної та фінансової інфраструктури, порушення сталих виробничих, торговельних і логістичних ланцюгів, зростання тіньової економіки та неформальних фінансових розрахунків, а також стрімка цифровізація фінансових послуг і поширення дистанційних каналів обслуговування в умовах воєнного стану створили сприятливе середовище для розвитку прихованих і технологічно складних фінансових злочинів.

Дослідження також засвідчило, що фінансування війни та тероризму тісно переплітається зі схемами відмивання коштів, обходу санкцій, корупційних і податкових злочинів. Злочинці активно використовують як традиційні фінансові інструменти (готівку, підставних осіб «дропів», фіктивні компанії), так і сучасні цифрові рішення – криптовалюти, DeFi-платформи, онлайн-казино, соціальні мережі та інструменти штучного інтелекту.

Запропонована систематизація групування інструментів, типових схем і індикаторів підозрілості учасників та фінансових операцій формує практичну основу для застосування ризик-орієнтованого підходу та розвитку аналітичних систем. Вона дає змогу підвищити ефективність виявлення складних схем ВК/ФТ, зменшити вплив людського фактора.

Загалом типологічне дослідження за 2025 рік є важливим аналітичним документом для суб'єктів фінансового моніторингу, правоохоронних і регуляторних органів. Глобалізація злочинних фінансових потоків, висока швидкість руху активів і доступність цифрових інструментів суттєво ускладнюють виявлення протиправних схем та вимагають від інституцій України впровадження інноваційних, аналітично орієнтованих підходів, зокрема із застосуванням штучного інтелекту, автоматизованих систем виявлення ризиків і міжнародного обміну інформацією.

У цьому контексті розвиток ринку аналітичних продуктів і технологічних рішень для фінансового моніторингу набуває ключового значення для забезпечення своєчасного виявлення ризиків, якісного аналізу даних і ефективної міжвідомчої та міжнародної взаємодії.

Держфінмоніторинг як національний підрозділ фінансової розвідки у 2025 році посилює протидію фінансовим злочинам, фінансуванню тероризму та схемам обходу санкцій, забезпечуючи захист фінансової системи України та роблячи внесок у міжнародні зусилля у сфері ПВК/ФТ/ФРЗМЗ.

ПОПЕРЕДНІ ТИПОЛОГІЧНІ ДОСЛІДЖЕННЯ

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

Типологічні дослідження мають практичне значення:

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

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

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

Перелік типологічних досліджень Держфінмоніторингу

Рік	Тематичний напрямок	Тема типологічного дослідження
2024	ВК/ФТ	«Ризики та загрози легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансування тероризму в умовах військової агресії російської федерації – 2024»
2023	ВК/ФТ	«Ризики та загрози легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансування тероризму в умовах військової агресії російської федерації»
2022	ВК/ФТ	«Фінансування тероризму та отримання кримінальних доходів від вчинення інших злочинів в умовах військової агресії російської федерації»
2021	загальна	«Актуальні методи, способи, інструменти легалізації (відмивання) злочинних доходів та фінансування тероризму (сепаратизму)» (2021 рік)
2020	податки	«Відмивання доходів від податкових злочинів»
2019	бюджет	«Відмивання доходів від привласнення коштів і майна державних підприємств та інших суб'єктів, які фінансуються за рахунок державного та місцевих бюджетів»
2018	бенефіціари	«Ризики використання суб'єктів з непрозорою структурою власності у схемах відмивання кримінальних доходів»

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

ДОДАТОК. ІНСТРУМЕНТИ, ТЕХНОЛОГІЇ, РЕСУРСИ ДЛЯ КОНТРОЛЮ ТА ФІНАНСОВОГО МОНІТОРИНГУ

1. АНАЛІТИЧНІ ІНСТРУМЕНТИ ТА АНАЛІТИЧНІ ПЛАТФОРМИ

У 2025 році аналітичні інструменти та платформи трансформуються в інноваційні, інтегровані та адаптивні рішення, що поєднують генеративний штучний інтелект, хмарні технології, блокчейн-аналітику та сучасні архітектури даних. Такі платформи забезпечують прозору, масштабовану й точну аналітику в режимі реального часу, що є критично важливим у протидії зростанню фінансових злочинів і обсягу даних.

Злиття інформації з глобальних баз даних, відкритих джерел (OSINT) і санкційних списків у поєднанні з можливостями ШІ сприяє ефективному моніторингу ризиків та виявленню підозрілих транзакцій.

Сучасні аналітичні системи повинні бути гнучкими та здатними швидко адаптуватися до нових викликів і регуляторних вимог, зберігаючи при цьому високу продуктивність і прозорість. Фактично вони виступають основою для забезпечення прозорості, безпеки та дотримання глобальних регуляторних стандартів.

Для забезпечення актуальності та повноти даних, сучасні аналітичні платформи інтегруються з зовнішніми інформаційними джерелами через API. Це забезпечує збагачення профілів клієнтів, оперативне оновлення інформації та більш точне виявлення ризикових факторів у режимі реального часу.

Разом із цим, одна й та сама технологія може працювати по-різному в різних компаніях, бо все залежить від їхніх умов і можливостей.

Основні напрямки розвитку:

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

фінансовою системою. Використання поведінкових даних сприяє запровадженню точних моделей оцінки ризиків, враховуючи динаміку дій клієнтів;

- **автоматизовані системи моніторингу транзакцій**. Моніторинг та аналіз конкретних фінансових операцій клієнта для виявлення підозрілих транзакцій. Використання алгоритмів виявлення аномалій у транзакціях відповідно до індикаторів, фільтрацію за правилами;
- **динамічний моніторинг транзакцій у реальному часі**. Загальний моніторинг фінансових потоків забезпечує постійне спостереження за всіма транзакціями в реальному часі та дає змогу оперативно виявляти й реагувати на аномалії, що можуть свідчити про підозрілі дії. Динамічний моніторинг передбачає автоматизовані оповіщення та блокування транзакцій у разі виявлення підозр;
- **інтеграція даних із криптовалютних платформ** для формування ризиків. Інформація з блокчейнів забезпечить: виявлення зв'язків між криптовалютними гаманцями та нелегальними операціями; відстеження транзакцій у криптовалютах для ідентифікації підозрілих потоків;
- **розширення можливостей автоматизації**, що спрощує підготовку регуляторних звітів і забезпечує відповідність глобальним стандартам;
- **сценарний аналіз із використанням ШІ**, який здатний прогнозувати потенційні загрози та моделювати ризики. Використання прозорого штучного інтелекту для підвищення довіри до моделей та відповідності вимогам регуляторів шляхом пояснення логіки прийняття рішень;
- **впровадження генеративного штучного інтелекту** (Generative AI) для створення адаптивних аналітичних сценаріїв, автоматизованих шаблонів ризиків і звітів.

Для забезпечення ефективного фінансового моніторингу та управління ризиками використовують сучасні інструменти та підходи, зокрема скорингові моделі.

Скорингові моделі. Скорингові моделі – це інструменти оцінки ризиків клієнтів, які застосовуються як під час встановлення ділових відносин, так і в процесі їх подальшого обслуговування. Вони базуються на машинному навчанні та формують ризик-профіль у реальному часі, враховуючи не лише базові дані, а й поведінкові патерни та динаміку транзакцій.

На початковому етапі скорингові моделі допомагають:

- ідентифікувати клієнта (KYC) – збираючи та верифікуючи базову інформацію;
- оцінити ризик-профіль (CDD) – за такими факторами, як географічний ризик, сфера діяльності, джерело коштів, зв'язки з політично значущими особами (PEP), наявність негативних згадок тощо;
- здійснити скринінг – перевірити клієнтів за міжнародними та національними реєстрами (санкційні списки, переліки терористів тощо).

На цьому рівні модель визначає початковий ризик-профіль клієнта та формує рішення щодо прийняття або відмови у встановленні ділових відносин.

Етап моніторингу транзакцій і поведінкового аналізу. Після встановлення ділових відносин скорингові моделі здійснюють динамічний аналіз клієнтської активності:

- відстежують транзакційні потоки в реальному часі, виявляють відхилення від звичних патернів і сигналізують про потенційно підозрілі операції;
- застосовують поведінкові моделі для розпізнавання типової та ризикової активності;
- оновлюють ризик-профіль клієнта з урахуванням нових дій і транзакцій.

Такий підхід формує основу адаптивного ризик-скорингу – механізму, що забезпечує гнучке реагування на зміну клієнтської поведінки та ризикових факторів у режимі реального часу.

У межах розвитку національної системи фінансового моніторингу розглядається можливість упровадження (розвитку) предиктивної аналітики на базі штучного інтелекту.

Це дозволить доповнити наявні ризикові моделі інструментами, здатними не лише виявляти відомі злочинні схеми, а й прогнозувати появу нових – шляхом аналізу поведінкових аномалій клієнтів, нестандартної активності, ринкових трендів і змін у цифровому середовищі.

Використання таких інструментів забезпечить виявлення ще не ідентифікованих загроз та створить підґрунтя для їхнього превентивного реагування. Стратегічно потрібно адаптуватись до нових викликів, пов’язаних із розвитком цифрових технологій і змін у ландшафті фінансових загроз.

Матриця оцінки рівня ризику публічних осіб (PEP). Застосовування матриці розрахунку рівня ризику публічних осіб дозволяє оцінити репутаційні та фінансові ризики клієнтів.

Ключові елементи матриці ризику розрахунку рівня ризику публічних осіб можуть бути:

Посада та рівень політичної значущості. Оцінка клієнтів за їхнім статусом (національний чи міжнародний рівень впливу) та аналіз пов’язаних осіб (членів сім’ї, близьких партнерів).

Фінансова діяльність**.** Виявлення джерел доходів для визначення їхньої прозорості. Оцінка походження активів, зокрема, великих фінансових потоків.

Географічні ризики. Аналіз країни походження або основної діяльності клієнта, зокрема, юрисдикцій із підвищеним рівнем корупції або ризиком фінансових злочинів.

Репутаційні фактори. Моніторинг відкритих джерел (OSINT), новин та інших публікацій та санкційних списків дозволяє виявляти інформацію про минулі випадки корупції, шахрайства чи інших ризикових дій, забезпечуючи всебічну оцінку репутації та потенційних загроз, пов’язаних із клієнтом.

Динаміка фінансової активності. Аналіз змін у транзакціях чи поведінці клієнтів, особливо публічно значущих осіб (PEP), дозволяє ідентифікувати аномалії, такі як раптове збільшення обсягів операцій або використання нових напрямків. Врахування рівня ризику PEP включає оцінку їхньої репутації, джерел доходів та можливих зв'язків із корупційними чи ризикованими діями.

Сценарії відбору підозрілих фінансових операцій (діяльності)

Звіти та власні сценарії відбору підозрілих фінансових операцій - ключовий інструмент системи фінансового моніторингу. Вони забезпечують систематизацію даних, аналіз транзакцій і виявлення потенційно ризикових дій клієнтів.

Сценарії розвиваються відповідно до нових технологій і ризиків:

- правила відбору операцій можуть включати такі поля: дата здійснення, призначення платежу, сума, рівень встановленого ризику, країна, тип рахунку тощо;
- використовується динамічний сценарний аналіз, що охоплює як загальний рух активів клієнта, так і аналіз окремих операцій у динаміці;
- СПФМ інтегрують до своїх аналітичних систем додаткові дані про учасників операцій та іншу інформацію, що суттєво розширює обсяг доступних для аналізу відомостей.

Ключові тренди:

- перехід від статичних правил до систем із машинним навчанням та поведінковою аналітикою, яка може передбачати ризик, а не лише реагувати;
- застосування підходу «risk-based monitoring» – сценарії адаптуються до профілю клієнта, каналу обслуговування, продукту, географії;
- зменшення кількості хибних спрацювань завдяки інтелектуальній обробці сигналів та контекстному аналізу транзакцій;
- тісніша співпраця та обмін даними для створення більш повних сценаріїв ризику.

Штучний інтелект і біометрія: Еволюція цифрової фінансової безпеки - від запізнілої реакції до проактивного управління ризикам

Сучасний фінансовий сектор вступає в нову еру боротьби із злочинами, де традиційні методи вже не витримують натиску високотехнологічних загроз. Фінансовий сектор у всьому світі, включно з Україною, активно збільшує інвестиції у ШІ-рішення для виявлення аномалій, поведінкову аналітику та біометричні системи.

Фрагментованість даних та висока швидкість еволюції злочинних схем ставлять під сумнів ефективність класичних моделей реагування. Стає очевидним, що майбутнє – за адаптивними моделями ризику, створенням поведінкових профілів користувачів, інтеграцією біометрії та обміном інформацією між банками й фінтех-компаніями через спільні чорні списки.

Фінансовий ринок входить у фазу, де злочини (наприклад, шахрайство) набуває рис масового виробництва – з використанням автоматизованих ботів, фішингових фабрик та соціальної інженерії. У цій реальності виграє не той, хто пропонує найзручніший інтерфейс, а той, хто впроваджує багаторівневу систему захисту, мислить у категоріях «нас уже зламали», і будує гнучкі системи реагування на нові типи загроз.

У відповідь на зростання загроз, пов’язаних із використанням технологій діпфейку у сфері фінансових послуг, до переліку сучасних автоматизованих систем перевірки клієнтів (KYC) слід включити інноваційні цифрові рішення, орієнтовані на виявлення цифрових підробок особистості.

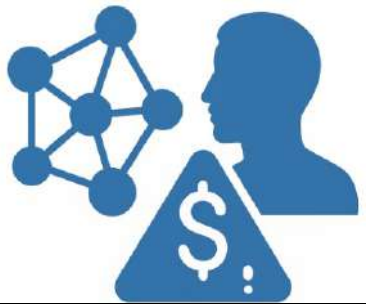
Liveness Detection (визначення «живості») – ці алгоритми використовуються під час біометричної ідентифікації для перевірки того, чи є перед камерою справжня людина, а не підроблене відео, зображення або 3D-маска.

Системи Liveness Detection аналізують: мікрорухи обличчя; природну зміну кольору шкіри; частоту кліпання очей; реакцію на зміну освітлення тощо. Це дозволяє ефективно блокувати спроби використання діпфейків під час віддаленої верифікації.

Аналіз голосу для виявлення голосових діпфейків – ШІ-системи для біометричної ідентифікації голосу здатні виявляти підроблений голос на основі: тембральних особливостей; ритміки мовлення; типових інтонацій; частотних характеристик.

Такі рішення дозволяють ідентифікувати ознаки синтетичного або склеєного аудіо, навіть якщо воно створене за допомогою передових генераторів мовлення.

Застосування графових баз і поведінкових моделей у протидії фінансовим ризикам

	У сучасному світі використовується низка технологій, які дозволяють не лише реагувати на вже відомі схеми відмивання коштів, а й прогнозувати появу нових ризиків.

Серед ключових засобів:

Графові бази даних й аналіз мереж (Graph Analytics / Graph Databases). ШІ-алгоритми будують та аналізують мережі взаємозв'язків між клієнтами, рахунками, транзакціями та контрагентами. Це дає змогу виявити приховані зв'язки, кола переводу коштів та схемні маршрути.
Сценарне моделювання та прогнозування ризиків (Scenario Modelling / Risk Forecasting). На основі історичних даних, поведінкових патернів та ринкових тенденцій створюються моделі, які оцінюють ймовірність появи нових схем або змін у поведінці клієнтів. Наприклад: аналіз аномалій, незвичних транзакцій.
Виявлення патернів поведінки клієнтів (Behavioral Pattern Detection). Алгоритми навчаються на даних транзакцій, KYC-інформації клієнтів та зовнішніх джерел, щоб визначити, коли клієнт чи група клієнтів поводиться інакше, ніж зазвичай – наприклад, різке нарощування транзакцій, зміна географії переказів або поява нетипових зв'язків.
Прогнозування появи нових схем (Emerging Typologies Detection). Завдяки машинному навчанню та глибокому аналізу великих обсягів даних, системи можуть ідентифікувати «невідомі невідомі» (unknown-unknowns) - тобто методи, які ще не були формально зафіксовані як схеми, але проявляються через аномалії.

Впровадження нових технологій (зокрема, графових баз даних, сценарного моделювання, прогнозування ризиків і поведінкової аналітики тощо) дозволяє значно підвищити ефективність ПВК/ФТ.

Використання автоматизованих систем

В умовах війни, викликаної агресією росії, виявлення фінансових операцій, що підлягають моніторингу, стає ще більш критичним завданням.

Застосування автоматизованих систем із вбудованим аналізом критеріїв ризику та індикаторів підозрілості дає змогу своєчасно ідентифікувати операції, пов'язані з незаконними фінансовими операціями.

Нижче наведена інформація про інноваційні підходи, які допомагають виявляти схеми ВК, про які зазначили в запитальники СПФМ.

Приклад 1. Роботизація та штучний інтелект для виявлення схем відмивання коштів через онлайн-казино

Один із суб'єктів первинного фінансового моніторингу (банк) впровадив роботизовану систему моніторингу інтернет-ресурсів (Robotic Process Automation – RPA), спрямовану на ідентифікацію потенційно ризикових клієнтів, залучених до незаконних фінансових операцій, пов'язаних з онлайн-казино.

RPA-модулі автоматично здійснюють сканування та аналіз веб-сайтів онлайн-казино з метою виявлення згадок або ознак використання платіжних інструментів клієнтів банку. До системи інтегровано елементи штучного інтелекту (AI) для розпізнавання даних у зображеннях, текстах та HTML-структурах, що дозволяє виявляти приховані або завуальовані реквізити (логотипи, карткові номери тощо).

Результати зіставляються з базами внутрішнього скорингу, KYC-профілями та поведінковими моделями клієнтів.

Впровадження роботизованої системи дало змогу автоматизувати пошук нових схем, знизити навантаження на СПФМ та скоротити час реагування на підозрілі операції. Такий підхід демонструє тренд інтелектуальної автоматизації фінансового моніторингу (AI та RPA).

Приклад 2. Машинне навчання для виявлення клієнтів-«дропів» у нелегальній діяльності

Один із суб'єктів первинного фінансового моніторингу (банк) впроваджує інноваційний підхід на основі DataScience-моделювання для ідентифікації клієнтів, які можуть бути залучені до нелегального грального бізнесу або неофіційної діяльності криптобірж. Модель має назву «Модель ймовірності приналежності клієнта до дропів казино (1 рівня)» і побудована на аналізі p2p та IBAN операцій клієнтів.

Для розробки моделі застосовано градієнтний бустинг над деревами рішень (LightGBM). Бустинг над деревами рішень (Gradient Boosting over

Decision Trees) - це метод машинного навчання, який використовується для підвищення точності прогнозування моделей.

Модель реалізує підхід бінарної класифікації, де результатом є ймовірність належності клієнта до групи «дропів» (учасників схем переказу та обготівкування коштів).

Алгоритм здійснює самооптимізацію під час навчання, визначаючи закономірності в поведінці клієнтів. Модель аналізує частоту, напрямки та типи p2p-операцій, виявляючи нетипові зв'язки між клієнтами. Використовується система вагових коефіцієнтів, що дозволяє ранжувати клієнтів за рівнем ризику участі у підозрілих операціях.

Модель дозволяє автоматизовано формувати перелік клієнтів із підвищеним ризиком та завчасно виявляти потенційних учасників схем ВК/ФТ, що використовують електронні платіжні засоби для обходу фінансового моніторингу. Використання LightGBM-моделей демонструє перехід СПФМ від ручного сценарного моніторингу до інтелектуальних систем аналізу ризику, заснованих на машинному навчанні, поведінковій аналітиці та real-time scoring.

Приклад 3. Адаптивна аналітика та ранговий аналіз для підвищення ефективності виявлення підозрілих операцій

Один із суб'єктів первинного фінансового моніторингу упровадив адаптивну аналітичну систему, що поєднує внутрішні правила, сценарії, машинне навчання (ML) та штучний інтелект (AI).

Система автоматично оновлює параметри моніторингу на основі рангового аналізу транзакцій та діяльності клієнтів, включно з їх контрагентами.

Для кожного клієнта формується профіль ризику за сукупністю індикаторів підозрілості (географія, частота, тип операцій, контрагенти).

Алгоритм визначає ранг ризиковості - від низького до високого - залежно від кількісних і якісних показників.

Вага (значущість) кожного індикатора автоматично коригується на основі виявлених трендів і реальних результатів розслідувань.

Система здатна додавати нові критерії ризику в режимі реального часу, коли виникають нові типології чи з'являються нові схеми ВК/ФТ.

Результати впровадження: скорочення часу на обробку великого обсягу транзакцій, оперативне виявлення клієнтів і контрагентів із високим рівнем ризику, зменшення кількості хибних спрацювань завдяки точнішому розподілу вагових коефіцієнтів ризику, а також підвищення адаптивності системи до нових загроз без потреби ручного оновлення правил.

Застосування адаптивної аналітики та рангового аналізу демонструє перехід від статичних сценаріїв до самонавчальних моделей ризику (AI-driven Risk Models). Такі рішення підсилюють спроможність СПФМ швидко реагувати на нові типи схем ВК/ФТ, покращують ризик-орієнтоване управління та підвищують аналітичну точність фінансового моніторингу.

Приклад 4. Автоматизована перевірка клієнта через інформаційну платформу під час онлайн-онбордингу

Банківські установи запроваджують автоматизовану перевірку клієнтів на етапі онлайн-онбордингу.

Перед відкриттям рахунку система автоматично звіряє дані особи з інформаційною платформою Єдиної міжбанківської аналітичної системи (ЄМА), яка містить відомості про осіб, причетних до фінансового шахрайства або дроп-активності.

Якщо виявлено збіг даних потенційного клієнта, онбординг блокується або направляється на додаткову перевірку. Процес повністю інтегрований у процес онбордингу і відбувається в режимі реального часу без залучення працівників.

Результати впровадження: зменшення кількості шахрайських реєстрацій під час дистанційного відкриття рахунків; підвищення ефективності KYC-процедур та якості ідентифікації; оптимізація процесу онбордингу – клієнти проходять перевірку швидше, а ризикові особи автоматично виявляються.

Інтеграція автоматизованих аналітичних платформ у процес онлайн-ідентифікації клієнтів (digital onboarding) дозволяє фінансовим установам поєднувати швидкість цифрових сервісів із надійністю перевірок, підвищуючи ефективність запобігання шахрайству та схемам ВК/ФТ.

Різні суб’єкти первинного фінансового моніторингу реалізують комплексний підхід до:

- автоматичного збагачення даних клієнта інформацією з офіційних відкритих реєстрів;
- формування динамічних ризик-профілів клієнтів - система аналізує поведінкові патерни, структуру операцій, географію та типи контрагентів, автоматично виявляючи нетипові або ризикові дії;
- використання ChatGPT як допоміжного інструмента для пошуку та агрегації публічних даних про клієнтів із відкритих джерел (ЗМІ, публічні реєстри, офіційні сайти). Це дозволяє виявляти репутаційні ризики або зв’язки з відомими випадками незаконної діяльності.

Реквізити для встановлення сценарію відбору підозрілих фінансових операцій (діяльності) клієнта

Сценарій відбору підозрілих фінансових операцій (діяльності) формується на основі аналізу профілю клієнта та його фінансової активності, що відхиляється від типового поведінкового патерну або містить ознаки, характерні для типологій відмивання ВК/ФТ.

Реквізити щодо профілю клієнта

зв'язки з агресором

- наявність зв'язків з країнами, які причетні до військової агресії проти України;

загальна інформація про клієнта

- клієнт належить до соціально вразливих верств населення;
- період співпраці клієнта з СПФМ (тривалість ділових відносин);
- адреса реєстрації клієнта;
- клієнт є політично значущою особою;
- наявність зв'язку з політично значущою особою;
- регулярні зміни у реєстраційних документах, включаючи часті зміни адреси чи назви компанії;
- країна реєстрації клієнта. Наприклад, до таких юрисдикцій належать країни, що внесені до списків FATF як зони з високим ризиком, або ті, які мають репутацію офшорних зон з низьким рівнем фінансової прозорості;
- розмір статутного капіталу суб'єкта господарювання, оскільки розмір може бути критерієм ризику, якщо він суттєво занижений порівняно із заявленою діяльністю чи масштабом фінансових операцій, що може свідчити про фіктивність компанії, відсутність реальних фінансових ресурсів або її використання для непрозорих операцій і транзитних схем;
- вид діяльності суб'єкта господарювання;
- кількість працівників суб'єкта господарювання як відповідність масштабам та характеру заявленої діяльності;
- період діяльності юридичної особи/вік фізичної особи, оскільки короткий період існування компанії чи молодий вік особи можуть свідчити про недостатній досвід, низький рівень репутації або навіть створення суб'єкта виключно для участі у схемах відмивання коштів чи інших непрозорих операціях;

інформація про власників та управлінців

- кінцевий бенефіціарний власник або керівник клієнта належить до соціально вразливих верств населення;

- адреса реєстрації кінцевого бенефіціарного власника або керівника клієнта;
- наявність зв'язку кінцевого бенефіціарного власника або керівника клієнта з політично значущою особою;
- кінцевий бенефіціарний власник або керівник займає аналогічні посади у багатьох компаніях;
- інформація про кінцевого бенефіціарного власника, посадово-засновницький склад суб'єкта господарювання та їх участь в інших юридичних особах (резидентність);
- інформація про зміни кінцевого бенефіціарного власника та посадово-засновницького складу суб'єкта господарювання;

юридичні аспекти

- наявність інформації про відкриті кримінальні провадження з розслідування злочинів у сфері господарської діяльності щодо власника істотної участі/контролера або юридичної особи, її керівників та/або представників;
- історія судових рішень щодо клієнта;

задекларована фінансова інформація

- використання особою необґрунтованої кількості банківських установ для проведення фінансових операцій та здійснення діяльності. За виключенням банків із високим рівнем цифровізації що може бути поясненням використання різних функціональних мобільних додатків;
- розмір доходів та сплачені податки суб'єкта господарювання;
- потенційна сума (оборот) коштів, що може бути використаний суб'єктом господарювання за допомогою послуги (продукту);
- оцінка відповідності заявленої діяльності фактичній операційній активності (за даними звітності чи зовнішніх джерел);

господарська діяльність

- наявність виробничих потужностей/торговельно-складських приміщень, інших активів, необхідних для ведення задекларованої господарської діяльності суб'єкта господарювання;

географічні та зовнішньоекономічні аспекти

- взаємодія з особами чи компаніями із санкційних списків;
- взаємодія з особами чи компаніями із високоризикових юрисдикцій;
- дані про взаємодію з суб'єктами, які зареєстровані в офшорних зонах;

технологічні аспекти

- використання криптовалютних гаманців та участь у криптовалютних транзакціях;
- ідентифікація криптовалютних гаманців, пов'язаних із нелегальними транзакціями;

відкриті джерела (OSINT)

- залученість особи до сумнівних дій, що можуть вплинути на його репутацію та підвищити ризик за даними із відкритих джерел інформації (OSINT);

аналіз цифрових слідів: електронні адреси

- необґрунтоване використання однієї електронної адреси кількома особами може свідчити про спробу приховати справжніх бенефіціарів чи зв'язки між суб'єктами. Така практика часто вказує на фіктивність компаній, номінальне керівництво або контроль одного власника над кількома організаціями. Використання однієї адреси для різних суб'єктів господарювання може створювати ризик шахрайських дій, порушення регуляторних норм або участі у схемах відмивання коштів;
- використання доменів електронних адреси, які можуть бути пов'язані із сервісами розташованими у ризикових або підозрілих географічних зонах. Наприклад, домени, зареєстровані в країнах із високим ризиком корупції чи причетних до військової агресії;
- використання тимчасових або анонімних доменів (наприклад, @mailinator.com, @protonmail.com) може свідчити про спроби уникнути ідентифікації;

аналіз цифрових слідів: IP-адрес

- автоматизація процесів аналізу IP-адрес;
- необґрунтоване використання інструментів для анонімізації транзакцій, таких як VPN або Tor. Приховування реального розташування;
- невідповідність IP-адреси заявленій локації клієнта або часте використання IP-адрес із різних країн. Регулярне переміщення за даними IP-адрес між різними географічними зонами без очевидної причини.

Ідентифікація пристроїв та цифровий відбиток користувача

- використання одного Device ID для кількох облікових записів, що може свідчити про спроби маскування бенефіціарів або створення фіктивних клієнтів;
- раптова зміна пристрою або конфігурації fingerprint, особливо якщо вона супроводжується ризиковими транзакціями чи спробами доступу з нових геолокацій;
- збіг цифрового відбитка пристрою в осіб, не пов'язаних між собою формально, що може вказувати на централізоване управління кількома акаунтами (наприклад, дропами);
- невідповідність Device ID заявленому типу пристрою або операційній системі, що може свідчити про емуляцію, ботнет-діяльність чи шахрайські дії;
- регулярна заміна FingerPrint без об'єктивних причин - свідчення можливого використання інструментів маскування;
- Device ID пов'язаний із відомими шахрайськими схемами.

Реквізити щодо фінансових операцій клієнта

структурування та уникнення моніторингу

- спроби структурувати фінансових операцій для обходу порогових значень особою для уникнення моніторингу транзакцій;
- велика кількість однотипних транзакцій за короткий період (наприклад, багато переказів невеликих сум із метою структуризації операцій);

баланс та рух коштів

- значний дисбаланс між кредитовими та дебетовими операціями (наприклад, великі обсяги вхідних коштів без відповідного руху на вихід);
- постійний «нульовий» баланс наприкінці дня за рахунком, що може вказувати на транзитний характер операцій;
- різке збільшення активності на рахунку та проходження за рахунком значних сум після тривалого періоду низької активності;
- готівкові операції (обсяги, кількість);
- нетипова активність по рахунку (сплеск активності);
- значне перевищення обсягів операцій над заявленими доходами клієнта;

сутність операцій

- проведення систематично фінансових операцій суб'єктом господарювання без зазначення суті платежу в полі призначення платежу. Наприклад, без посилань на відповідні договори чи конкретні зобов'язання;
- невідповідність між вхідними та вихідними операціями (ознаки «скруток»);
- проведення великої кількості P2P-переказів (особливо в короткий період часу або без видимого економічного сенсу);

контрагенти та пов'язані рахунки

- наявність фінансових операцій із рахунками інших осіб, які часто асоціюються з підозрілими операціями, фігурують у розслідуваннях або внесені до переліку заблокованих чи зупинених, а також щодо яких наявна негативна інформація;
- здійснення операцій з контрагентами, з якими банком було розірвано ділові відносини;

фінансова діяльність неповнолітніх осіб

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

- використання рахунку неповнолітньої особи для тимчасового зберігання коштів у значних розмірах.

Для виявлення фінансових операцій, які можуть бути пов'язані з ВК/ФТ/ФРЗМЗ, СПФМ дедалі частіше використовують сучасні програмні комплекси.

Ці системи базуються на автоматизованих алгоритмах і сценаріях, що дозволяють ідентифікувати підозрілі операції на основі заданих критеріїв.

В Україні працюють національні IT-компанії, які спеціалізуються на розробці програмних рішень (RegTech та SupTech), адаптованих під потреби та вимоги українського фінансового ринку, зокрема у сфері ПВК/ФТ. СПФМ мають два основні шляхи для виконання законодавчої вимоги щодо автоматизації процесів: вони можуть або розробити власну внутрішню систему автоматизації «з нуля», або придбати та інтегрувати вже готове комерційне рішення.

Програмні рішення B2:FinMon, АБС SCROOGE, САБ SrBank та AML.Point пропонують інструменти для автоматизації фінансового моніторингу. Зазначений перелік програмних рішень може бути доповнений відповідно до розвитку ринку IT-продуктів в Україні у сфері фінансового моніторингу.

Приклад. Система автоматизації AML.Point для ПВК/ФТ та комплаєнсу.

Основні функції та можливості AML.Point:

- ***автоматизація процедур KYC (Know Your Customer)****:* система дозволяє вести електронні анкети клієнтів і проводити автоматизовану ідентифікацію та верифікацію даних;
- ***перевірки за списками санкцій****:* AML.Point автоматично перевіряє клієнтів та контрагентів на наявність у списках терористів, санкційних списках (включаючи міжнародні та українські), а також інших офіційних джерелах даних;
- ***моніторинг транзакцій****:* рішення включає модуль для відстеження фінансових операцій з метою виявлення підозрілих транзакцій та поведінки клієнтів;
- ***оцінка та управління ризиками****:* система оцінює ризики, пов'язані з клієнтами та їхніми операціями, і призначає відповідні рівні ризику;
- ***звітність та комплаєнс****:* система автоматично генерує звіти у форматах, визначених Національним банком України та Держфінмоніторингом;

- ***інтеграція**:* завдяки структурованому API, система легко інтегрується з існуючими CRM, ERP та іншими обліковими системами компаній;
- ***хмарна інфраструктура**.*

Системи автоматизації фінансового моніторингу забезпечують своєчасне та повне виконання обов'язків СПФМ, підсилюючи ефективне управління ризиками ВК/ФТ/ФРЗМЗ.

Автоматизація процесів фінансового моніторингу є ключовим елементом забезпечення прозорості, безпеки та стійкості фінансової системи.

2. ПУБЛІЧНІ ІНФОРМАЦІЙНІ РЕСУРСИ КОНТРОЛЮЮЧИХ (ДЕРЖАВНИХ) ОРГАНІВ ТА ПРИВАТНИХ ОРГАНІЗАЦІЙ

У сучасних умовах автоматизація збору та аналізу даних з відкритих джерел стала важливим елементом для забезпечення прийняття ефективних управлінських рішень.

Автоматизація збору та аналізу даних з відкритих джерел є ключовим елементом для ефективного управління ризиками ВК/ФТ/ФРЗМЗ. Суб'єкти первинного фінансового моніторингу активно впроваджують інноваційні рішення, що забезпечують швидкість, масштабованість та стійкість до загроз.

Завдяки сучасним технологіям можлива обробка великих масивів даних за один клік, що суттєво підвищує якість аналітики, сприяє виявленню аномалій та посилює здатність протидіяти фінансовим злочинам.

Збір інформації OSINT. Базовим інструментом OSINT є пошукові системи, спеціалізовані бази даних та аналітичні платформи, які дозволяють ефективно обробляти великі обсяги даних. Вибір джерел залежить від цілей дослідження, а для кращого результату доцільно комбінувати кілька ресурсів. Для загального пошуку ефективні Google, Bing, DuckDuckGo; для регіонального - локальні платформи. Спеціальні задачі виконують Shodan, а для конфіденційності – StartPage або DuckDuckGo. Використання пошукових операторів і розширень значно підвищує точність та релевантність результатів.

Розвиток AI-браузерів. У 2025 році з'явилися AI-браузери, що поєднують пошук і AI-асистента: наприклад, Comet від Perplexity AI — браузер із вбудованим AI-помічником для автоматизованого пошуку та взаємодії.

Google у 2025 році розширив інтеграцію штучного інтелекту у свій пошук – зокрема увів AI Mode для обробки складних запитів з генерацією відповідей на основі великих моделей AI.

2025 рік став роком глибшої інтеграції штучного інтелекту в пошукові системи – від генерації відповідей у самих результатах пошуку до появи AI-браузерів та розширених джерел.

Виявлення ризикових операцій. Для виявлення ризикових фінансових операцій та аналізу підозрілої активності клієнтів суб'єкти первинного фінансового моніторингу, які відповідали на запитальник до типологічного дослідження, зазначили, що використовують низку відкритих джерел.

Серед основних - державні реєстри, сайти правоохоронних органів, сайт НКЦПФР, ресурс «Миротворець», аналітичні платформи для перевірки

компаній, офіційні сайти Європейського Союзу та Великобританії щодо реєстрації юридичних осіб, санкційний список OFAC, ChatGPT, а також платформа ЄМА для обміну інформацією про потенційних шахраїв і підставних осіб (платформа ЄМА дозволяє, також, взаємодіяти з кіберполіцією та вести реєстр інцедентів).

Наведений перелік не є вичерпним - залежно від конкретної ситуації СПФМ також залучають інші релевантні джерела, пов'язані з клієнтом, активами або фінансовими операціями.

Розширена OSINT-аналітика на базі штучного інтелекту.

У межах напряму використання відкритих джерел (OSINT) дедалі більшого значення набуває впровадження інструментів ШІ. Зокрема, автоматизований аналіз соціальних мереж дозволяє в реальному часі виявляти ознаки нових схем шахрайства, незаконних зборів коштів («псевдозборів»), а також спроб вербування «дропів» для фінансових злочинів. Окрім того, застосовується масштабована перевірка – ШІ-системи здатні обробляти тисячі записів, профілів і повідомлень з відкритих джерел, класифікуючи їх за рівнем ризику та релевантністю. Такі підходи значно підвищують ефективність моніторингу та реагування у фінансовому секторі.

ChatGPT. ChatGPT може виступати допоміжним інструментом у процесі первинного пошуку відкритої інформації щодо клієнтів суб'єктів первинного фінансового моніторингу. Зокрема, для формування запитів, виявлення потенційних джерел, структурування наявних даних або генерації гіпотез для подальшої перевірки. ChatGPT не є джерелом первинних офіційних даних і не замінює перевірку через санкційні списки, державні реєстри чи спеціалізовані аналітичні платформи. Його ефективність залежить від навичок користувача, правильності запитів і критичного підходу до отриманої інформації.

	Держфінмоніторинг регулярно виявляє публічні інформаційні джерела для отримання додаткової інформації. Корисні посилання наводяться у типологічних дослідженнях відповідно до їх тематики.

Актуальні відкриті джерела, що стосуються широкого кола питань наведено нижче.

А. Перевірка осіб, причетних до ризикової діяльності

А1. 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.
Офіс Генерального прокурора України  https://gp.gov.ua/detectable	**Список підозрюваних магістральної справи «24 лютого»** «Магістральна» кримінальна справа щодо повномасштабного вторгнення росії в Україну.
Служба безпеки України  https://ssu.gov.ua/u-rozshuku	Розшук осіб, які звинувачуються у вчиненні злочинів проти основ національної безпеки.

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**
https://www.chesno.org	База даних про українських державних зрадників: політиків, медійників, юристів та правоохоронців. Дізнайтесь імена колаборантів і повідомляйте про факти співпраці з ворогом.

A2. 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	

А3. Санкції: національні ресурси

Апарат РНБО https://drs.nsdc.gov.ua	**Державний реєстр санкцій** Реєстр створено з метою надання безоплатного публічного доступу до актуальної та достовірної інформації про суб'єктів, щодо яких застосовано санкцій.

http://www.me.gov.ua/SpecialSanctions/List?lang=ukUA&showFrgn=True&company=linge	**Міністр економіки, довкілля та сільського господарства України** Перелік осіб, до яких застосовані спеціальні санкції.

А4. Санкції: міжнародні ресурси

Санкції Європейського Союзу  https://ec.europa.eu	Європейський Союз із 2014 року запроваджує масштабні санкції проти російської федерації – спочатку у відповідь на анексію Криму, а з 2022 року – через повномасштабне вторгнення в Україну. Після визнання росією тимчасово окупованих територій Донецької та Луганської областей, Європейський Союз значно розширив санкційний тиск: до списків були включені тисячі фізичних осіб, компаній, банків та установ.
Санкції спрямовані на послаблення економічної, енергетичної та військової спроможності російської федерації – зокрема через обмеження на експорт технологій, заборону імпорту енергоносіїв, фінансові та візові обмеження. Станом на 2025 рік санкційний режим залишається чинним, регулярно оновлюється та координується з країнами G7. Європейський Союз продовжує вимагати від російської федерації припинення агресії та поваги до суверенітету й територіальної цілісності України.	
https://finance.ec.europa.eu/eu-and-world/sanctions-restrictive-measures/sanctions-adopted-following-russias-military-aggression-against-ukraine_en?utm_source=chatgpt.com	

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	

Міністерство фінансів США	OFAC публікує список осіб і компаній, які належать, контролюються або діють за чи від імені цільових країн. Санкції, пов'язані з Україною та росії. У списку також перераховані окремі особи, групи та організації, зокрема, терористи та торговці наркотиками, визначені в рамках програм, які не стосуються конкретної країни. У сукупності такі особи та компанії називаються «спеціально призначеними громадянами» або «SDN». Їхні активи заблоковані, і громадянам США, як правило, заборонено мати з ними справу.
https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-list-data-formats-data-schemas https://sanctionssearch.ofac.treas.gov https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information/ukraine-russia-related-sanctions	

А5. Санкції: альтернативні/агреговані джерела

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. Sanctions 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 https://www.opensanctions.org	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.

SanctionsExplorer https://sanctionsexplorer.org	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.	

В. ДЖЕРЕЛА ПЕРЕВІРКИ ФІЗИЧНИХ ОСІБ ТА ДОКУМЕНТІВ

В1. Дані щодо фізичних осіб

Дані щодо фізичних осіб

http://wanted.mvs.gov.ua/searchperson	**Міністерство внутрішніх справ України** Особи, які переховуються від органів влади. Набір даних містить інформацію щодо осіб, які переховуються від органів влади. Інформація в наборі розділена на окремі ресурси, кожен з яких відповідає вказаній щодо нього інформації.
https://corruptinfo.nazk.gov.ua https://public.nazk.gov.ua/	**Національне агентство з питань запобігання корупції** Єдиний державний реєстр осіб, які вчинили корупційні або пов'язані з корупцією правопорушення. Реєстр декларацій осіб, уповноважених на виконання функцій держави або місцевого самоврядування https://public.nazk.gov.ua.

https://www.ema.com.ua	EMA AntiFraud Hub (AFH) – інструмент для фінансових установ та інших учасників ринку, який можна використовувати для перевірки клієнтів щодо приналежності до шахрайської діяльності.

AFH – це захищений портал і програмне рішення, створене Асоціацією ЄМА для обміну інформацією між учасниками ринку фінансових та суміжних послуг з метою запобігання шахрайству. Зокрема, він надає можливість перевіряти суб'єктів – клієнтів, отримувачів платіжних послуг, кредитів, переказів тощо – на наявність ознак шахрайської діяльності, непрозорих операцій, зловживань платіжними інструментами.

Ключові компоненти AFH:

База дропів та інцидентів – база персональних даних, призначена для обміну інформацією про інциденти, підозрілих клієнтів, платіжні та кредитні ризики.

Сервіси перевірки клієнтів:

Mobile Check – перевірка статусу SIM-картки, інформації про мобільний номер.

Cardholder Verification – перевірка власника платіжної картки.

Fraud Payments Tracker – модуль для відстеження підозрілих платіжних операцій.

Crime Check Online – модуль для взаємодії з правоохоронними структурами (наприклад, кіберполіцією) для перевірки за даними про кримінальні інциденти.

Stolen IDentity (SID) - реєстр випадків використання викрадених цифрових особистостей із застосуванням deepfake в цілях фінансового шахрайства. Реєстр має функцію автоматизованого повідомлення фінансових установ про факти використання викрадених особистостей в їх інформаційних системах.

API-інтерфейси та веб-інтерфейс дають змогу інтегрувати перевірки у системи банку чи платіжної установи, а також використовувати через веб-портал AFH.

YouControl https://youcontrol.com.ua	Система YouControl дозволяє перевіряти фізичних осіб на ризики.
Опендатабот Опендатабот https://opendatabot.ua	Opendatabot надає доступ до державних реєстрів України, дозволяючи перевіряти штрафи, наявність арештів на автомобілі, інформацію про нерухомість, а також перевіряти осіб за ІПН та у базах розшуку.
VKURSI	VKURSI – це аналітична платформа, яка забезпечує ідентифікацію особи, перевірку на наявність у санкційних списках, переліках PEP і пов’язаних осіб. Сервіс агрегує дані з відкритих та офіційних джерел, дозволяє виявляти зв’язки фізичних осіб із бізнесом та іншими особами, оцінювати репутаційні ризики й налаштовувати автоматичний моніторинг змін.
SIDCON INTERNATIONAL CONSULTING COMPANY	Айсберг – аналітична інформаційна система від компанії «СІДКОН». Дозволяє здійснити перевірку фізичних осіб та аналіз пов’язаних осіб.

В2. Судові органи

Реєстр судових рішень Стан розгляду справ  https://reyestr.court.gov.ua/ https://court.gov.ua/fair	Єдиний державний реєстр судових рішень. Інформація щодо стадій розгляду судових справ.

Міжнародний кримінальний суд  Справи та провадження: https://www.icc-cpi.int/cases Пошук по судовим рішенням: https://www.icc-cpi.int/court-records	Міжнародний кримінальний суд – офіційний орган, що розглядає справи про найтяжчі міжнародні злочини, зокрема: геноцид, воєнні злочини, злочини проти людяності та злочини агресії. Сайт корисний коли фігурантом може бути особа, причетна до міжнародних злочинів.

Міжнародний суд ООН  **Список справ (All Cases)**: https://www.icj-cij.org/list-of-all-cases	Міжнародний суд ООН (International Court of Justice, ICJ) - це головний судовий орган Організації Об'єднаних Націй, який розглядає спори між державами, а не між фізичними чи юридичними особами. Можна знайти: позови між державами, включно з позовами України проти росії. Судові рішення (Judgmentsand Advisory Opinions): містить тексти рішень, які мають юридичну силу.

Архів судових рішень  https://www.worldcourts.com	WorldCourts.com – це архів міжнародного права та судових рішень, який збирає документи з понад 50 міжнародних та регіональних судів і трибуналів. Корисний інструмент для пошуку юридичної інформації, особливо у випадках, коли мова йде про міжнародні справи, права людини, кримінальні злочини, інвестиційні спори тощо.

https://e-justice.europa.eu/ecli	European Case Law Identifier – це європейська система пошуку судових рішень, яка уніфікує доступ до прецедентів та справ судів держав ЄС. Портал забезпечує уніфікований доступ до судових рішень країн ЄС.

Система дозволяє здійснювати пошук за єдиним ідентифікатором рішень (ECLI), охоплюючи як національні суди держав-членів, так і наднаціональні інституції – Суд Європейського Союзу (CJEU) та Європейський суд з прав людини (ECHR).

Платформа підтримує перехресний пошук у реєстрах різних країн, що суттєво спрощує перевірку судового бекграунду фізичних та юридичних осіб у міжнародному контексті.

B2. Перевірка чинності документів

	**Перевірка чинності документів**

Державна міграційна служба України (ДМСУ)	База даних недійсних, викрадених або втрачених документів, що посвідчують особу.
https://dmsu.gov.ua/services//nd.html	

C. КОМПАНІЇ ТА КОРПОРАТИВНА АНАЛІТИКА

C1. Інформація Міністерства юстиції України та НКЦПФР

	**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.

Єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадських формувань	Офіційний інструмент від Міністерства юстиції України для перевірки юридичних осіб, фізичних осіб-підприємців та громадських формувань.
https://usr.minjust.gov.ua/content/free-search	

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. Публікуються: нормативно-правові акти, реєстри учасників ринку, повідомлення, рішення, новини.

З метою захисту прав споживачів фінансових послуг Національна комісія з цінних паперів та фондового ринку здійснює моніторинг діяльності сумнівних інвестиційних проєктів (https://www.nssmc.gov.ua/activity/insha-diialnist/zakhyst-investoriv).

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).

С2. Національні аналітичні платформи

Аналітичні платформи – це цифрові інструменти, спрямовані на підвищення прозорості, безпеки, ефективності управління ризиками та прийняття рішень.

Інтернет адреси	Аналітичні платформи для перевірки компаній, зареєстрованих в Україні відіграють важливу роль у забезпеченні прозорості, безпеки та ефективності бізнесу. Ці сервіси працюють із відкритими державними даними, надаючи інструменти для перевірки юридичних та фізичних осіб, моніторингу змін у реєстрах, виявлення зв'язків, оцінки ризиків. Сервіси охоплюють дані з понад сотні джерел – від реєстрів юридичних осіб і судових рішень до санкційних списків, декларацій та державних закупівель.
https://youcontrol.com.ua https://vkursi.pro https://opendatabot.ua https://finap.com.ua https://sidcon.com.ua https://clarity-project.info https://ca.ligazakon.net	

YouControl / YC World https://youcontrol.com.ua https://youcontrol.world	YouControl та YCWorld – це аналітична система для бізнес-аналітики. Система формує інформацію на кожного суб'єкта та дозволяє візуалізувати зв'язки.

VKURSI https://vkursi.pro	VKURSI – це аналітична платформа, яка призначена для комплексної перевірки юридичних і фізичних осіб, моніторингу бізнес-структур і майна, а також аналізу ринку. Вона інтегрує дані з державних реєстрів, судових рішень, реєстрів майна (нерухомого та рухомого) та інших публічних джерел.

Опендатабот https://opendatabot.ua/open/russian-federation-business	Опендатабот – це інструмент для фінансового моніторингу та управління ризиками. Сервіс дозволяє аналізувати зв'язки компаній, групи компаній, перевіряти судові рішення та виявляти можливі зв'язки зі країною-агресором. Для перевірки фізичних осіб доступні різні підходи: ручна перевірка, масова обробка даних та автоматична перевірка через API.

Опендатабот спрощує процеси онбордингу та KYC, забезпечуючи відстеження змін статусу PEP-клієнтів, а також суттєвих змін у юридичних особах.

https://finap.com.ua	FinAP – це програмний комплекс, орієнтований на автоматизацію систем фінансового моніторингу та запобігання фінансовим зловживанням у банках, небанківських фінансових установах, страхових компаніях та інших суб'єктах, що підпадають під нормативи первинного фінансового моніторингу.

https://sidcon.com.ua	Айсберг – аналітична інформаційна система від компанії «СІДКОН», призначена для комплексної перевірки контрагентів, моніторингу ризиків та аналізу пов'язаних осіб. Система об'єднує дані з державних реєстрів, ЗМІ, відкритих джерел, санкційних списків, історичних масивів та власних баз користувача, формуючи повну картину діяльності компаній та фізичних осіб з 2000 року. Це глибокий аналітичний інструмент, який значно перевищує за можливостями класичні пошукові системи та агрегатори даних.

С3. Компанії в ЄС та Великобританії

	Реєстри підприємств – пошук компанії в ЄС.
https://e-justice.europa.eu/content_find_a_company-489-en.do	
Реєстри бізнесу, банкрутства та землі Інформація про бізнес, земельні реєстри та реєстри банкрутства на рівні ЄС та національному рівні.	
https://e-justice.europa.eu/514/EN/registers__business_insolvency_amp_land	
Реєстри підприємств у країнах ЄС У Європі бізнес-реєстри пропонують ряд послуг, які можуть відрізнятися від однієї держави-члена до іншої.	
https://e-justice.europa.eu/106/EN/business_registers_in_eu_countries	
Земельні книги - рівень ЄС У цьому розділі коротко обговорюються дії, вжиті для покращення координації між земельними реєстрами на європейському рівні.	
https://e-justice.europa.eu/108/EN/land_registers__eu_level	
Земельні книги в країнах ЄС	

Земельні реєстри в державах-членах пропонують широкий спектр послуг, які можуть відрізнятися від однієї країни до іншої.
https://e-justice.europa.eu/109/EN/land_registers_in_eu_countries
Реєстри банкрутства та неплатоспроможності Усі країни-члени ЄС мають реєстри неплатоспроможності та банкрутства, інформацію про які можна знайти. Ці реєстри знаходяться в процесі з'єднання та пошуку з центральної точки.
https://e-justice.europa.eu/110/EN/bankruptcy_and_insolvency_registers
Реєстри банкрутства та неплатоспроможності - пошук неплатоспроможних боржників в ЄС Пошук неплатоспроможних організацій, фізичних або юридичних осіб, у межах ЄС.
https://e-justice.europa.eu/246/EN/ bankruptcy_amp_insolvency_registers__search_for_insolvent_debtors_in_the_eu
Реєстри бенефіціарних власників – пошук інформації про бенефіціарних власників Система взаємозв'язку реєстрів бенефіціарної власності («BORIS») — це інструмент для підключення національних центральних реєстрів, що містять інформацію про бенефіціарну власність корпоративних та інших юридичних осіб, трастів та інших типів юридичних угод.
https://e-justice.europa.eu/38590/FR/beneficial_ownership_registers_interconnection_system_boris?action=maximize&clang=en&idSubpage=1

https://find-and-update.company-information.service.gov.uk	Офіційний реєстр компаній Великобританії, де можна безкоштовно шукати та переглядати інформацію про зареєстровані юридичні особи.

https://crbr.podatki.gov.pl https://crbr.podatki.gov.pl/adcrbr/#/wyszukaj	Реєстр CRBR– офіційна платформа для безкоштовного пошуку кінцевих бенефіціарів (UBO) компаній, зареєстрованих у Польщі. Доступна інформація про структуру власності, дати подання та оновлення даних за назвою.

С4. Європейські бізнес-реєстри та дані

Відкритий портал даних Європейського союзу http://data.europa.eu	Офіційний портал відкритих даних European Union, який надає доступ до даних, опублікованих установами, агентствами, органами ЄС, а також до метаданих із національних, регіональних і тематичних порталів даних Європи.

Відкритий портал даних Європейського союзу https://ebra.be/worldwide-registers	EBRA – асоціація фахівців з реєстрів підприємств у Європі, що співпрацює задля покращення роботи, управління та стандартизації бізнес-реєстрів. На сайті EBRA є картка, яка дозволяє шукати реєстри підприємств та компаній по всьому світу.

С5. Інформаційні платформи з аналізу компаній

Інформаційні ресурси щодо перевірки компаній нерезидентів

OpenCorporates	
https://opencorporates.com	OpenCorporates – це база відкритих корпоративних даних, яка надає доступ до інформації про компанії з усього світу. Платформа була заснована з метою підвищення прозорості бізнесу та боротьби з корупцією, шахрайством і відмиванням коштів. Зібрані дані містять назву організації, дату реєстрації, зареєстровані адреси, імена директорів та іншу корисну інформацію.

LSEG Risk Intelligence	
https://www.lseg.com	LSEG – це офіційний сайт London Stock Exchange Group (LSEG), до складу якої входить World-Check, один з провідних інструментів для перевірки ризиків, клієнтів і контрагентів (KYC/AML-screening), який раніше обслуговувався Refinitiv.

Sayari	Sayari – це аналітична платформа, що спеціалізується на прозорості бізнес-зв'язків, торгівлі та корпоративних мережах у глобальному масштабі. Сервіс для бізнес-розвідки, медіа-розслідувачів та аналітичних підрозділів правоохоронних органів, орієнтований на збір документів та інформації про комерційний і фінансовий світ. Платформа 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	

Orbis	Orbis – ресурс даних про приватні компанії, що також охоплює підприємства, які котируються на біржі. Він збирає широкий спектр даних, обробляє їх, доповнює та стандартизує, щоб зробити ці дані багатшими, потужнішими й легшими для інтеграції. Orbis, раніше флагманське рішення компанії Bureau van Dijk (BvD).
MOODY'S https://www.moodys.com https://login.moodys.com https://login.bvdinfo.com/Orbis	

	Рішення з управління ризиками та комплаєнсу. Ресурс для перевірки структури власності.
DOW JONES https://riskcenter.dowjones.com	

DatoCapital	Онлайн база про компанії та їх директорів.
en.datocapital.com	
Збирає відкриті дані про компанії та їхніх директорів з багатьох країн, включно з Великобританією, Іспанією, Панамою, Кайманові островами тощо. Він працює як агрегатор корпоративної інформації: ви можете знайти компанію за назвою або директором і переглянути її базову інформацію безкоштовно. За детальні звіти потрібно платити.	

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 PandoraPapers, ParadisePapers, BahamasLeaks, PanamaPapers та OffshoreLeaks.

https://www.marketscreener.com	MarketScreener – аналітична платформа, що надає комплексну інформацію про публічні компанії з усього світу.

Цей інструмент забезпечує огляд фінансових ринків, включаючи:

- дані про акції, облігації, ETF, індекси, сектори, валюти, криптовалюти та інші фінансові інструменти;
- профілі компаній, зокрема: структура власності, основні акціонери, обсяги випусків акцій, динаміка котирувань;
- макроекономічні показники, новини ринку, прогнози та інсайти для інвесторів.

С6. Ризикові юрисдикції: корпоративні дані та реєстри

https://egrul.nalog.ru	Податкова служба росії. Сайт містить дані про суб'єктів господарювання.
List-Org https://www.list-org.com	Основні відомості про будь-яку російську юридичну особу чи підприємця.
rupep https://rupep.org	База даних з інформацією про політично значущих осіб росії, білорусі, Казахстану та інших країн регіону. Інформація в базі базується на даних, зібраних із публічних джерел: державні сайти; офіційні державні реєстри; публікації в ЗМІ; інформація з витоку баз даних (ParadisePapers, PanamaPapers, Transbordercorruptionarchive, Aleph OCCRP тощо); профілі в соціальних мережах.

Засоби масової інформації почали більше розслідувань, які направлені на оточення керівництва росії.

ЗМІ	Опис	Адреса
Forbes	Публікує список російських товстосумів	https://www.forbes.ru
FinancialTimes	Почали стежити за найближчим оточенням керівництва росії та заможними олігархами.	https://www.ft.com
WallStreetJournal	Почали стежити за найближчим оточенням керівництва росії та заможними олігархами.	https://www.wsj.com

D. ЕЛЕКТРОННІ СЕРВІСИ КОНТРОЛЮ ДЕРЖАВНИХ ФІНАНСІВ

D1. Портал використання бюджетних котів

Єдиний веб-портал використання публічних коштів	Spending.gov.ua – це державна онлайн-платформа, створена для забезпечення прозорості витрат державних та місцевих бюджетів, а також інших розпорядників публічних коштів. Однією з ключових функцій є пошук транзакцій (виплат).
https://spending.gov.ua	

Користувачі можуть переглядати повну інформацію про бюджетні перекази: хто саме здійснив платіж, кому були перераховані кошти, яка сума була переказана, в яку дату та з яким призначенням.

Ще одна важлива функція — пошук розпорядників коштів, що дозволяє дізнатися, які державні органи, установи чи підприємства отримують і витрачають публічні кошти.

Портал також містить розділ фінансової аналітики, де через інтерактивні карти та графіки можна побачити, як розподіляються бюджетні кошти за регіонами та категоріями.

Окремо доступний пошук зобов’язань – інформація про заплановані витрати розпорядників коштів, навіть до фактичного здійснення платежу.

Щоб користуватися порталом, достатньо застосовувати фільтри за назвою організації, кодом ЄДРПОУ, періодом або сумами.

D2. Електронна система публічних закупівель

	Prozorro – це державна електронна система публічних закупівель. Цей портал дає змогу державним та комунальним установам оголошувати тендери на закупівлю товарів, послуг і робіт. Усі закупівлі проводяться в онлайн-режимі, а вся інформація про процес закупівлі є відкритою та доступною**.**
https://prozorro.gov.ua	

Система Prozorro суттєво знижує ризики корупції, сприяє економії державних коштів і підвищує довіру до державних інституцій.

D3. Громадський контроль публічних закупівель

DOZORRO	DOZORRO – це громадська ініціатива та онлайн-платформа, створена для моніторингу публічних закупівель в Україні. Вона заснована організацією Transparency International Ukraine і працює як інструмент громадського контролю: будь-хто може залишити звернення або зауваження щодо закупівлі через систему.
https://dozorro.org	

Платформа допомагає виявляти порушення, аналізувати ризики, створювати аналітику та передавати інформацію контролюючим органам.

Е. РЕПУТАЦІЙНІ ДЖЕРЕЛА ТА МЕДІА

Е1. Репутація в медіа

У межах напрямку «Репутація в медіа та журналістські розслідування» доцільним є використання авторитетних іноземних та українських джерел як додаткового інструмента для репутаційного аналізу клієнтів, контрагентів і пов’язаних осіб під час здійснення фінансового моніторингу.

Такі джерела допомагають виявляти корупційні ризики, згадки у кримінальних провадженнях, участь у тіньових схемах або фігурування у гучних публікаціях.

В Україні існує близько 15 активних джерел, які системно займаються журналістськими розслідуваннями, медіа-моніторингом або публікацією матеріалів про корупційні/фінансові ризики. Перелік основних, авторитетних в контексті фінансового моніторингу та KYC/AML може змінюватись.

F. ІНСТРУМЕНТИ OSINT ТА АРХІВУВАННЯ
F1. Набори корисних посилань

Фінансові посередники, правоохоронні та розвідувальні органи, журналісти також покладаються на ті ж інструменти, щоб дізнатися більше про злочин, підозрюваного, організацію чи особу, яка їх цікавить.

На жаль, слід також визнати, що шахраї та злочинці можуть використовувати ті ж самі інструменти та методи. Наприклад, при створенні фальшивого посвідчення особи шахрай може об'єднати дані, отримані з даркнет-ринку, з даними, отриманими з відкритих джерел.

Посилання	Опис
https://www.maltego.com	Професійна платформа для збору та аналізу відкритих даних (OSINT), яка дозволяє будувати графічні зв'язки між різними сутностями.
Maltego використовується в кіберрозслідуваннях, журналістиці, аналітиці загроз і пентестингу для виявлення прихованих зв'язків та інфраструктур. Система працює за принципом автоматизованих запитів до баз даних, що формують інтерактивні графи. Maltego доступна у безкоштовній версії з обмеженнями, а також у комерційних варіантах з розширеним функціоналом.	
https://osintframework.com	Спеціалізований веб-ресурс, який містить великий каталог інструментів та ресурсів для збору відкритої інформації (OSINT).
Ресурс був створений із фокусом на безкоштовні чи умовно-безкоштовні онлайн-інструменти, які допомагають у пошуку публічних даних – зокрема, за доменами, адресами, соціальними мережами, документами тощо. Ресурс охоплює різноманітні категорії, надаючи упорядкований список інструментів: наприклад, за іменами користувачів, електронною поштою, юзеракаунтами, геолокацією, публічними записами тощо.	
https://gijn.org/ru/istorii/sovety-po-poisku-tajnyh-vladelcev-podstavnyh-kompanij	Набір корисних посилань для пошуку даних про корпорації та їх власників.

F2. Інструменти доступу до архівних вебданих

https://public.govdelivery.com	GovDelivery – це система для управління підписками на інформаційні розсилки від державних установ. Вона дозволяє користувачам підписуватися на теми, які їх цікавлять, і отримувати електронні листи тоді, коли установа публікує відповідну інформацію.

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.
https://cachedview.com	Інструмент для перегляду вмісту вебсторінки. Онлайн-інструмент, що підтримується Google і деякими іншими середовищами.

G. ВІРТУАЛЬНІ АКТИВИ

G1. Аналітика віртуальних активів

	У 2025 році спостерігається стрімке зростання обсягів операцій із віртуальними активами, що супроводжується ускладненням схем їх використання у злочинних цілях. Серед ключових трендів – активне застосування децентралізованих фінансових сервісів (DeFi), зростання обсягів транзакцій у стейблкоїнах, використання анонімізуючих протоколів та міжмережевих (крос-чейн) транзакцій.

Важливо використовувати **розширену аналітику**, яка враховує нові способи приховування походження цифрових активів. Один із таких напрямів – це **крос-чейн аналітика** (аналіз транзакцій між різними блокчейнами – наприклад, коли криптовалюта переміщується з мережі Bitcoin до Ethereum через так звані «мости»). Такий підхід допомагає відстежити шляхи руху коштів навіть тоді, коли зловмисники намагаються «розмити сліди», використовуючи складні технічні рішення.

Крім того, зростає потреба у **моніторингу стейблкоїнів –** це криптовалюти, прив’язані до фіатних валют (наприклад, долара США), які можуть використовуватись для уникнення моніторингу, зокрема у схемах обходу санкцій або «відмивання» коштів.

Для аналізу криптовалютних транзакцій можна використовувати набір відкритих та платних онлайн-інструментів:

Провідники блокчейнів (Blockchain Explorers). Це онлайн-платформи, які дозволяють переглядати транзакції, баланси гаманців, блоки та інші дані на конкретному блокчейні:

BTCScan – для перегляду транзакцій у мережі Bitcoin.

Etherscan – провідний оглядач блокчейну Ethereum.

Tronscan – оглядач для мережі Tron.

Chainz (Litecoin) – блокчейн-оглядач для Litecoin.

Крипторейтинги, ринки, ціни та біржі. Ці сайти агрегують інформацію про криптовалюти, їхню ринкову капіталізацію, динаміку цін, обсяги торгів та платформи обміну:

CoinGecko – популярний агрегатор інформації про криптовалюти, токени, біржі, DeFi-проєкти.

CoinMarketCap – ще один провідний агрегатор цін і ринкових даних.

Аналітичні платформи для аналізу ринку.

Для аналізу ринку віртуальних активів застосовуються аналітичні платформи, які забезпечують дослідження даних, що зберігаються безпосередньо в блокчейні (on-chain), а також даних поза мережею блокчейна (off-chain).

Santiment – платформа криптоаналітики для сигналів та контексту. Посилання: https://santiment.net

Glassnode спеціалізується на аналізі блокчейн-мереж, пропонуючи метрики потоків, ліквідності та активності власників. Посилання: https://glassnode.com

CryptoMiso оцінює проєкти за активністю, що є важливим критерієм визначення життєздатності та надійності криптоактивів. Посилання: https://www.cryptomiso.com

CoinMetrics забезпечує формування аналітичних даних, які використовуються для моніторингу ризиків та побудови моделей фінансової аналітики. Посилання: https://coinmetrics.io

Інструменти для аналізу ризиків, трейсингу та AML.

Більш складні платформи (часто платні), які застосовують аналітику для ідентифікації джерел походження коштів, перевірки гаманців, виявлення шахрайства чи відмивання коштів: Chainalysis, Crystal Blockchain, Elliptic, TRM Labs, Scorechain.

Ці ресурси є ключовими інструментами у сфері комплаєнсу, AML (протидія відмиванню коштів) та OSINT-аналітики в екосистемі криптовалют. Вони можуть використовуватися як фінансовими установами, так і правоохоронними органами для виявлення порушень та посилення контролю над віртуальними активами.

Чорні списки криптогаманців. Існують спеціалізовані **чорні списки криптогаманців** та осіб, пов'язаних із хакерськими угрупованнями або підсанкційною діяльністю. Вони використовуються для моніторингу та блокування транзакцій, пов'язаних із відмиванням коштів, кібершахрайством чи фінансуванням тероризму, що дозволяє ефективно виявляти ризикові фінансові операції у криптопросторі.

Інформування регулятора.

	Національний банк України здійснює регулярні публікації про порушення на фінансовому ринку з метою захисту споживачів. Наприклад, щодо ведення незаконної діяльності онлайн-сервісів з надання позик у криптоактивах споживачам. Поглиблений аналіз регулятора показав, що сервіси формально надають позики в USDT, а фактично видають кредити в національній валюті України.

Національний банк України публікує на офіційному сайті перелік установ, які здійснюють кредитування фізичних осіб без дотримання вимог чинного законодавства України та уникаючи відповідного нагляду Національного банку, в тому числі шляхом маскування послуг з надання кредитів під нібито інші правочини (Захист прав споживачів/Попередження: безліцензійна діяльність). Посилання: https://bank.gov.ua/ua/consumer-protection/bezlicenzijna-djalnist-fraud

H. ТРАНСПОРТУВАННЯ, ЛОГІСТИКА ТА МОБІЛЬНІСТЬ

H1. Відстеження літаків

	У 2025 році моніторинг авіаційного трафіку залишається важливою частиною OSINT-аналізу, зокрема у сфері протидії відмиванню коштів, фінансуванню тероризму, незаконним перевезенням.

Завдяки розвитку цифрових технологій, онлайн-платформи дозволяють відстежувати польоти в режимі реального часу з використанням GPS, ADS-B, MLAT та супутникових даних.

Спостереження за авіацією через аеродроми та їх оточення.

Використання відкритих джерел (OSINT) для моніторингу авіації є ефективним інструментом у розслідуваннях, пов'язаних із відмиванням коштів, фінансуванням тероризму та іншими злочинами.

Аналіз аеродромів і маршрутів літаків, особливо тих, що регулярно відвідують нетипові локації без очевидної логістичної мети, дозволяє виявляти потенційно незаконні фінансові схеми. Аеропорти, як точки концентрації капіталу, вантажів і пасажирів, часто виступають ключовими орієнтирами для OSINT-розслідувань.

Одним із головних ідентифікаторів літака є його реєстраційний номер (tailnumber), який може змінюватися. Водночас серійний номер (MSN) залишається незмінним і дозволяє точно відстежувати історію та переміщення повітряного судна.

Атрибути для пошуку	Назва ресурсу	Посилання на сайт	Опис ресурсу
Фотографії повітряних суден			
Модель літака, тип повітряного судна	Planespotters.net	planespotters.net	Вебсайт з фотографіями повітряних суден, що допомагає ідентифікувати літаки.
Модель літака, хвостовий номер	JetPhotos.com	jetphotos.com	База даних з фотографіями літаків та можливістю пошуку за реєстраційним номером.
Відстеження польотів			
Номер рейсу, місце знаходження	Flightradar24	flightradar24.com	Вебсайт для відстеження польотів у реальному часі по всьому світу.
Номер рейсу, місце знаходження	ADSBExchange	globe.adsbexchange.com	Глобальна мережа для обміну даними по відстеженню літаків за допомогою ADS-B.
Номер рейсу, місце знаходження	RadarBox	radarbox.com	Платформа для відстеження рейсів та аналізу даних авіаперевезень.
Номер рейсу, місце знаходження	FlightAware	flightaware.com	Платформа для відстеження рейсів з можливістю перегляду історії польотів.

Н2. Відстеження кораблів

У 2025 році онлайн-сервіси для відстеження морських суден залишаються ключовим джерелом у розслідуваннях, пов’язаних із обходом санкцій, незаконними постачаннями та відмиванням коштів.

Відстеження руху кораблів особливо важливе для викриття «тіньового флоту», що здійснює перевезення без розголошення пунктів призначення або вантажів. Частина суден, зокрема російських, маніпулює сигналами AIS (Automatic Identification System) – системи, яка призначена для безпеки судноплавства та контролю вантажів. Через такі маніпуляції створюються фіктивні маршрути або «зникають» ділянки подорожі, що ускладнює контроль за дотриманням санкційного режиму.

Відстеження суден	Опис ресурсу
IMO https://webaccounts.imo.org	Глобальна інтегрована інформаційна система судноплавства.
IMO Web Accounts – це офіційна система облікових записів Міжнародної морської організації (IMO), яка забезпечує централізований доступ до низки цифрових сервісів організації. Користувачі можуть отримати доступ до таких ресурсів, як IMODOCS (документи IMO), GISIS (інформація про судна, компанії, інциденти), IMO e-Learning, IMO Publishing та інших платформ. Система підтримує два типи користувачів. PublicAccount – для широкої аудиторії (аналітики, дослідники, журналісти, фахівці у сфері безпеки морських перевезень). MemberState/OrganizationAccount – для уповноважених представників держав-членів або офіційних спостерігачів IMO. У сфері OSINT-аналізу обліковий запис IMO є корисним для: дослідження суден та судноплавних компаній, перевірки фактів про інциденти чи санкції, вивчення морської логістики та безпеки.	
Equasis https://www.equasis.org	Онлайн-сервіс, який надає відкриту інформацію про морські судна та судноплавні компанії.
Платформа дозволяє безкоштовно (після реєстрації) шукати дані про конкретні судна або компанії, переглядати їх історію, класифікацію, прапори, та інші характеристики.	
MarineTraffic https://www.marinetraffic.com	Онлайн-сервіс, що дозволяє в режимі близькому до реального часу відслідковувати положення суден по всьому світу.

Сервіс використовує дані системи AIS (Automatic Identification System), яка передає таку інформацію як ім’я судна, його курс, швидкість, місце положення. Сервіс містить базу даних щодо кораблів (наприклад, де побудовано, які габарити, тоннаж, IMO-номер) та портів, а також надає карту з відображенням суден у реальному часі. Базова версія доступна безкоштовно, але розширені можливості надаються за підпискою.	
VesselFinder https://www.vesselfinder.com	Онлайн-платформа, яка дозволяє відстежувати судна в режимі реального часу. Використовує мережу наземних AIS-приймачів та супутникові дані.
Сервіс дозволяє шукати судна за назвою, IMO або MMSI-номером, переглядати їхнє місце розташування, курс, швидкість, порт призначення, ETA, а також отримувати технічну інформацію про судно. Окрім безкоштовної базової версії, доступні платні підписки та API-доступ, що дають можливість історичного трекінгу, відстеження флоту, доступу до детальних даних.	

Н3. Дані про логістику та торгівлю товарами

Бази даних про міжнародні поставки залишаються ключовим інструментом OSINT-аналізу у 2025 році, особливо коли досліджуваний суб’єкт займається транспортуванням або торгівлею товарами.

У контексті протидії відмиванню коштів та фінансуванню тероризму ці бази даних допомагають: виявляти ризики, пов’язані з фіктивним експортом або імпортом; аналізувати ланцюги поставок, де можуть використовуватись компанії-«прокладки»; фіксувати факти обходу санкцій, зокрема шляхом переорієнтації маршрутів, зміни документів або використання третіх країн.

Особливо важливими є дані з морських реєстрів, портів, митниць, а також інтегровані дані з глобальних платформ. Вони дозволяють:

- зіставляти фактичні логістичні дії з офіційною документацією;
- виявляти аномалії в маршрутах постачання;
- ідентифікувати можливі канали фінансування тероризму через логістику;
- виявляти фіктивні постачання, що можуть слугувати прикриттям для відмивання коштів;
- ідентифікувати компанії, що торгують товарами подвійного призначення;
- виявляти обхід міжнародних санкцій. Аналізувати ланцюги поставок, пов’язані з санкційними юрисдикціями;
- знаходити випадки завищення цін чи обсягів товарів для легалізації доходів.

Бази даних допомагають забезпечити прозорість операцій, посилити контроль за фінансовими та логістичними потоками, а також запобігти використанню міжнародної торгівлі у злочинних схемах.

Імпортно/експортні операції	Пошук глобальних записів імпорту/експорту від митниці США. ImportGenius має повні дані про торгівлю для 18 країн. ImportGenius відстежує транспортну діяльність по всьому світу, щоб показати, що саме відбувається в імпортно-експортному бізнесі.
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.
https://panjiva.com	

Імпортно/експортні операції	Дані про імпорт із США, а також записи про глобальний експорт та імпорт. Онлайн-платформа, яка надає доступ до митних та логістичних даних, зокрема щодо імпортно-експортних операцій. Сервіс спеціалізується на зборі, структуризації та аналізі вантажних документів, зокрема коносаментів, даних про судна, одержувачів та відправників товарів, а також маршрутів переміщення вантажів.
https://importkey.com	

ЗАСТЕРЕЖЕННЯ

Практичний OSINT і кібергігієна аналітика.

OSINT потребує володіння технічними навичками, зокрема в роботі з пошуковими операторами, аналітичними платформами, візуалізаційними інструментами та базами даних. Фахівець має вміти застосовувати ці знання для збору, фільтрації та інтерпретації відкритої інформації.

Світ відкритих даних постійно змінюється: з'являються нові платформи, змінюються алгоритми пошуку, посилюються обмеження доступу. Тому фахівець має постійно вдосконалювати свої знання, вивчати нові інструменти та слідкувати за трендами в галузі OSINT.

Робота з відкритими джерелами, особливо в умовах військової агресії, вимагає високого рівня цифрової гігієни. Фахівці повинні захищати свої пристрої, особисті дані й онлайн-активність від можливого стеження, зламів або викриття.