АКТУАЛЬНІ МЕТОДИ, СПОСОБИ, ІНСТРУМЕНТИ ЛЕГАЛІЗАЦІЇ (ВІДМИВАННЯ) ЗЛОЧИННИХ ДОХОДІВ ТА ФІНАНСУВАННЯ ТЕРОРИЗМУ (СЕПАРАТИЗМУ)

2021

Державна служба
фінансового моніторингу
України

Державна служба фінансового моніторингу України

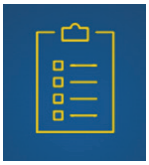
АКТУАЛЬНІ МЕТОДИ, СПОСОБИ, ІНСТРУМЕНТИ ЛЕГАЛІЗАЦІЇ (ВІДМИВАННЯ) ЗЛОЧИННИХ ДОХОДІВ ТА ФІНАНСУВАННЯ ТЕРОРИЗМУ (СЕПАРАТИЗМУ)

Київ 2021

Держфінмоніторинг створено як підрозділ фінансової розвідки та призначений для протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, та фінансуванню тероризму.

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

Ключова роль Держфінмоніторингу полягає в тому, що він відпрацьовує отримані від суб'єктів первинного фінансового моніторингу повідомлення про підозрілі фінансові операції та передає правоохоронним і розвідувальним органам України узагальнені матеріали у разі наявності підозр щодо ВК/ФТ/ЗМЗ.



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

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

EUACI EUROPEAN UNION ANTI-CORRUPTION INITIATIVE

Збірка реалізована за підтримки Антикорупційної ініціативи ЄС (EUACI)

ЗАТВЕРДЖЕНО
Наказ Державної служби
фінансового моніторингу України
20.12.2021 №146

Типологічне дослідження на тему: «Актуальні методи, способи, інструменти легалізації (відмивання) злочинних доходів та фінансування тероризму (сепаратизму)»

У типологічному дослідженні проведено вивчення питань, пов'язаних з виявленням, розкриттям та розслідуванням актуальних схем легалізації (відмивання) злочинних доходів та фінансування тероризму (сепаратизму), розкрито зміст і характеристику різних схем відмивання доходів та вчинення інших злочинів.

Висвітлено методи, способи та інструменти легалізації (відмивання) злочинних доходів та фінансування тероризму (сепаратизму), індикатори виявлення учасників протиправних схем.

Визначена важлива роль застосування ризико-орієнтованого підходу з метою стримування вищевказаних злочинів.

Типологічне дослідження може стати підґрунтям для визначення підозрілості фінансової операції або діяльності з відмивання доходів та вчинення інших злочинів.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

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

ПЕРЕДМОВА

Дане типологічне дослідження відображає актуальні схеми легалізації (відмивання) злочинних доходів та фінансування тероризму (сепаратизму) та інших злочинів.

Досвід останніх років дозволив визначитись зі структуруванням схем за певними найбільш поширеними категоріями кейсів, щодо яких здійснювались фінансові розслідування.

Зокрема, Держфінмоніторингом за останні роки проведено типологічні дослідження за наступними актуальними тематиками: відмивання коштів від податкових злочинів (2020 рік), привласнення коштів і майна державних підприємств та інших суб'єктів, які фінансуються за рахунок державного та місцевих бюджетів (2019 рік), ризики використання суб'єктів з непрозорою структурою власності у схемах відмивання кримінальних доходів (2018 рік), ризики використання готівки (2017 рік), ризики тероризму та сепаратизму (2017 рік), відмивання доходів, отриманих від корупційних діянь (2016 рік) та інші.

Типологічні дослідження Держфінмоніторингу надали змогу суб'єктам фінансового моніторингу сформувати уявлення про ризики та покращити практику застосування ризик-орієнтованого підходу.

В цілому, слід зазначити, що типології відмивання коштів та фінансування тероризму швидко еволюціонують, але розуміння учасниками системи ПВК/ФТ ідентифікованих схем надає можливості для впровадження відповідних заходів, що мінімізують можливу шкоду.

Зважаючи на негативний вплив на економіку країни злочинних доходів, що продукуються в різних сферах та видах злочинів, Держфінмоніторингом обрано відповідну тему, що містить актуальні тенденції у схемах, що використовуються.

ВСТУП

З початку 2020 року пандемія COVID-19 вплинула не тільки на громадян та економічні процеси в державі, але й на схеми відмивання доходів, одержаних злочинним шляхом, фінансування тероризму та фінансування розповсюдження зброї масового знищення.

Під впливом пандемії COVID-19 відбулись певні зміни в економічних процесах у застосуванні нових сучасних технологій для здійснення фінансової діяльності, що надало можливості злочинцям відкрити нові можливості для вчинення економічних злочинів та отримання злочинних доходів.

Значно збільшились випадки різноманітного шахрайства, вчинення кіберзлочинів та використання новітніх технологій для їх вчинення.

У зв'язку з цим, цілком логічно, що Держфінмоніторингом здійснюється активна робота стосовно дослідження та фінансового розслідування наступних фактів:

a. відмивання доходів, отриманих від корупційних діянь;
b. відмивання доходів, отриманих від розкрадання, нецільового використання державних коштів та коштів суб'єктів господарювання державного сектору економіки;
c. відмивання доходів від податкових злочинів;
d. розслідування справ, пов'язаних з фінансуванням тероризму та сепаратизму;
e. відмивання доходів через страховий ринок та ринок цінних паперів;
f. відмивання доходів, отриманих від торгівлі зброєю;
g. відмивання доходів, отриманих від торгівлі наркотичними та психотропними речовинами;
h. відмивання доходів, отриманих від торгівлі людьми та розповсюдження відео зображень порнографічного характеру;
i. відмивання доходів від вчинення шахрайських дій;
j. відмивання доходів від кіберзлочинів;
k. вчинення злочинів та відмивання доходів через віртуальні активи.

Метою даного дослідження є аналіз та узагальнення інструментів, індикаторів та способів ВК/ФТ/ЗМЗ.

У типологічному дослідженні використано практику учасників національної системи фінансового моніторингу.

РОЗДІЛ І.
ЗАГАЛЬНІ ТЕНДЕНЦІЇ

1.1. Загрози та ризики щодо вчинення незаконних фінансових операцій

Економічна безпека держави є складовою її національної безпеки та перебуває в тісному взаємозв'язку з усіма економічними процесами, що відбуваються в суспільстві.

Злочини у сфері відмивання коштів вчиняються не лише з метою подальшого використання отриманих доходів у економічній діяльності для одержання прибутку, або задля власного збагачення осіб, але й для фінансування тероризму, незаконного обігу зброї, організації вбивств на замовлення, фінансування груп сепаратистського спрямування та інших злочинів.

Україна протягом останніх років перебуває у стані терористичної загрози та загрози сепаратизму. Використання фінансової системи з метою інтеграції та переадресації фінансових потоків, що спрямовуються на підтримку такої злочинної діяльності, – це виклик для держави.

Економічна злочинність в Україні характеризується постійним вдосконаленням схем ВК/ФТ. Зокрема, існують масштабні зловживання з бюджетними коштами, прояви корупції, виведення капіталів в іноземні юрисдикції, діяльності конвертаційних центрів («скруток»), шахрайства, ухилення від сплати податків та зборів, приховування реальних власників інвестиційних проєктів, які інвестують в найбільш прибуткові галузі економіки тощо.

Поширення тіньової економіки та зростання організованої злочинності значною мірою підриває національну економічну безпеку України.

Виявлення та руйнування схем легалізації доходів, одержаних злочинним шляхом, фінансування тероризму є цілеспрямованою роботою суб'єктів фінансового моніторингу та правоохоронних органів, які виявляють та розслідують економічні злочини.

Держфінмоніторингом протягом травня 2020 – вересня 2021 років отримано від суб'єктів первинного фінансового моніторингу 37 728 (у 2020 – 11 465 та у 2021 – 25 763) повідомлень про підозрілі фінансові операції (діяльність).

Привертає увагу, що як у 2020, так і у 2021 році понад 50% підозрілих операцій та «кейсів» приходили з ознакою «Інші ознаки», тобто суб'єкти первинного фінансового моніторингу визначали інші підозри. Практика аналізу таких повідомлень та «кейсів» свідчить, що це суб'єкти господарювання, які мають ознаки «фіктивності», їх операції носять «транзитний характер» з

метою «надання послуг» з ухилення від сплати податків через механізм «зустрічних потоків», «скруток», з подальшим обготівковуванням.

Також, значна кількість кейсів за 2021 рік отримані за підозрою «конвертація безготівкових коштів у готівку», «фінансові операції з активами, що не відповідають профілю клієнта», «фіктивне підприємництво», «шахрайські дії».

Переважна більшість підозрілих операцій та «кейсів» (80%) пов'язані з схемами щодо ухилення від сплати податків та зборів.

1.2. Ризики залучення суб'єктів господарювання в розрізі видів діяльності до вчинення ВК/ФТ/ЗМЗ

В залежності від виду діяльності суб'єкти мають різний ризик бути залученими до вчинення ВК/ФТ/ФЗМЗ. Детальна інформація щодо ймовірного рівня ризику наведена у таблиці.

Ризик різних суб'єктів господарювання за видом діяльності[1]

Секція	A	Назва виду діяльності	Сільське господарство, лісове господарство та рибне господарство
Ризики за видом діяльності	Фактором ризику для зазначених видів діяльності є використання значних обсягів готівки для проведення розрахунків з контрагентами та важкий контроль реальних обсягів виробництва/вирощування/продажу продукції. Даний фактор значно ускладнює контроль та відстеження обсягів розрахунків з кожним окремим суб'єктом господарювання. У багатьох випадках відсутні документи, що підтверджують розрахунки, а також вид діяльності дає можливість формувати продукцію поза обліком шляхом заниження показників виробництва. Можливі ризики: • здійснення експортних операцій без повернення валютної виручки або введення в обіг продукції невідомого походження. За різними оцінками, значна частина обсягу земель сільськогосподарського призначення обробляється поза межами обліку та сплати податків.		

1 Джерело: результати опитування суб'єктів державного фінансового моніторингу та правоохоронних органів

Секція	B	Назва виду діяльності	Добувна промисловість і розроблення кар'єрів
Ризики за видом діяльності	Даний вид діяльності передбачає видобуток корисних копалин, реальні обсяги видобутку яких важко контролювати. Суб'єкти господарювання, які здійснюють діяльність даного виду, мають можливість приховати реальні обсяги видобутих корисних копалин, не обліковувати їх на балансі підприємств та продати їх неофіційно, тим самим ухилившись від сплати податків та зборів. Можливі ризики: • привласнення значної частини видобутих корисних копалин; • заниження податків при продажу корисних копалин, а також за користування надрами; • здійснення видобутку корисних копалин без оформлення дозвільних документів.		

Секція	C	Назва виду діяльності	Переробна промисловість
Ризики за видом діяльності	Існує можливість формувати продукцію поза обліком шляхом закупівлі сировини за готівку та заниження показників виробництва. Також є ризик у завищенні витрат для ухилення від сплати податків. Можливі ризики: • виробництво та продаж не облікованої продукції; • придбання значної частини сировини у фізичних осіб-підприємців, які перебувають на спрощеній системі оподаткування (можлива конвертація); • декларування податкового кредиту від суб'єктів господарської діяльності з ознаками «фіктивності».		

Секція	D	Назва виду діяльності	Постачання електроенергії, газу, пари та кондиційованого повітря
Ризики за видом діяльності	Для даного виду діяльності характерні наступні ризики: складність визначення споживчого попиту; маніпуляції учасників ринку; відсутність досконалої конкуренції на ринку (непрозоре встановлення тарифів); відсутність можливості контролю здійснення виконання зобов'язань контрагентами. Можливі ризики: • отримання незаконних доходів від схем використання енергоносіїв; • декларування податкового кредиту від суб'єктів господарської діяльності з ознаками «фіктивності»; • взаємовідносини з фізичними особами-підприємцями, які перебувають на спрощеній системі оподаткування (можлива конвертація безготівкових коштів у готівку).		

Секція	E	Назва виду діяльності	Водопостачання, каналізація, поводження з відходами
Ризики за видом діяльності	Відносно ризиків у цій діяльності слід зазначити: непрозорість системи оплати за надані послуги; відсутність ефективного контролю за компаніями сектору житлово-комунального господарства; відсутність можливості контролю здійснення виконання зобов'язань контрагентами.		

Секція	F	Назва виду діяльності	Будівництво
Ризики за видом діяльності	Даний вид діяльності є високоприбутковим, але діяльність суб'єктів господарювання даного виду потребує значних неофіційних «видатків» для її здійснення. Це своєю чергою зумовлює необхідність виведення коштів в тіньовий обіг, тим самим ухилившись від сплати податків та зборів. Здійснення будівництва передбачає використання ресурсів (будівельних матеріалів) в значних обсягах, що дає змогу суб'єктам господарювання завищувати показники реального об'єму використаних ресурсів, тим самим завищуючи валові видатки та ухиляючись від сплати податків та зборів. Також слід відзначити: значний рівень корупції в будівельній сфері; можливе використання коштів не за цільовим призначенням; недобросовісність забудовників та шахрайські схеми; використання великої кількості субпідрядників; відсутність ефективного контролю. Можливі ризики: • несплата податків та ВК у будівництві з використанням інститутів спільного інвестування; • оформлення продажу квартир через громадян, які не зареєстровані як суб'єкти підприємницької діяльності; • привласнення бюджетних коштів, які виділяються для цільових програм; • декларування податкового кредиту від суб'єктів господарської діяльності з ознаками «фіктивності».		

Секція	G	Назва виду діяльності	Оптова та роздрібна торгівля; ремонт автотранспортних засобів і мотоциклів
Ризики за видом діяльності	Підприємства оптової торгівлі можуть бути використані для «транзитних» операцій та формування податкового кредиту. Великі підприємства роздрібної торгівлі можуть виступати «продавцями» готівки. Фактори ризику у цій сфері: велика кількість обігу готівкових коштів; використання схем ухилення від сплати податків з використанням механізмів «транзиту», «скруток»; фіктивне підприємництво; конвертаційні центри; здійснення незаконних валютних операцій за фіктивними зовнішньоекономічними контрактами; значна кількість учасників фінансових операцій; великий ступінь «тінізації»; здійснення схемних імпортних операцій; оформлення продажів через фізичних осіб-підприємців, які перебувають на спрощеній системі оподаткування, для мінімізації прибутків; незаконний продаж підакцизних товарів; виплата заробітної плати «в конвертах»; використання готівки для ведення бізнесу; «продаж» податкового кредиту суб'єктам реального сектору економіки для мінімізації податків. На ринку роздрібної торгівлі товари, які потрапили в Україну або були вироблені без сплати податків, реалізуються за такими схемами: • повністю нелегальна («чорна») торгівля, коли товари реалізуються без сплати будь-яких податків та без оформлення документів. Така схема масово використовується в реалізації тютюнових виробів; • торгівля в магазинах, кіосках, АЗС тощо, які мають реєстраційні документи (ТОВ, ФОП), проте через систему реєстрації розрахункових операцій реалізується лише частина товарів, інша частина реалізується без фіскальних чеків або з видачею псевдофіскального чека. Така схема масово використовується в реалізації алкоголю, тютюнових виробів, паливо-мастильних матеріалів; • дистанційна торгівля алкогольною продукцією через мережу Інтернет без використання реєстратора розрахункових операцій та без відображення реальних обсягів продажів у деклараціях.		

Секція	H	Назва виду діяльності	Транспорт, складське господарство, поштова та кур'єрська діяльність
Ризики за видом діяльності	За допомогою транспортних підприємств та складських господарств можуть формуватися підвищені витрати. Маскування ввезення промислових партій товарів на митну територію України під поштові та кур'єрські відправлення або під виглядом особистого імпорту або провезення особистих речей – ввезення фізичними особами товарів у ручній поклажі або у супроводжуваному багажі (велика партія товару за допомогою стійких угрупувань з декількох десятків або сотень фізичних осіб (частіше мешканців прикордонних районів) дрібниться на дозволені до безплатного провезення партії, а після перетину кордону пішки або на автомобілях чи автобусах, збирається в одному місті та розвозиться по всій країні).		

Секція	I	Назва виду діяльності	Тимчасове розміщування й організація харчування
Ризики за видом діяльності	Даний вид діяльності дає можливість формувати продукцію поза обліком шляхом закупівлі сировини за готівку та заниження показників виробництва. Фактори ризику: значний обіг готівкових коштів; велика кількість суб'єктів господарювання; складність належного контролю за обсягом наданих послуг; неофіційне працевлаштування працівників та виплата заробітної плати «в конвертах».		

Секція	J	Назва виду діяльності	Інформація та телекомунікації
Ризики за видом діяльності	Даний вид діяльності є складним з боку контролю. Зокрема, з публічного збору благодійних пожертв із використанням телекомунікаційних повідомлень.		

Секція	K	Назва виду діяльності	Фінансова та страхова діяльність
Ризики за видом діяльності	Даний вид об'єднує діяльність фінансових та страхових компаній, які мають можливість сприяти в ухиленні від сплати податків з використанням інструментів, що характерні для даних видів діяльності (наприклад: договори відступлення боргу, позики, договори факторингу, перестрахування, цінні папери тощо). Можливі приклади залучення фінансових та страхових компаній до схем ВК: • «схемне» страхування та/або перестрахування; • організація фіктивних страхових випадків; • ухилення від сплати податків та зборів; • отримання страховою компанією грошових коштів за малоймовірними страховими ризиками з перерахуванням коштів на користь підприємств з ознаками фіктивності; • проведення операцій з перестрахування між значною кількістю підконтрольних СК без декларування отриманих доходів; • перерахування СК значних сум коштів ФОПам за удаваними агентськими угодами; • видача фінансовими та банківськими установами кредитів афілійованим позичальникам; • ділові відносини з компаніями з ознаками фіктивності; • виведення майна з-під застави шляхом переведення права власності на третіх осіб; • необґрунтоване використання операцій фінансової допомоги.		

Секція	L	Назва виду діяльності	Операції з нерухомим майном
Ризики за видом діяльності	Заниження реальних цін з метою зменшення податків, нерухоме майно має балансову та ринкову вартість, тому суб'єкти мають можливість здійснюючи продаж нерухомого майна за балансовою вартістю (яка зазвичай є нижчою від ринкової), тим самим не показуючи реальний дохід від продажу майна та ухиляючись від сплати податків. Також слід відзначити: спекулятивні операції купівлі-продажу; значний обіг готівкових коштів; правову несвідомість переважної частини українців.		

Секція	M	Назва виду діяльності	Професійна, наукова та технічна діяльність
Ризики за видом діяльності	Можливе використання неофіційної робочої сили (заробітна плата «у конвертах»).		

Секція	N	Назва виду діяльності	Діяльність у сфері адміністративного та допоміжного обслуговування
Ризики за видом діяльності	Можливе використання неофіційної робочої сили (заробітна плата «у конвертах»).		

Секція	O	Назва виду діяльності	Державне управління й оборона; обов'язкове соціальне страхування
Ризики за видом діяльності	Значний рівень ризику притаманний оборонній сфері, оскільки оборонний сектор передбачає значні обсяги фінансування з державного бюджету, чим користуються недобросовісні посадові особи та суб'єкти господарювання, тим самим здійснюючи розкрадання коштів державного бюджету через сумнівні тендери, завищення цін тощо. Відносно будівництва масштабних інфраструктурних об'єктів є можливість отримання незаконних доходів у вигляді хабарів. Загалом слід відзначити: значний рівень корупції серед державних службовців та політично значущих осіб. Ризик нецільового витрачання коштів з державного та місцевих бюджетів.		

Секція	P	Назва виду діяльності	Освіта
Ризики за видом діяльності	На ризики у цій сфері можуть впливати: системність корупції; недостатній рівень відкритості та прозорості.		

Секція	Q	Назва виду діяльності	Охорона здоров'я та надання соціальної допомоги
Ризики за видом діяльності	Можлива корупційна складова при проведенні тендерів підприємствами державної/комунальної власності щодо закупівлі обладнання, препаратів та отримання посадовими особами так званих «відкатів». На ризики у цій сфері можуть впливати: системність корупції; недостатній рівень відкритості та прозорості; розкрадання бюджетних коштів; різноманітні незаконні оборудки (фальсифікація, підробка документів). Існує ризик привласнення бюджетних коштів шляхом завищення витрат на придбання товарів, робіт, послуг.		

Секція	R	Назва виду діяльності	Мистецтво, спорт, розваги та відпочинок
Ризики за видом діяльності	Складовою даного виду діяльності є «організація азартних ігор», що передбачає отримання значних прибутків та може спонукати недобросовісних суб'єктів знаходити можливості для ухилення від сплати податків та зборів. На ризики у цій сфері також можуть впливати: операції з готівкою; функціонування нелегальних туристичних фірм; тіньова зайнятість населення.		

Секція	S	Назва виду діяльності	Надання інших видів послуг
Ризики за видом діяльності	Найбільший ризик виникає у послугах, які складно оцінити та перевірити їх надання (дослідження ринку, маркетингові, юридичні тощо). Зустрічаються непоодинокі випадки «фіктивного» надання послуг, або надання послуг за завищеними цінами, що дає змогу збільшувати видатки та ухилятися від сплати податків та зборів. На ризики у цій сфері також можуть впливати: операції з готівкою, тіньова зайнятість населення, недостатній рівень відкритості та прозорості.		

Секція	T	Назва виду діяльності	Діяльність домашніх господарств
Ризики за видом діяльності	Існує можливий ризик несплати податків та зборів до державного та місцевого бюджету при продажі створених домашніми господарствами товарів, робіт, послуг. На ризики у цій сфері також можуть впливати: операції з готівкою; тіньова зайнятість населення; недостатній рівень відкритості та прозорості.		

Наведені ризики за видом діяльності є корисними для оцінки ризиків діяльності клієнтів суб'єктів первинного фінансового моніторингу.

РОЗДІЛ ІІ. ОГЛЯД ТРЕНДІВ МІЖНАРОДНИХ ОРГАНІЗАЦІЙ ТА ПРОВЕДЕНІ ДОСЛІДЖЕННЯ

2.1. FATF щодо COVID-19 і заходів боротьби із незаконним фінансуванням

Члени FATF, як на національному, так і на міждержавному рівні використовують усі можливі ресурси для боротьби із пандемією COVID-19.

FATF закликає країни співпрацювати із фінансовими установами та іншими підприємствами з метою використання гнучкості ризик-орієнтованого підходу для подолання викликів, спричинених COVID-19, приділяючи при цьому увагу новим ризикам щодо незаконного фінансування.

FATF заохочувати якнайшвидше використовувати цифрові фінансові послуги у світлі заходів щодо соціального дистанціювання, ефективного впровадження Стандартів для більшої прозорості фінансових операцій.

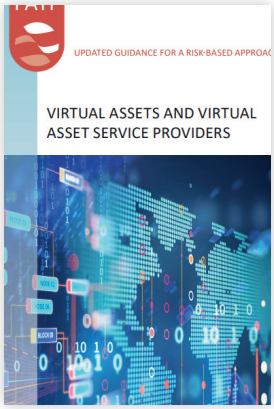
Злочинці користуються пандемією COVID-19 для здійснення фінансового шахрайства, махінацій, у тому числі рекламу та незаконну торгівлю контрафактними (підробленими) медичними препаратами, пропонуючи сумнівні можливості інвестування, і залучаючи фішингові схеми, що базуються на страхах, пов'язаних із вірусом.

Значна кількість злочинців має на меті отримати вигоду від пандемії, використовуючи стан людей, які потребують невідкладної допомоги та добру волю суспільства разом із поширенням дезінформації щодо COVID-19.

Терористи, як і злочинці, можуть також використовувати COVID-19 для збільшення своїх злочинних активів шляхом пошуку прогалин та слабких місць в національних системах ПВК/ФТ/ЗМЗ.

2.2. Огляд досліджень

Міжнародними організаціями проведено ряд досліджень з питань легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансування тероризму та фінансування розповсюдження зброї масового знищення.

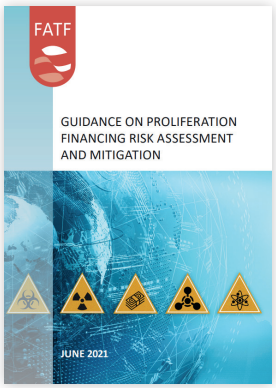


Virtual Assets and Virtual asset service providers
Віртуальні активи та постачальники послуг віртуальних активів (оновлені)

https://bit. ly/3yDsZiV

COVID-19-Related Money Laundering and Terrorist Financing Risks
Ризики відмивання грошей та фінансування тероризму, пов'язані з COVID-19

https://bit. ly/3sTwmzn

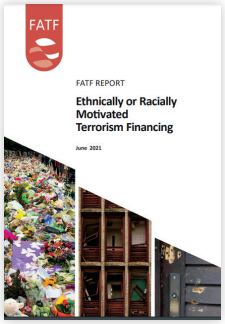


Guidance on Proliferation Financing Risk Assessment and Mitigation
Керівництво з оцінки та зменшення ризиків фінансування розповсюдження зброї масового знищення

https://bit. ly/3q9BJcZ

Terrorist Financing Risks Assessment Guidance
Керівництво з оцінки ризиків фінансування тероризму

https://bit. ly/3jjG0rV



Ethnically or Racially Motivated Terrorism Financing
Етнічно та расово мотивоване фінансування тероризму

https://bit. ly/3D1HQ7C

Money Laundering from Environmental Crime
Відмивання грошей від екологічної злочинності

https://bit. ly/3BmVvG1

Trade-Based Money Laundering: Risk Indicators
Відмивання грошей на основі торгівлі: показники ризику

https://bit. ly/3gCJLHv

РОЗДІЛ ІІІ. ТИПОЛОГІЇ ВІДМИВАННЯ КОШТІВ

Результати проведених фінансових розслідувань свідчать, що злочинці з метою отримання вигоди з пандемії COVID-19 активізували свої зусилля у вчиненні економічних злочинів, зокрема щодо ВК/ФТ.

В загальному значенні, ВК полягає в тому, щоб узяти гроші, отримані від злочинної діяльності, та провести їх крізь низку операцій, маскуючи їхнє походження та інтегруючи їх до фінансової системи для подальшого використання в інтересах злочинців.

За останні роки відбулось зростання рівня тіньової економіки, насамперед через складні, незвичні умови ведення бізнесу під час пандемії COVID-19.

Фінансова сфера, завдяки розвитку нових продуктів та технологій, надає злочинцям нові практики дистанційного способу вчинення злочину як в реальному світі, так і у віртуальному.

Основними факторами трансформації фінансових злочинів є перехід світової економіки до нового технологічного укладу, інформатизація суспільства у всіх сферах, глобалізація, використання різних юрисдикцій до здійснення ВК.

Держфінмоніторинг продовжує у тісній співпраці з суб'єктами первинного фінансового моніторингу, державними та правоохоронними органами виявляти підозрілі фінансові операції та факти незаконної діяльності юридичних та фізичних осіб.

Особливу увагу Держфінмоніторинг приділяє аналізу підозрілих транзакцій, які мають ознаки відмивання коштів та фінансування тероризму (сепаратизму).

Протягом 11 місяців 2021 року Держфінмоніторингом до правоохоронних органів направлено **1 091** матеріал (з них 717 узагальнених матеріалів та 374 додаткових узагальнених матеріали).

У вказаних матеріалах сума фінансових операцій, які можуть бути пов'язані з легалізацією коштів, та із вчиненням кримінального правопорушення, становить **92,7 млрд гривень**.

У 2020 році Держфінмоніторингом до правоохоронних органів направлено **1 036** матеріалів (з них 607 узагальнених матеріалів та 429 додаткових узагальнених матеріалів). У вказаних матеріалах сума фінансових операцій, які можуть бути пов'язані з легалізацією коштів, та із вчиненням кримінального правопорушення, становить **76,2 млрд гривень**.

За 11 місяців 2021 року Офісом Генерального прокурора обліковано наступні окремі кримінальні правопорушення:

Кількість КП	Стаття КК України
18	ст 209 «Легалізація (відмивання) майна, одержаного злочинним шляхом» КК України
295	ст 258 «Терористичний акт» КК України
1	ст 258[1] «Втягнення у вчинення терористичного акту» КК України
4	ст 258[2] «Публічні заклики до вчинення терористичного акту» КК України
125	ст 258[3] «Створення терористичної групи чи терористичної організації» КК України
1	ст 258[4] «Сприяння вчиненню терористичного акту» КК України
34	ст 258[5] «Фінансування тероризму» КК України

Кримінальні правопорушення за ст 439 «Застосування зброї масового знищення» Офісом Генерального прокурора не обліковано.

Найбільш яскраві приклади щодо ВК/ФТ наведено нижче. Інформація щодо корисних посилань для отримання додаткової інформації стосовно юридичних та фізичних осіб наведені у додатку.

3.1. Відмивання доходів, отриманих від корупційних діянь

Корупція є однією із найнебезпечніших загроз як для суспільства, так і для держави в цілому. Саме корупція має безпосередній вплив на розвиток суспільства, соціальний прогрес, економічну, національну безпеку України, інвестиційний клімат та міжнародний імідж.

На сьогодні в Україні здійснюються заходи щодо запобігання та протидії корупції, але як і раніше, найбільш масштабні корупційні схеми, як правило, здійснюються посадовими особами органів державної влади, державних та комунальних підприємств.

Найпоширенішими видами корупційних злочинів є: хабарництво, розкрадання бюджетних коштів, службове підроблення, зловживання владою або службовим становищем.

Посадовими особами органів державної влади, державних та комунальних підприємств з метою приховування злочинних доходів, отриманих від здійснення корупційних діянь, використовуються різноманітні схеми.

Узагальнені типові приклади, пов'язані з корупційними діяннями, наведено нижче.

Приклад 3.1.1.

Відмивання доходів посадовою особою державного підприємства

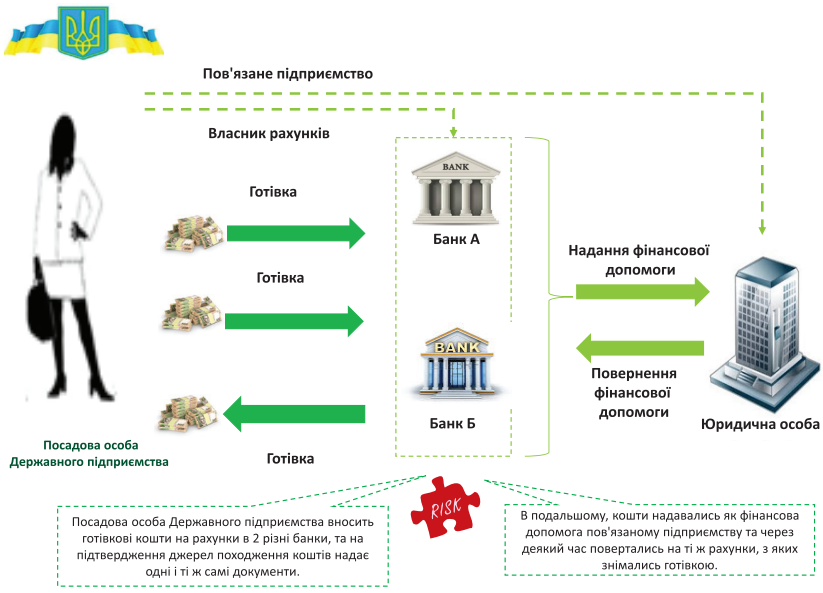
Держфінмоніторингом в ході фінансового розслідування виявлено схему приховування джерел походження коштів, отриманих від незаконної діяльності.

Встановлено, що **посадовою особою Державного підприємства** було здійснено внесення мільйонних сум готівки на поточні рахунки у двох різних фінансових установах.

Надалі, кошти перераховано як фінансову допомогу на користь юридичної особи, яка пов'язана з посадовою особою **Державного підприємства**. Через деякий час, юридичною особою повернуто фінансову допомогу на рахунки посадової особи **Державного підприємства**. Отримані кошти обготівковано.

З метою підтвердження джерела походження готівкових коштів, посадовою особою **Державного підприємства** до різних банківських установ надані одні й ті ж документи.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 3.1.2.

Відмивання доходів членами сім'ї національного публічного діяча шляхом інвестування в дороговартісне майно

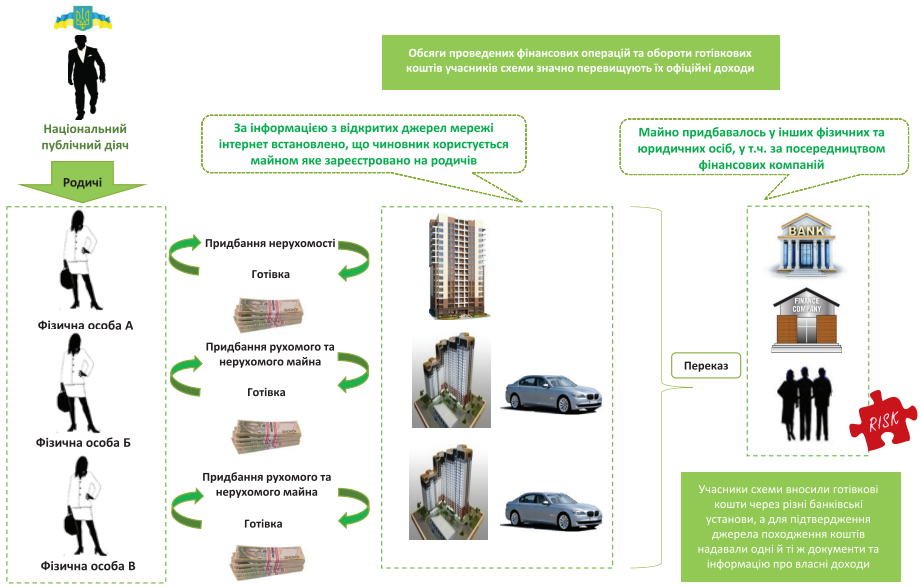
Спільним розслідуванням правоохоронного органу та Держфінмоніторингу виявлено схему приховування джерел походження незаконних доходів.

В ході фінансового розслідування встановлено, що **Члени сім'ї національного публічного діяча** придбавали у власність рухоме та нерухоме майно. При цьому, за інформацією з відкритих джерел мережі Інтернет встановлено, що дане майно було у користуванні самого **національного публічного діяча**.

Придбання майна здійснювалось за готівку в інших фізичних та юридичних осіб, фінансових компаній. Учасники схеми вносили готівкові кошти через різні банківські установи, а для підтвердження джерела походження коштів надавали одні й ті ж документи про джерела походження.

При цьому, обсяги проведених фінансових операцій та обороти готівкових коштів по рахунках учасників схеми значно перевищували офіційно задекларовані ними доходи. Це може свідчити, що фінансові операції були спрямовані на легалізацію (відмивання) доходів, одержаних злочинним шляхом (використання коштів з непідтверджених джерел).

Правоохоронним органом здійснюється досудове розслідування.



Приклад 3.1.3.

Відмивання коштів членом сім'ї національного публічного діяча шляхом формування статутного капіталу

Держфінмоніторингом в ході фінансового розслідування виявлено схему з приховування джерел походження коштів, імовірно отриманих від незаконної діяльності.

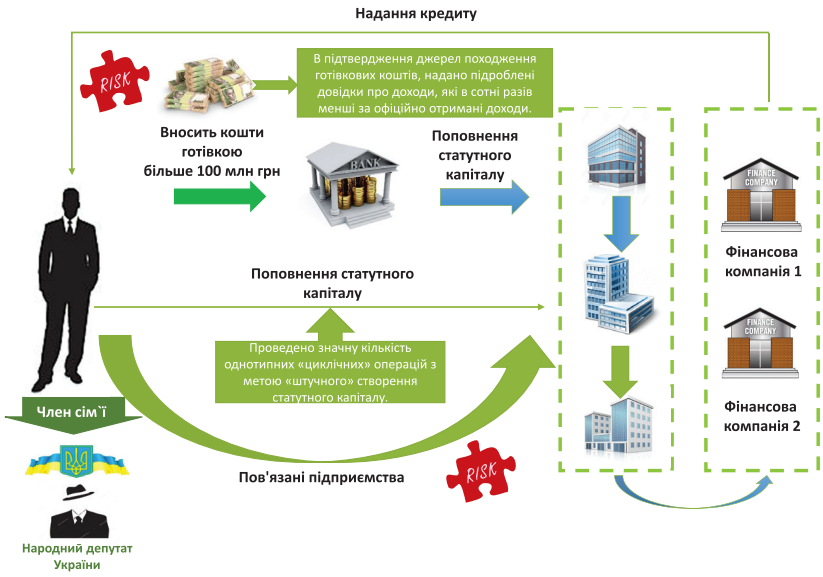
Встановлено, що **членом сім'ї національного публічного діяча** внесено понад 100 млн грн готівкових коштів на власний банківський рахунок.

Привертає увагу, що для підтвердження джерел походження готівкових коштів до банку надано підроблені довідки про доходи, які в сотні разів більші за офіційно отримані доходи **члена сім'ї національного публічного діяча**.

Надалі, кошти перераховано на користь підконтрольного **члену сім'ї національного публічного діяча** підприємства у якості формування статутного капіталу, з подальшим спрямуванням на афілійовані юридичні особи та циклічним поверненням у складі з іншими коштами у зворотному напрямку, на користь **члена сім'ї національного публічного діяча**.

В подальшому, кошти знову перераховувано на користь пов'язаного підприємства. Загалом проведено значну кількість однотипних «циклічних» фінансових операцій з метою «штучного» створення статутного капіталу.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 3.1.4.

Відмивання коштів членом сім'ї екс-посадової особи шляхом придбання майнових прав

За результатами проведеного фінансового розслідування Держфінмоніторингом виявлено схему приховування джерел походження коштів, імовірно отриманих від незаконної діяльності.

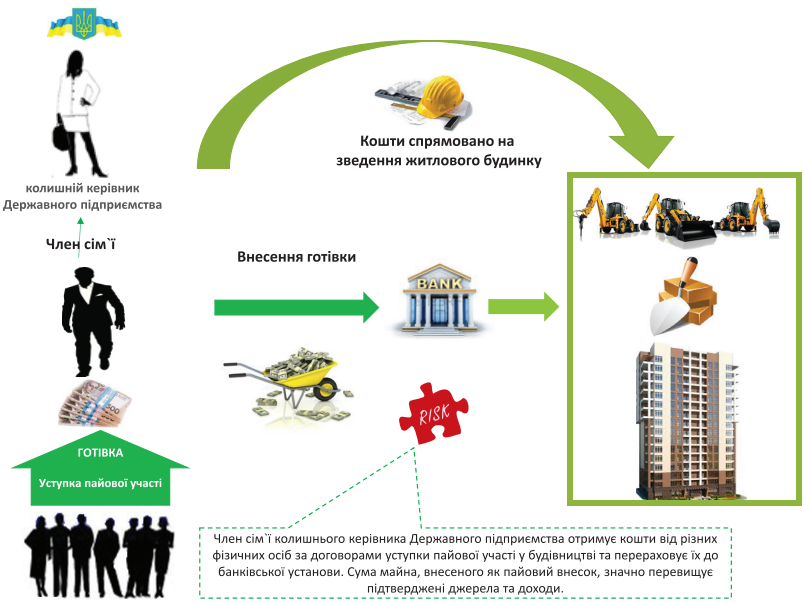
Встановлено, що членом сім'ї **колишнього керівника Державного підприємства** було здійснено внесення значних сум готівки на рахунок житлового кооперативу в якості сплати пайового внеску.

Джерелом походження коштів надано документи про отримання коштів від різних фізичних осіб за договорами уступки пайової участі у будівництві.

Сума майна, внесена як пайовий внесок до житлового кооперативу, значно перевищує суми коштів, отриманих від фізичних осіб.

Членом сім'ї **колишнього керівника Державного підприємства** здійснено фінансові операції та правочини з майном на суму, що значно перевищує його офіційні доходи та інші підтверджені джерела (кошти отримані від фізичних осіб).

Правоохоронним органом здійснюється досудове розслідування



3.2. Відмивання доходів отриманих від розкрадання, нецільового використання державних коштів та коштів суб'єктів господарювання державного сектору економіки

Бюджетні кошти є досить привабливим джерелом для отримання злочинних доходів, враховуючи значні їх обсяги, що виділяються для фінансування діяльності державних підприємств, територіальних громад (об'єднаних територіальних громад) та інших суб'єктів, які фінансуються коштом державного та місцевих бюджетів.

На даний час значна частина бюджетних коштів виділяється на проведення ремонту доріг в рамках програми «Велике будівництво». Також, значні бюджетні закупівлі проводяться для військового сектору, медичної галузі (придбання лікарських засобів і обладнання для боротьби з пандемією COVID-19), що створює ризики для корупції та розкрадання бюджетних коштів.

Зазначений вид ризиків може виникати все частіше та частіше при зменшенні контролю над проведенням державних закупівель.

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

Приклад 3.2.1.

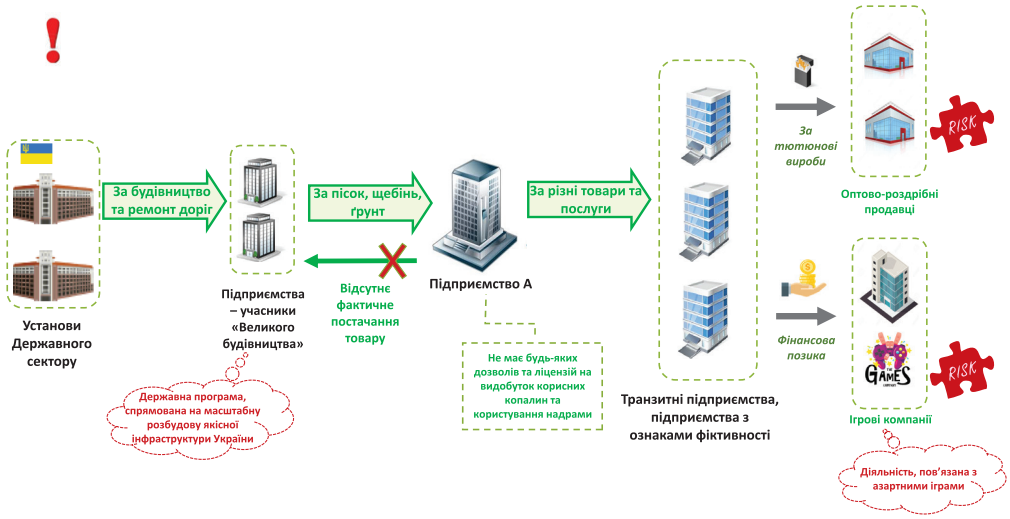
Відмивання доходів, отриманих від розкрадання бюджетних коштів з використанням підприємств з ознаками фіктивності та прихованого обготівковування

Правоохоронним органом спільно з Держфінмоніторингом виявлено схему розкрадання коштів державних підприємств, залучених до будівництва доріг.

В ході фінансового розслідування встановлено, що кошти, які попередньо були перераховані від установ Державного сектору на користь підприємств-учасників Державної програми «Велике будівництво» як оплата за роботи з будівництва та ремонту доріг, перераховано на користь **Підприємства А** як оплата за пісок, щебінь, ґрунт.

У **Підприємства А** відсутні будь-які дозволи та ліцензії на видобування корисних копалин, воно є посередником, фактичного постачання товару на користь підприємств-учасників Державної програми не відбувалось.

Отримані **Підприємством А** кошти від підприємств-учасників «Великого будівництва» надалі із використанням низки підприємств з ознаками фіктивності транзитом перераховані як оплата різноманітних робіт, послуг та як фінансова допомога на користь суб'єктів господарювання, що потенційно володіють готівковими коштами та здійснюють діяльність у сфері оптової та роздрібної торгівлі, а також у сфері азартних ігор (лотерей).



Приклад 3.2.2.

Відмивання доходів, отриманих від привласнення коштів комунального підприємства через підконтрольні підприємства

Правоохоронним органом викрито протиправну діяльність керівництва комунального підприємства.

Посадовці комунального підприємства налагодили схему привласнення коштів, призначених для відновлення столичних дитячих садочків та шкіл.

Організатори «схеми» діяли через підконтрольні підприємства, які вони залучили до виконання капітальних будівельних та ремонтних робіт як підрядні організації.

«Партнери» виконували роботи частково і не в повному обсязі, до того ж за суттєво завищеними розцінками. Деякі роботи не виконувалися взагалі, хоча зазначали, що вони «виконані».

За даними слідства, впродовж 2019 року комунальники провели конкурсні торги на суму понад 100 млн грн, 30% з яких вивели у «тінь», розподіливши їх між учасниками оборудки.

Розпочато кримінальне провадження за ч. 3 ст. 191 (привласнення, розтрата майна або заволодіння ним шляхом зловживання службовим становищем, вчинені повторно або за попередньою змовою групою осіб) КК України.

Приклад 3.2.3.

Відмивання доходів, отриманих від привласнення коштів державних установ

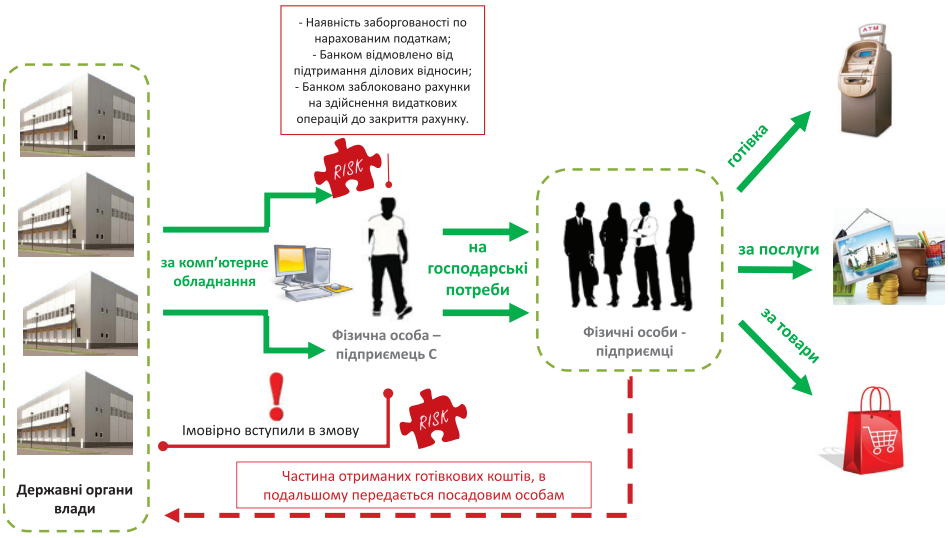
Держфінмоніторингом в ході фінансового розслідування виявлено схему розкрадання коштів **Державних установ**.

Так, **Державними установами** перераховано кошти на користь **Фізичної особи – Підприємця С** з ознаками фіктивності (наявність заборгованості по нарахованих податках, а також банком відмовлено від підтримання ділових відносин та заблоковано рахунки), у якості сплати за комп'ютерне обладнання.

Отримані **Фізичною особою – Підприємцем С** державні кошти невеликими обсягами та транзакціями перераховано на рахунки інших **Фізичних осіб – підприємців**. Надалі, вказані фізичні особи отримані кошти використали на власні потреби та частково зняли готівкою.

Варто зазначити, що за інформацією правоохоронного органу посадові особи **Державних установ** вступили в змову з вищезазначеними фізичними особами, які передали готівкові кошти вказаним посадовим особам.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 3.2.4.

Відмивання доходів, отриманих від розкрадання державних коштів через фіктивні підприємства

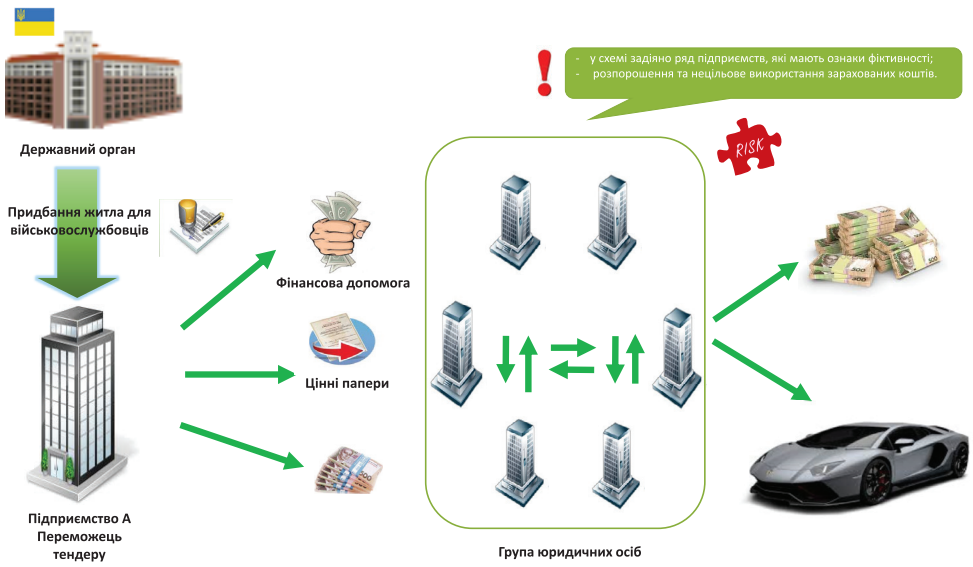
Правоохоронним органом спільно з Держфінмоніторингом виявлено схему розкрадання державних коштів під час придбання житла для військовослужбовців на умовах пайової участі та подальшої їх легалізації.

В ході фінансового розслідування встановлено, що **Державним органом** перераховано кошти на користь переможця тендеру – **Підприємства А** у якості оплати за придбання житла для військовослужбовців на умовах пайової участі.

Частина бюджетних коштів **Підприємством А** витрачена на придбання цінних паперів, надання/повернення фінансової допомоги та знята готівкою, а інша частина – перерахована на рахунки групи **Юридичних осіб**. Надалі кошти знято готівкою та використано на придбання елітного автомобіля.

Юридичні особи є підприємствами, які мають ознаки фіктивності – одноосібний посадово-засновницький склад, не сплачують податки, не мають відповідного персоналу та основних засобів, які використовуються для надання робіт та послуг у запланованих обсягах.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 3.2.5.

Відмивання доходів від привласнення бюджетних коштів шляхом завищення вартості укладеного державного контракту

Держфінмоніторингом з урахуванням інформації, отриманої від правоохоронного органу, виявлено схему привласнення бюджетних коштів шляхом завищення вартості укладеного державного контракту з подальшою легалізацією незаконних доходів через посадових осіб та фізичних осіб-підприємців з використанням механізму обготівковування коштів.

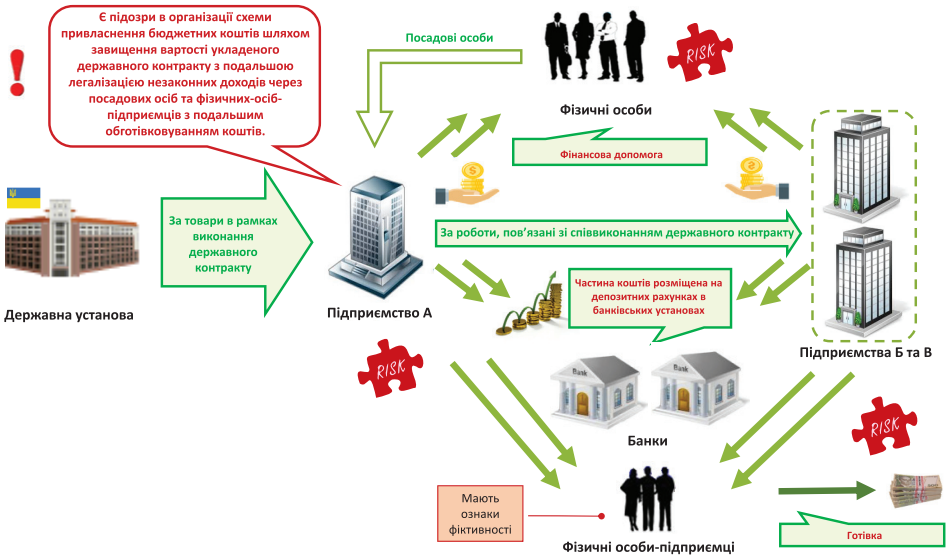
В ході фінансового розслідування встановлено, що **Державною установою** перераховано бюджетні кошти, виділені в рамках укладеного державного контракту, на користь **Підприємства А** як оплата за спорядження зброї для потреб Збройних сил України.

Підприємством А залучено **Підприємство Б** та **Підприємство В**, як співвиконавці робіт з виробництва зброї.

Під час виконання державного замовлення **Підприємство А** здійснило перерахування коштів, отриманих в рамках державного контракту, на користь **Підприємства Б** та **Підприємства В** за виконані ними роботи.

Більша частина отриманих коштів була витрачена **Підприємством А, Підприємством Б** та **Підприємством В** не за цільовим призначенням, а саме: перерахована посадовим особам як фінансова допомога, розміщена на депозитних рахунках в банківських установах, а також перерахована на рахунки суб'єктів підприємницької діяльності з ознаками фіктивності (одноосібний посадово-засновницький склад, не сплачують податки, відсутні наймані працівники), якими надалі обготівкована.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 3.2.6.

Відмивання доходів, отриманих від нецільового використання коштів комунального підприємства

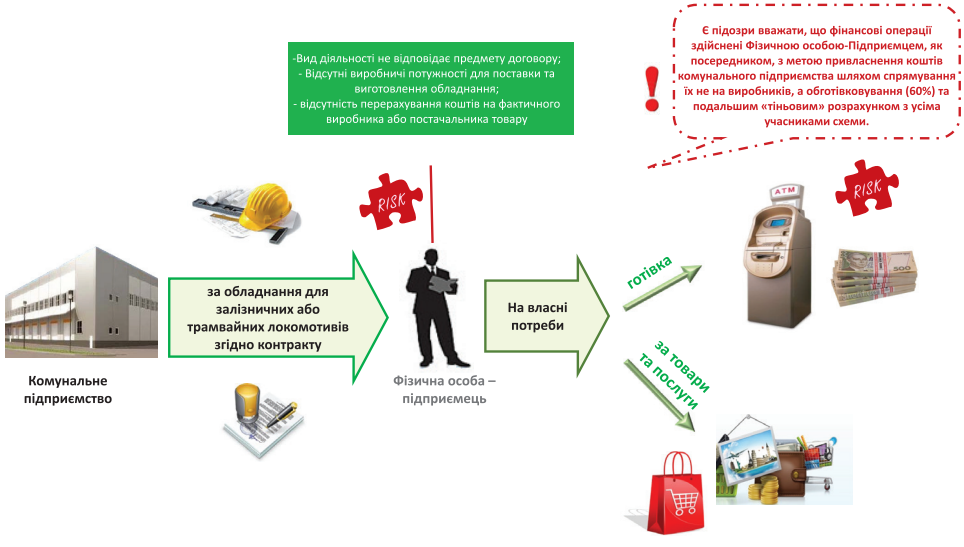
Держфінмоніторингом в ході фінансового розслідування виявлено схему використання коштів Комунального підприємства, сплачених згідно з договором постачання обладнання для залізничних або трамвайних локомотивів на користь **Фізичної особи – підприємця** не за цільовим призначенням.

Встановлено, що комунальне підприємство перерахувало кошти на користь **Фізичної особи – підприємця** у якості сплати за обладнання згідно контракту. Отримані кошти комунального підприємства **Фізичною особою – підприємцем** перераховано на власні рахунки та надалі переважно знято готівкою, а також частково витрачено на власні потреби.

Варто зазначити, що вид діяльності **Фізичної особи – підприємця** не відповідає предмету договору, який укладено з **Комунальним підприємством**, а також відсутні виробничі потужності для виготовлення обладнання, крім того, відсутнє перерахування коштів на користь фактичного виробника або постачальника товару.

Враховуючи наведене, є підозри вважати, що проведені фінансові операції **Фізичною особою – підприємцем**, як посередником, здійснено з метою приховування реальної вартості обладнання для привласнення коштів комунального підприємства шляхом спрямування їх не на рахунки виробників, а з подальшим обготівковуванням (60%). Ймовірно такі операції здійснені з метою розподілу незаконних прибутків між зацікавленими особами.

Правоохоронним органом здійснюється досудове розслідування.



3.3. Відмивання доходів від податкових злочинів

Практика фінансових розслідувань показує, що попит на «продаж» необлікованої готівки залишається на високому рівні. Такі «операції» здійснюються поза банківською системою, що значно ускладнює їх виявлення.

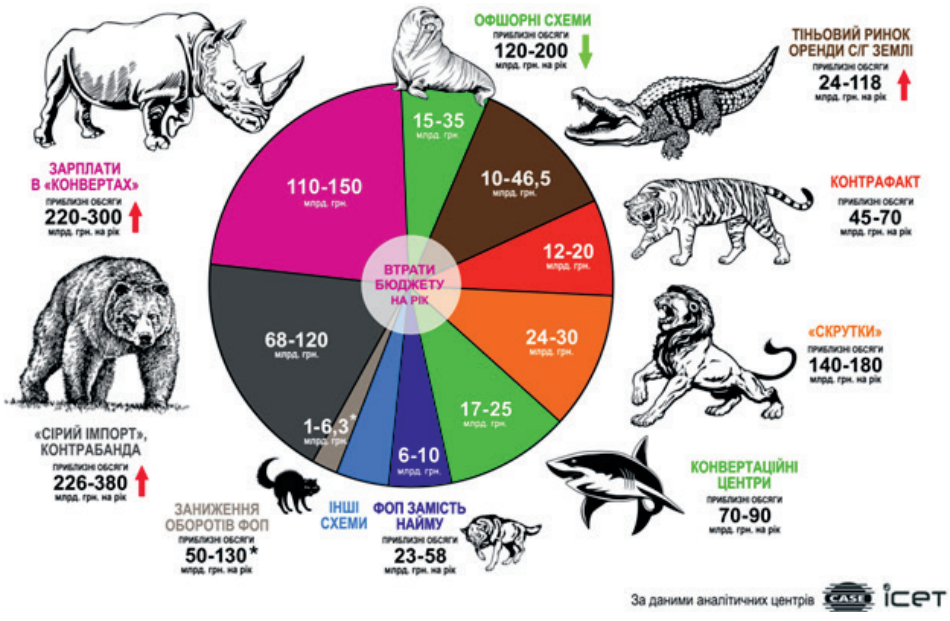
Підприємства реального сектору економіки намагаються різними шляхами зменшити свої зобов'язання з податку на додану вартість, а отже попит на «послуги» «зустрічних потоків» та «скруток» залишається досить високим.

Зазвичай послуги з ухилення від сплати податків надаються професійними мережами, до складу яких можуть входити юридичні особи, що акумулюють гроші, транзитні суб'єкти, фізичні особи-підприємці, підприємства реального сектору економіки, які мають готівкові кошти.

CASE Україна та Інститутом соціально-економічної трансформації проведено дослідження за темою «Порівняльний аналіз фіскального ефекту від застосування інструментів ухилення/уникнення оподаткування в Україні: 2021».

https://bit.ly/cxemy_podatky

Порівняльний аналіз річних обсягів та впливу на державний бюджет схем ухилення та уникнення оподаткування (2021 рік)



Механізми ухилення від сплати податків в Україні:

- порушення митних правил та контрабанда (маніпуляція з митною вартістю товарів, перерваний транзит, контрабанда);
- розкрадання податку на додану вартість (незаконне відшкодування з бюджету при експорті, фіктивне підприємництво (missing trader) – зокрема, «карусельні» схеми, підміна товару («скрутки»);
- контрафакт;
- переміщення прибутку до «податкових гаваней» («офшорів»);
- тіньові заробітні плати;
- викривлення бази оподаткування (приховування обсягів продажу);
- зловживання податковими пільгами, преференціями та спеціальними режимами;
- неофіційне підприємництво та індивідуальна економічна діяльність без реєстрації.

Узагальнені типові приклади, пов'язані із відмиванням злочинних доходів через «класичні» конвертаційні центри та із застосуванням механізму «зустрічні потоки», «скрутки» наведено нижче.

Приклад 3.3.1.

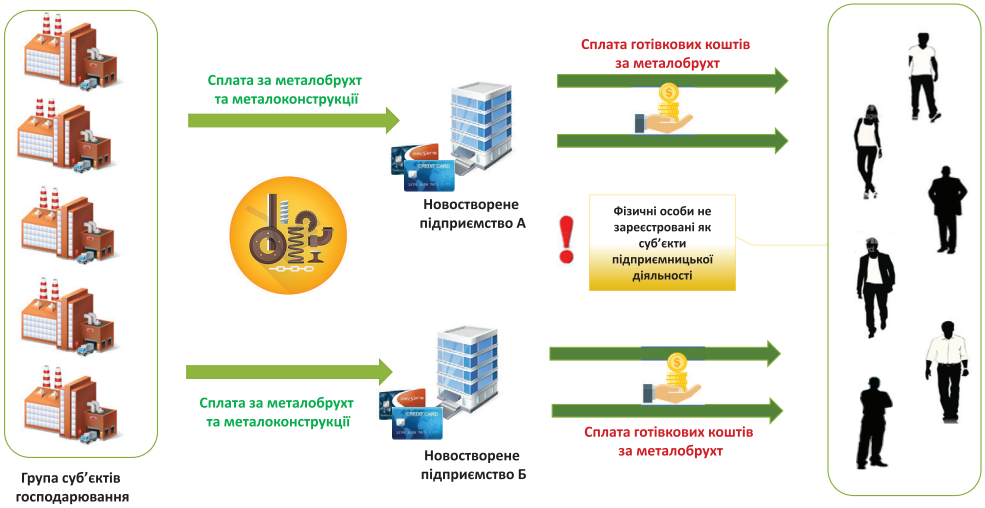
Відмивання доходів з використанням готівки через новостворених суб'єктів господарювання

Держфінмоніторингом з врахуванням інформації, отриманої від правоохоронного органу, виявлено схему «конвертації» безготівкових коштів у готівку групою новостворених підприємств з метою формування податкового кредиту та приховування отриманого доходу.

В ході фінансового розслідування встановлено, що **Групою юридичних осіб** з метою формування податкового кредиту перераховано кошти на користь новостворених **Підприємств А** та **Б** як оплату за металоконструкції та металобрухт. Надалі зазначені кошти було обготівковано **Групою фізичних осіб**, у вигляді розрахунку за металобрухт.

При цьому зазначені **фізичні особи** не були зареєстровані як суб'єкти підприємницької діяльності.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 3.3.2.

Відмивання доходів через «зустрічні потоки»

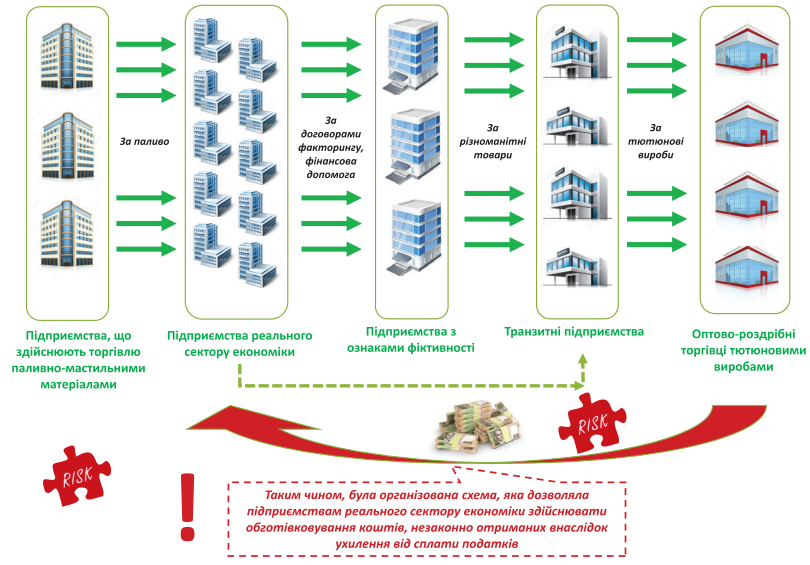
Держфінмоніторингом спільно з правоохоронним органом виявлено масштабну схему за участі професійної мережі з відмивання коштів, що сприяє ухиленню від сплати податків шляхом штучного формування податкового кредиту з ПДВ з подальшим переведенням безготівкових коштів у готівку через механізм «зустрічних потоків» із використанням підприємств оптово-роздрібної торгівлі тютюновими виробами.

В ході фінансового розслідування встановлено, що на рахунки **Групи підприємств** з ознаками фіктивності надходили кошти від ряду **Підприємств реального сектору економіки**, які в свою чергу отримували їх від інших підприємств, що здійснювали діяльність на ринку торгівлі паливо-мастильними матеріалами.

Привертає увагу, що при перерахуванні коштів на користь **Групи підприємств з ознаками фіктивності** (новостворені підприємства з одноособовим посадово-засновницьким складом, підприємства не декларують доходи та не сплачують податки, відсутні ресурси для здійснення господарської діяльності) було використано такі фінансові інструменти як «оплата за договором факторингу» та «фінансова допомога», за допомогою яких здійснюється розірвання ланцюгу переміщення товарів згідно з податковими накладними, що ускладнює об'єднання окремих суб'єктів господарювання у єдину конвертаційно-транзитну групу.

Встановлені фінансові потоки щодо подальшого руху коштів з рахунків **Групи підприємств з ознаками фіктивності** через транзитні підприємства, з використанням механізму «зустрічних потоків» кошти переказано на користь **Оптово-роздрібних торговців тютюновими виробами**, що надають послуги з переведення безготівкових коштів у необліковану готівку.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 3.3.3.

Відмивання привласнених коштів банківських установ з використанням механізму «скрутки»

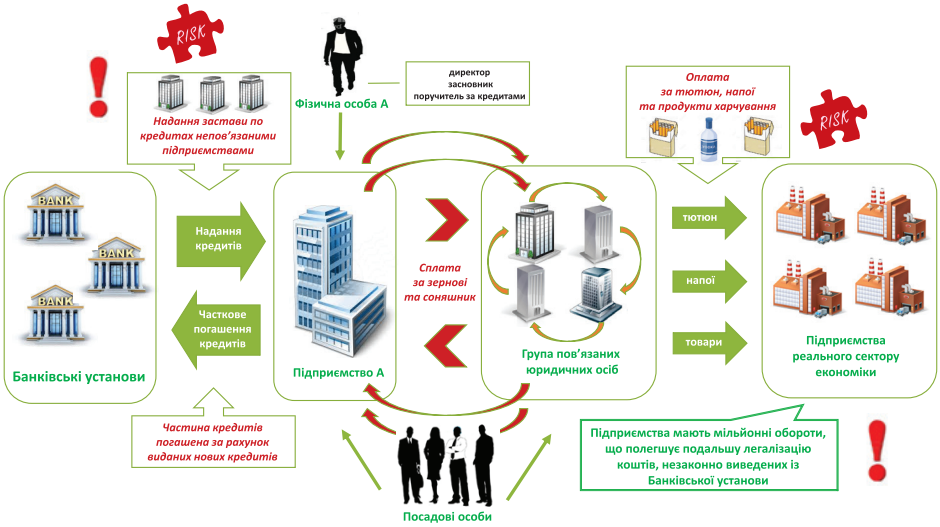
Держфінмоніторингом з врахуванням інформації, отриманої від правоохоронного органу, виявлено схему привласнення та відмивання коштів банківських установ з використанням механізму «скрутки».

В ході фінансового розслідування встановлено, що **Підприємство А** протягом року послідовно здійснювало оформлення кредитних договорів з різними банківськими установами із наданням у заставу майна непов'язаних підприємств. Поручителем при цьому виступала **Фізична особа А** – директор та засновник **Підприємства А**.

Надалі частина коштів, отриманих **Підприємством А** за вказаними договорами, перераховувалась на погашення попередньо отриманих кредитів (для отримання нового траншу). Основна частина коштів, перераховувалась на користь **Групи пов'язаних юридичних осіб** та у вигляді ряду циклічних операцій, як сплата за зернові та соняшник, перераховувались між їх рахунками з метою імітування активної діяльності та покращення іміджу **Підприємства А**.

На останньому етапі вказані кошти перераховувались у вигляді сплати за тютюн, напої та харчові продукти на користь **Групи підприємств реального сектору економіки,** які мають значні обсяги обороту коштів, що полегшувало легалізацію таких коштів.

Правоохоронним органом здійснюється досудове розслідування.



Окрім використання схем, які пов'язані із відмиванням злочинних доходів через «класичні» конвертаційні центри та із застосуванням механізму «зустрічні потоки», «скрутки», попит також мають схеми, пов'язані із зовнішньоекономічною сферою.

Такі схеми виведення коштів за кордон обслуговуються професійними мережами з надання незаконних послуг, до яких, як правило, залучаються вітчизняні юридичні особи, компанії-нерезиденти, що контролюються громадянами України, та іноземні «компанії-оболонки», лише з метою створення видимості проведення фінансово-господарської діяльності.

Приклад 3.3.4.

Відмивання доходів шляхом здійснення фіктивного імпорту

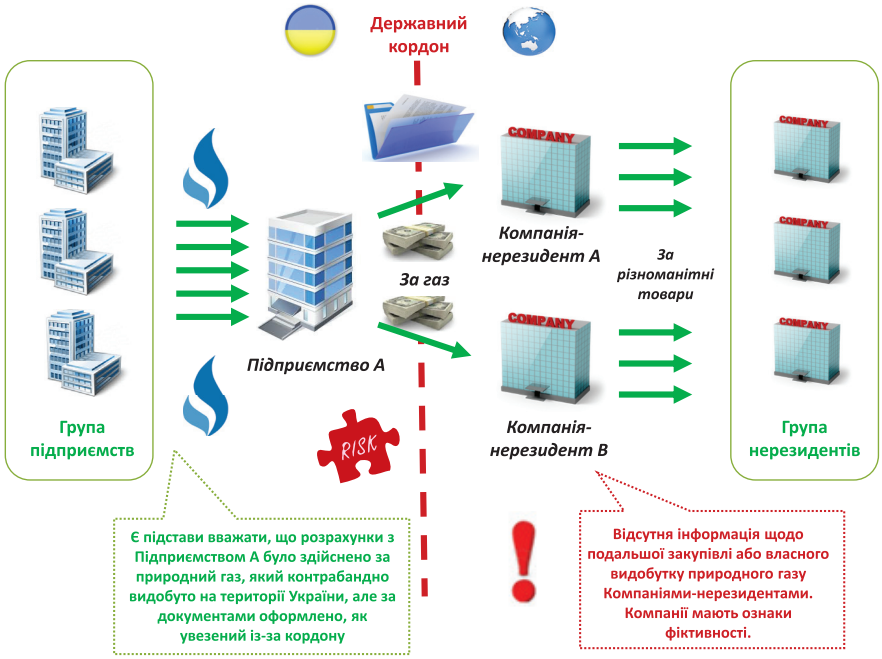
Держфінмоніторингом за результатами аналізу інформації, отриманої із різних джерел, виявлено крупномасштабну схему відмивання коштів, отриманих від реалізації природного газу, незаконно видобутого на території України.

В ході фінансового розслідування встановлено, що фінансовий потік рухався наступним чином: на рахунки **Підприємства А** надходили кошти від великої кількості вітчизняних підприємств як оплата за природний газ. Надалі акумульовані кошти конвертувались у долари США та перераховувались на користь двох **Компаній-нерезидентів**, які за інформацією ПФР мають ознаки фіктивності.

Надалі, кошти з рахунків **Компаній-нерезидентів** перераховувались на користь великої кількості інших компаній-нерезидентів з різноманітним призначенням платежу, та лише частково, у невеликій сумі, – за природний газ.

Відсутня інформація, що **Компанії-нерезиденти** здійснювали витрати на подальшу закупівлю або власний видобуток природного газу, таким чином **Підприємством А** було здійснено оплату за природний газ, який нелегально видобуто на території України, але за документами оформлено як увезений з-за кордону.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 3.3.5.

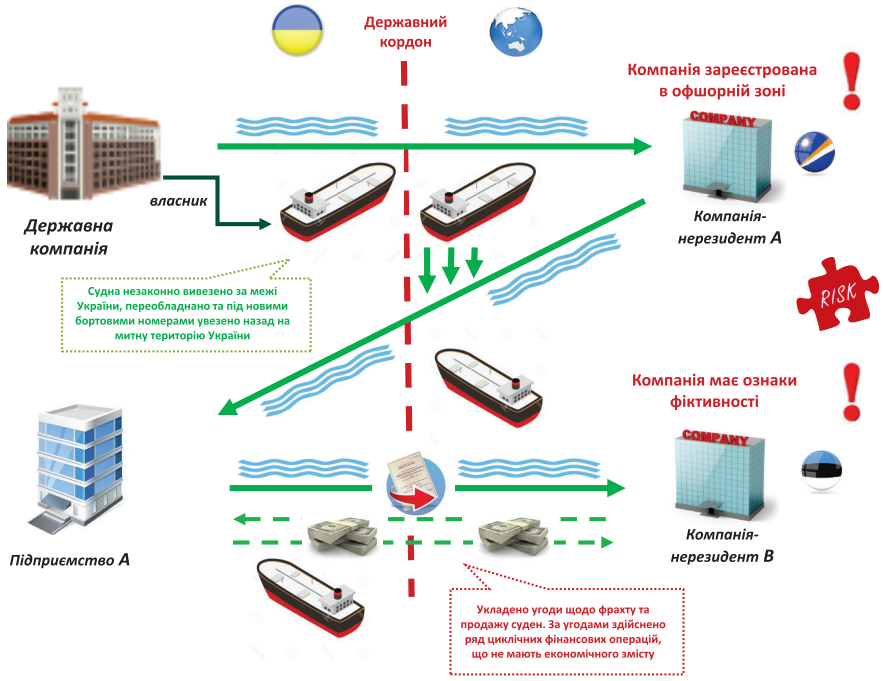
Відмивання доходів через зовнішньоекономічні операції з використанням документів з ознаками фіктивності

Держфінмоніторингом в ході фінансового розслідування встановлено, що за межі України було протиправно вивезено морські судна, які належать **Державній компанії**, переобладнано та під новими бортовими номерами увезено на митну територію України на користь **Підприємства А**. Відправником суден виступала **Компанія-нерезидент А**, зареєстрована в офшорній зоні.

Підприємством А надалі укладено заплутані за характером контракти та угоди, що не мають очевидного економічного сенсу, з **Компанією-нерезидентом В**, яка за інформацією ПФР має ознаки фіктивності. Предметом угод є фрахт та подальший продаж суден.

Після зарахування від **Компанії-нерезидента В** коштів по укладених контрактах, через деякий час кошти у повному обсязі з різноманітними призначеннями перераховувані у зворотному напрямку. Зазначена схема спрямована на привласнення державного майна, що належать **Державній компанії**, та відмивання доходів від вчинення цього злочину.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 3.3.6.

Відмивання доходів, ухилення від сплати податку на додану вартість за рахунок застосування пільгової ставки після оформлення вантажно-митної декларації

Держфінмоніторингом виявлено схему ухилення від сплати податків, пов'язану із реалізацією за межами митної території України експортованого зерна, неповерненням в Україну отриманої від його продажу валютної виручки та відмиванням коштів через торгові операції за кордоном.

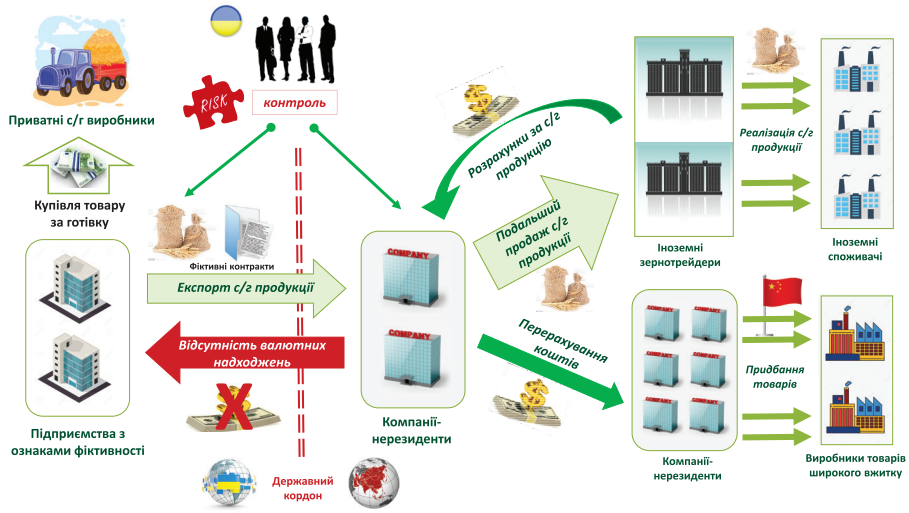
В ході фінансового розслідування встановлено професійну мережу з надання незаконних послуг, до складу якої входили юридичні особи, зареєстровані в Україні та за кордоном, за якою українськими **Підприємствами** з ознаками фіктивності – на підставі експортних контрактів з підконтрольними **Компаніями-нерезидентами** оформлено вантажно-митні декларації на експорт зерна, яке було придбано за готівкові кошти у приватних сільгоспвиробників.

Надалі, підконтрольними **Компаніями-нерезидентами** укладено договори продажу зерна на користь реальних **Іноземних зернотрейдерів**. Слід зауважити, що розрахунки за придбане зерно між учасниками схеми здійснено виключно на закордонні рахунки фіктивних **Компаній-нерезидентів**. Тобто, фактичні розрахунки за експорт українського зерна відбувались з дійсними покупцями за межами України. Крім того, встановлено, що кінцевими бенефіціарними власниками фіктивних **Компаній-нерезидентів** є громадяни України, а деякі з них є також власниками підприємств-експортерів.

Отримані кошти підконтрольними **Компаніями-нерезидентами** від **Іноземних зернотрейдерів** спрямовано до країн Азії для придбання товарів широкого вжитку. Експортна валютна виручка не надійшла на територію України, українськими **Підприємствами**, відповідно, не сплачені податки з отриманих за кордоном доходів.

Придбані в іноземних країнах та завезені на територію України товари широкого вжитку, оплата за які здійснена за рахунок коштів від реалізації зерна, реалізуються суб'єктами господарювання, що здійснюють оптово-роздрібну торгівлю та мають великий обсяг необлікованої готівки. Частина готівки, отриманої від реалізації завезених товарів, в наступному циклі спрямовується на закупівлю чергової партії українського зерна для експорту по новому колу.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 3.3.7.

Відмивання доходів, ухилення від сплати податків шляхом здійснення протиправних імпортних операцій.

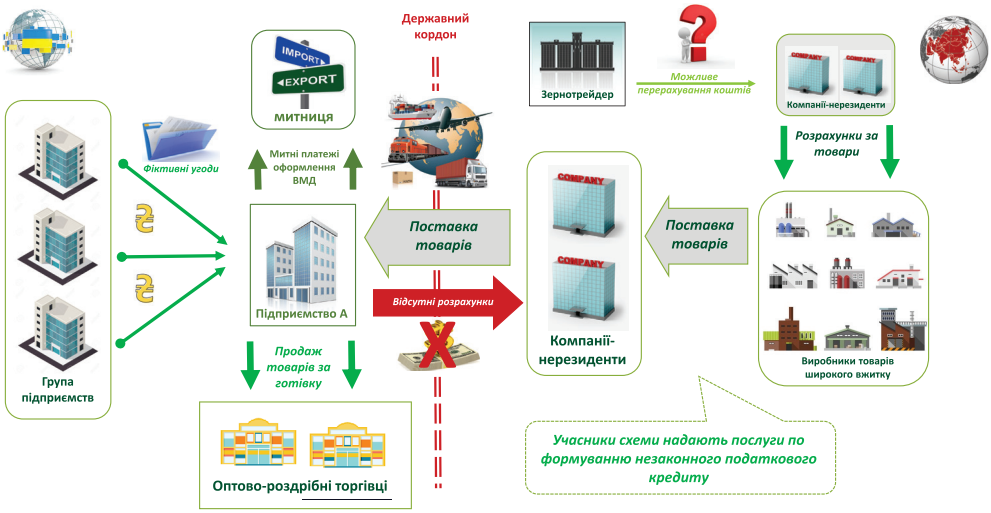
Держфінмоніторингом виявлено схему діяльності професійної мережі з надання незаконних послуг.

В ході фінансового розслідування встановлено, що **Підприємством А** отримано кошти від **Групи підприємств** як оплату товарів різного призначення, які в повному обсязі **Підприємством А** перераховано за митне оформлення. При цьому зовнішньоекономічні договори у банку відсутні, перерахування коштів за межі України **Підприємством А** не здійснювалось.

За даними Державної митної служби України, **Підприємством А** оформлені імпортні вантажно-митні декларації на товари широкого вжитку, отримані від **Компаній-нерезидентів**. При цьому виробниками цих товарів є різні компанії, розташовані, переважно, в країнах Азії. Відсутність оплати на користь нерезидентів свідчить про те, що розрахунки за імпортовані товари здійснюються за межами України коштами, які можуть мати злочинне походження.

Надалі імпортовані товари реалізовуються через мережі оптово-роздрібних торгівців за готівку, без відображення у бухгалтерському та податковому обліках.

Правоохоронним органом здійснюється досудове розслідування.



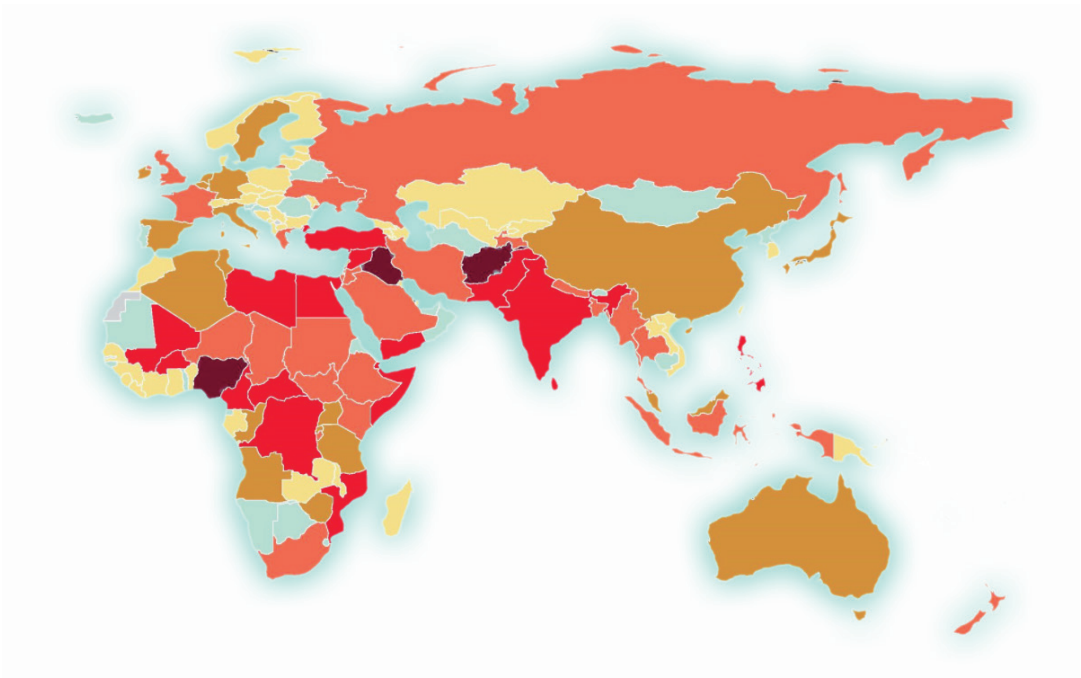
3.4. Розслідування справ, пов'язаних з фінансуванням тероризму та сепаратизму

Питання фінансування тероризму (сепаратизму) це одна з невирішених проблем сучасного суспільства, що характеризується високим рівнем суспільної небезпеки, виникнення якої може спричинити масову загибель людей, провокацію військового конфлікту.

Глобальний індекс тероризму (The Global Terrorism Index) і супутній з ним рейтинг країн світу за рівнем тероризму публікується щороку починаючи з 2012 року.

Глобальний індекс тероризму є комплексним дослідженням рівня терористичної активності у світі й відбиває масштаб терористичної загрози в розрізі держав.

У топ 10 країн світу з найвищим рейтингом рівня тероризму за 2020 рік увійшли Афганістан, Ірак, Нігерія, Сирія, Сомалі, Ємен, Пакистан, Індія, Демократична Республіка Конго, Філіппіни.



RANK	COUNTRY	SCORE	RANK CHANGE
84	Malawi	1.635	↑ 19
85	Denmark	1.484	↑ 15
86	Gabon	1.43	↑ 18
87	Norway	1.297	↑ 40
88	Madagascar	1.19	↓ 7
89	Costa Rica	1.066	↑ 74
90	Argentina	1.024	↓ 8
91	Austria	1.016	↓ 8
92	Kyrgyz Republic	0.95	↓ 8
93	Kazakhstan	0.901	↓ 8
94	Papua New Guinea	0.691	↓ 6
=95	Albania	0.677	↑ 13
=95	Bosnia and Herzegovina	0.677	↓ 9
=97	Benin	0.663	↑ 65
=97	Guatemala	0.663	↓ 8
99	South Korea	0.656	↑ 15
100	Georgia	0.635	↓ 11
101	Taiwan	0.607	↓ 6
102	Morocco	0.565	↓ 11
103	Hungary	0.551	↑ 15
104	Armenia	0.53	↓ 11
105	Guyana	0.477	↑ 26
106	Laos	0.439	↓ 12
=107	Montenegro	0.42	↓ 11
=107	Vietnam	0.42	↓ 11
109	Guinea	0.41	↓ 10
110	Senegal	0.391	↓ 18
111	Czech Republic	0.315	↓ 10
112	Azerbaijan	0.296	↓ 10
113	Switzerland	0.286	↑ 3
114	Poland	0.239	↓ 9
=115	Jamaica	0.229	↓ 11
=115	Lithuania	0.229	↓ 9
=115	Sierra Leone	0.229	↓ 9
118	Liberia	0.191	↑ 7
119	Bulgaria	0.172	↓ 9
120	Trinidad and Tobago	0.162	↑ 15
121	Zambia	0.153	↓ 9
=122	Latvia	0.115	↓ 6
=122	Cyprus	0.115	↓ 8
124	North Macedonia	0.105	↓ 11
125	Uruguay	0.086	↓ 5
=126	Estonia	0.057	↓ 4
=126	Moldova	0.057	↓ 4
=126	Serbia	0.057	↓ 4
129	Lesotho	0.048	↓ 3
130	Djibouti	0.038	↓ 19
131	Slovakia	0.029	↓ 3
132	Panama	0.019	↓ 1
133	Qatar	0.014	⟷
134	Uzbekistan	0.010	↑ 1
=135	Belarus	0.000	⟷
=135	Bhutan	0.000	↓ 27
=135	Botswana	0.000	⟷
=135	Cambodia	0.000	⟷
=135	Croatia	0.000	⟷
=135	Cuba	0.000	⟷
=135	Dominican Republic	0.000	↓ 44
=135	El Salvador	0.000	⟷
=135	Equatorial Guinea	0.000	⟷
=135	Eritrea	0.000	⟷
=135	Guinea-Bissau	0.000	⟷
=135	Iceland	0.000	↓ 30
=135	Kosovo	0.000	⟷
=135	Mauritania	0.000	⟷
=135	Mauritius	0.000	⟷
=135	Mongolia	0.000	⟷
=135	Namibia	0.000	⟷
=135	North Korea	0.000	⟷
=135	Oman	0.000	⟷
=135	Portugal	0.000	⟷
=135	Romania	0.000	⟷
=135	Singapore	0.000	⟷
=135	Slovenia	0.000	⟷
=135	Eswatini	0.000	⟷
=135	The Gambia	0.000	⟷
=135	Timor-Leste	0.000	⟷
=135	Togo	0.000	⟷
=135	Turkmenistan	0.000	⟷
=135	United Arab Emirates	0.000	↓ 34

На даний час, ризики поширення тероризму та сепаратизму в Україні залишаються актуальними з огляду на наявність низки зовнішніх та внутрішніх чинників, які негативно впливають на стан національної безпеки держави.

Чинники поширення тероризму та сепаратизму в Україні

Зовнішні чинники:

збільшення активності міжнародних терористичних організацій, формування сепаратистських ідей, організація та фінансування дій, спрямованих на порушення суверенітету та територіальної цілісності країни.

Внутрішні чинники:

Наявність у незаконному обігу значних обсягів зброї та боєприпасів, збільшення радикалізації суспільства тощо.

Загрози, пов'язані з тероризмом (сепаратизмом), зберігаються, терористичні угруповання можуть спробувати скористатися ситуацією з COVID-19 для того, щоб активізувати свою діяльність, поки увага влади зосереджена на пандемії.

Традиційні способи (методи) фінансування тероризму та сепаратизму складаються з законних джерел (надходжень від законного бізнесу, благодійних організацій), використання коштів від злочинної діяльності (торгівлі наркотиками, вимагання викупу, шахрайство), коштів від держав, які заохочують тероризм, а також фінансування безпосередньо терористами.

Узагальнені типові приклади, пов'язані з фінансуванням тероризму та сепаратизму, наведено нижче.

Приклад 3.4.1.

Фінансування сепаратизму через нелегальні криптообмінники[2]

За інформацією правоохоронного органу, виявлена мережа підпільних криптообмінників, які дозволяють проводити анонімні платежі та системно виводити тіньові кошти та переводити їх в готівку.

Послугами цих онлайн-обмінників здебільшого користувалися фізичні особи. Зокрема люди, які отримували кошти із заборонених в Україні електронних гаманців країни-агресора.

Зокрема, йдеться і про організаторів масових акцій протесту напередодні Дня Незалежності України. Саме через такі мережі вони отримували фінансування для оплати «послуг» провокаторів.

Мережа функціонувала від початку 2021 року та надала послуги з переказу понад 1 000 клієнтам.

Зловмисники щомісяця переказували через таку мережу майже 30 млн гривень. За «послуги» отримували 5-10 % від суми переказу.

Правоохоронним органом розпочато кримінальне провадження за ст. 200 «Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення» та ст. 209 «Легалізація (відмивання) доходів, одержаних злочинним шляхом» КК України.

Приклад 3.4.2.

Фінансування тероризму та сепаратизму за рахунок контрабандних поставок вугілля

Держфінмоніторингом в ході фінансового розслідування виявлено схему фінансування тероризму шляхом оплати за вугілля, що видобувається на тимчасово окупованих територіях Донецької та Луганської областей з подальшою легалізацією цих коштів шляхом імпорту в Україну незаконно видобутого вугілля.

Компанією-нерезидентом А (імпортер вугілля) на рахунок отримано близько 1 млн доларів США з призначенням платежу «передплата за вугілля». Кошти надійшли від **Підприємства А** (української вуглевидобувної компанії) і одразу були перераховані на рахунок іншої **Компанії-нерезидента Б** (посередника), відкритий в іноземному банку, який звинувачений у сприянні відмиванню коштів.

Відповідно до схеми транзакцій, компанія-нерезидент (посередник) придбала 20 000 тонн вугілля у компанії-нерезидента (продавця), а потім продала його компанії-нерезиденту

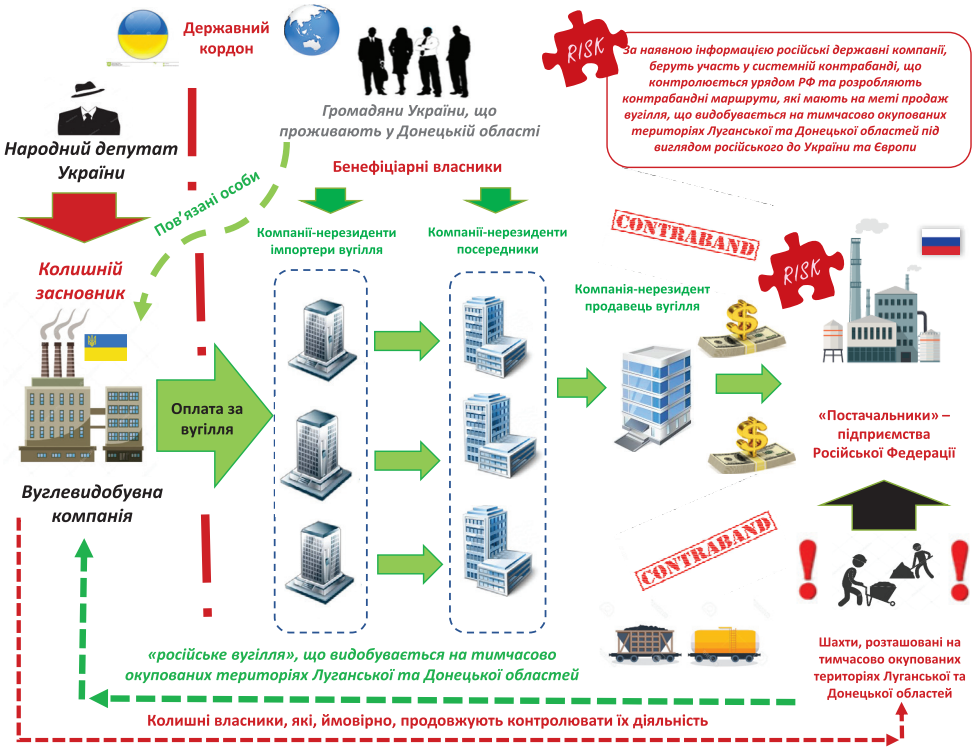
2 Режим доступу: https://ssu.gov.ua/novyny/sbu-zablokuvala-pidpilni-kryptoobminnyky-u-kyievi-cherez-nykh-finansuvaly-provokatsii-do-dnia-nezalezhnosti-ukrainy

(імпортеру вугілля), яка своєю чергою продала його кінцевому одержувачу – українській вуглевидобувній компанії, колишнім власником якої був народний депутат України.

За результатами аналізу укладеного контракту, вантажно-митних декларацій, інвойсів встановлено, що до України постачання російського вугілля мало здійснюватися з шахт Кузбасу (Російська Федерація). Але, за наявною іншою інформацією та порівняння маршрутів доставки, економічна вигода від таких поставок не має економічного сенсу. Вагони з вугіллям, які виїжджали з окупованих територій Донецької та Луганської областей, у Ростовській області досипались незначною кількістю сировини російського походження і під виглядом «російського вугілля» прямували до України для уникнення бути виявленими.

За результатами проведеного розслідування встановлено, що бенефіціарними власниками компаній-нерезидентів, залучених до описаної схеми, є **Громадяни України** – мешканці Донецької області, які пов'язані з українськими вуглевидобувними компаніями.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 3.4.3.

Фінансування тероризму за рахунок коштів, отриманих в якості приватного переказу

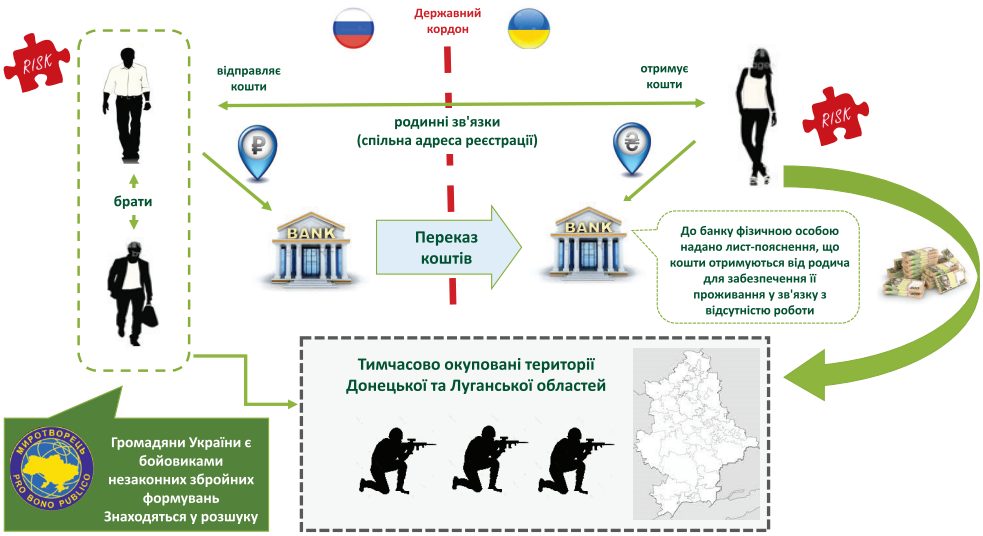
Держфінмоніторингом в ході фінансового розслідування встановлено, що на рахунок фізичної особи, яка зареєстрована на лінії розмежування з тимчасово окупованими територіями Донецької та Луганської областей зараховано значні кошти з території Російської Федерації.

До банківської установи **Фізична особа** надала лист-пояснення, в якому зазначила, що зазначені кошти отримує від родича для свого утримання у зв'язку з відсутністю роботи.

В ході фінансового розслідування встановлено, що відправником коштів є Громадянин України, який разом зі своїм братом є бойовиками незаконних збройних формувань та оголошені у розшук. Крім того, ці особи мають спільну адресу реєстрації з фізичною особою, що отримувала кошти.

Кошти, отримані з території Російської Федерації, від особи, яка переслідується правоохоронними органами України, можуть бути спрямовані на вербування та переправлення волонтерів для незаконних збройних формувань, що діють на тимчасово окупованих територіях Донецької та Луганської областей.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 3.4.4.

Фінансування сепаратизму з використанням неприбуткових організацій

Держфінмоніторингом виявлено схему фінансування іноземними благодійними фондами та установами українських підприємств та неприбуткових організацій у якості благодійної допомоги та грантів з подальшим перерахуванням на рахунки фізичних та юридичних осіб.

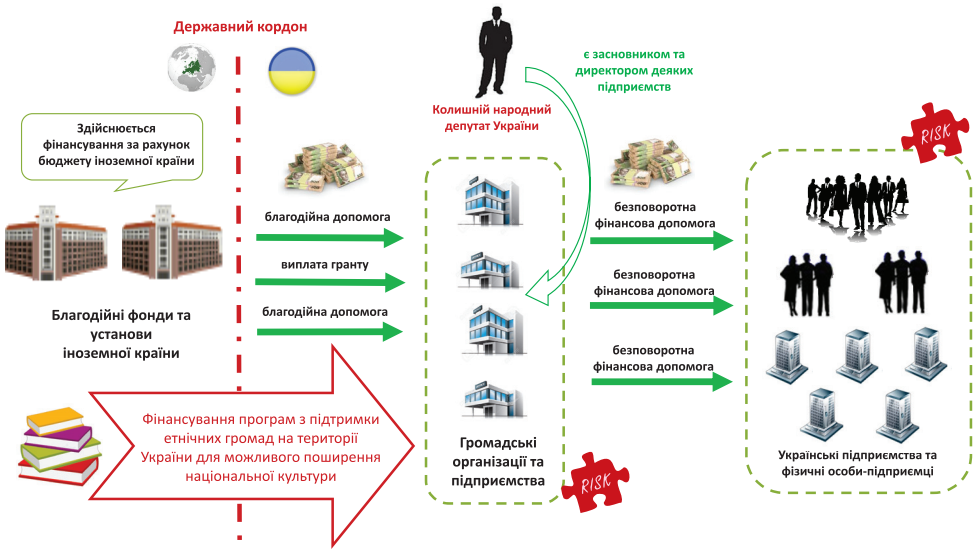
В ході фінансового розслідування встановлено, що протягом останніх років **Благодійними фондами та установами** іноземної країни регулярно перераховувались грошові кошти на мільйонні суми на рахунки українських **Громадських організацій та підприємств** у якості благодійної допомоги. Надалі зазначені кошти перераховувалися на рахунки фізичних осіб-підприємців та юридичних осіб у якості безповоротної фінансової допомоги.

Встановлено, що більшість фізичних осіб-підприємців була зареєстрована перед отриманням фінансової допомоги.

За інформацією з відкритих джерел, урядом іноземної країни через **Державні фонди та установи** надається фінансова допомога у якості сприяння економічного розвитку прикордонної області України, яка межує з цією країною та має серед громадян багато етнічних представників.

Разом з цим, використання коштів здійснюється для прикриття діяльності, спрямованої на дестабілізацію суспільно-політичної ситуації в певних регіонах України шляхом проведення антиукраїнських радикальних акцій та заходів (поширення сепаратистської літератури, викривлення історії, псування культурних пам'яток з метою розпалювання міжнаціональної ворожнечі та інше).

Одним із засновників підприємств, яким перераховано кошти від **іноземних НПО**, є колишній народний депутат України. Правоохоронним органом здійснюється досудове розслідування.



Приклад 3.4.5.

Використання громадських організацій для фінансування сепаратизму

Держфінмоніторингом виявлено схему фінансування російськими громадськими організаціями українських неприбуткових організацій, метою діяльності яких на території України є підтримка та популяризація російських стандартів.

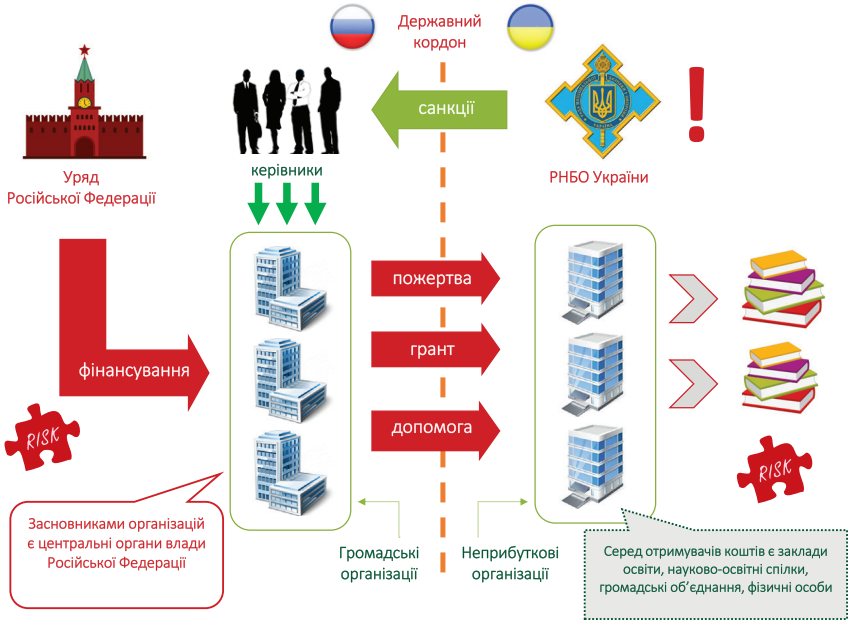
В ході фінансового розслідування встановлено, що протягом декількох років російською **Громадською організацією** було здійснено зарахування/спроби зарахування коштів у вигляді грантів, допомоги, пожертв на користь різних українських **Неприбуткових організацій**, які здебільшого здійснюють діяльність в освітній сфері. Такі ж перерахування на користь цих

Неприбуткових організацій надходили від інших **Громадських організацій (фондів)**, створених в Російській Федерації.

Привертає увагу, що засновниками цих російських фондів є органи центральної влади Російської Федерації (міністерства), а керівниками – російські високопосадовці, які рішенням РНБО України включені до національних санкційних переліків.

Надалі отримані кошти перераховано **Неприбутковими організаціями** на користь різного роду юридичних та фізичних осіб з метою друку видань для подальшого розповсюдження в освітніх навчальних закладах України та організації масових освітніх заходів. Разом з цим, тематика цих заходів дає підстави вважати їх елементами гібридної війни, спрямованими на розповсюдження проросійської інформаційної пропаганди.

Правоохоронним органом здійснюється досудове розслідування.



3.5. Відмивання доходів через страховий ринок та ринок цінних паперів

Страховий ринок є одним з невід'ємних елементів ринкової інфраструктури та фінансової системи будь-якої держави. Ефективно функціонуючий страховий ринок є важливою компонентою ринкової економіки і відіграє визначальну роль у формування загальноекономічної ситуації в країні, адже створює страхове середовище, здатне забезпечити страховий захист бізнесу від непередбачуваних подій та забезпечує соціальну підтримку населенню.

За своєю специфікою, український ринок страхування є дуже вразливим до використання у схемах легалізації (відмивання) коштів, отриманих злочинним шляхом.

Сумнівність фінансових операцій, здійснених за участю страхових компаній, можливо оцінювати за наступними основними критеріями:

- виведення коштів підприємств реального сектору економіки на підставі страхування ризиків, настання яких є мало ймовірним;
- сплата коштів у вигляді страхового відшкодування на підставі штучно створеного страхового випадку;
- виплата агентської винагороди на користь підприємств з ознаками фіктивності до здійснення операцій на ринку страхування послуг, надання яких важко підтвердити;
- здійснення розрахунків та формування резервів страхових компаній з використанням «сміттєвих» цінних паперів.

Взагалі такий фінансовий інструмент, як «сміттєві» цінні папери, часто використовується і в інших незаконних схемах (виведення активів за межі України, мінімізація податкових зобов'язань, ухилення від оподаткування тощо), які передують відмиванню злочинних доходів.

Одним з ризикованих інструментів фінансового ринку стали також операції з купівлі-продажу облігацій внутрішньої державної позики. З одного боку, цей вид цінних паперів можна вважати одним з найнадійніших фінансових інструментів завдяки високій ліквідності та широкому спектру застосування. Разом з цим, високий попит, особливості виконання укладених на біржі контрактів стосовно купівлі/продажу облігацій внутрішньої державної позики (ОВДП) робить їх привабливими у схемах легалізації незаконних доходів, особливо для публічних осіб, які повинні декларувати свої статки.

Приклад 3.5.1.

Виведення коштів через страхову компанію та ризикові інструменти

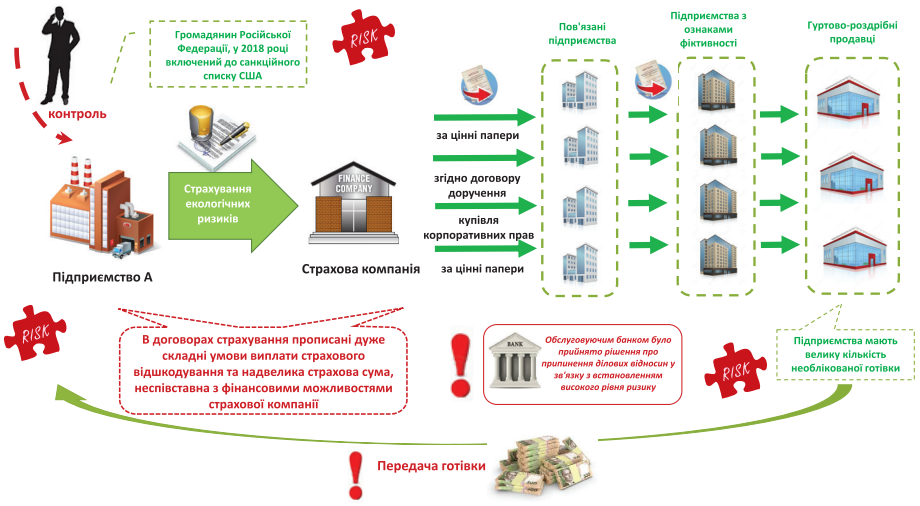
Держфінмоніторингом виявлено схему укладання державним підприємством фіктивних угод зі страховою компанією, спрямовану на виведення коштів у тіньовий сектор економіки, з подальшою легалізацією шляхом придбання «сміттєвих» цінних паперів, придбання корпоративних прав та виплат агентських винагород.

В ході фінансового розслідування встановлено, що **Страхова компанія** на свій банківський рахунок, отримала грошові кошти як страховий платіж від **Підприємства А**, що здійснює діяльність у сфері кольорової металургії. Зазначені кошти були перераховані на підставі договорів щодо страхування екологічних ризиків. Дуже складні умови виплати страхового відшкодування та надвеликий розмір страхової суми, неспівставний з фінансовими можливостями страхової компанії, може свідчити про «штучність» укладання договору, який не має на меті справжнє страхове покриття, а укладений виключно для виведення коштів з працюючого підприємства. Також встановлено, що контроль за діяльністю **Підприємства А** здійснює громадянин Російської Федерації, у 2018 році включений до санкційного списку США.

Надалі, отримані грошові кошти **Страховою компанією** було перераховано на рахунки пов'язаних між собою **Підприємств** з різноманітним призначенням платежів: згідно договору доручення, згідно договору купівлі-продажу корпоративних прав, згідно з договорами купівлі-продажу цінних паперів. При цьому придбані цінні папери належать до категорії «сміттєвих».

В кінцевому випадку кошти було спрямовано на рахунки підприємств з ознаками фіктивності, через які було переведено у готівку за допомогою підприємств, що здійснюють оптово-роздрібну торгівлю тютюновими виробами, алкогольною продукцією та мають великі обсяги необлікованої готівки.

Таким чином, була організована схема переведення безготівкових коштів у готівку, у якій фінансові операції зі страхування було використано як інструмент незаконного виведення коштів з підприємства реального сектору економіки. Правоохоронним органом здійснюється досудове розслідування.



Приклад 3.5.2.

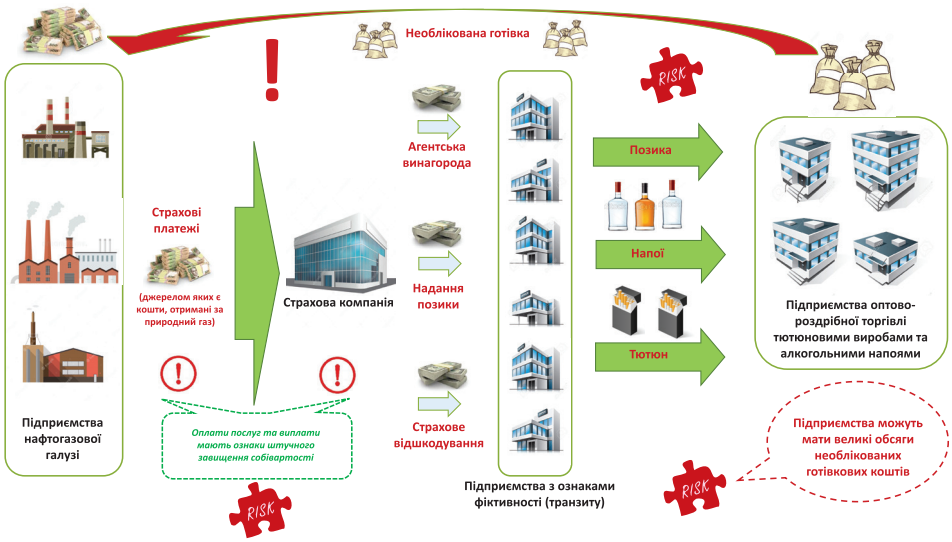
Виведення коштів через страхову компанію з подальшим використанням «зустрічних потоків»

Схема використання рахунків страхової компанії для надання податкової вигоди підприємствам реального сектору економіки та для транзитної маршрутизації безготівкових коштів із застосуванням механізму «зустрічних потоків».

В ході фінансового розслідування встановлено, що підприємствами реального сектору економіки, до складу яких входили **Підприємства газової та нафтогазової галузі**, було перераховано кошти на рахунки **Страхової компанії** як оплату страхових платежів. Джерелом походження перерахованих коштів, були кошти, отримані від продажу та надання послуг за постачання газу та нафтопродуктів. При цьому, такі платежі мали ознаки штучного завищення собівартості наданих послуг у нафтогазовій сфері, що передує отриманню надприбутків, які надалі легалізовані шляхом перерахування за страхові послуги.

Кошти, отримані **Страховою компанією**, в подальшому були перераховані на рахунки транзитних **Підприємств** з ознаками фіктивності як виплати страхового відшкодування, агентської винагороди та надання позики, які, своєю чергою, перераховували кошти на користь **Підприємств оптово-роздрібної торгівлі** тютюновими виробами та алкогольними напоями як оплату по договору факторингу, надання позики та розрахунків за алкогольну та тютюнову продукцію.

Підприємства оптово-роздрібної торгівлі тютюновими виробами та алкогольними напоями можуть мати значні обсяги готівкових коштів, у тому числі необліковані, які можуть бути використані в обміні безготівкових коштів підприємств реального сектору економіки на готівку. Правоохоронним органом здійснюється досудове розслідування.



Приклад 3.5.3.

Фальсифікація правочинів з метою приховування чи маскування незаконного походження коштів

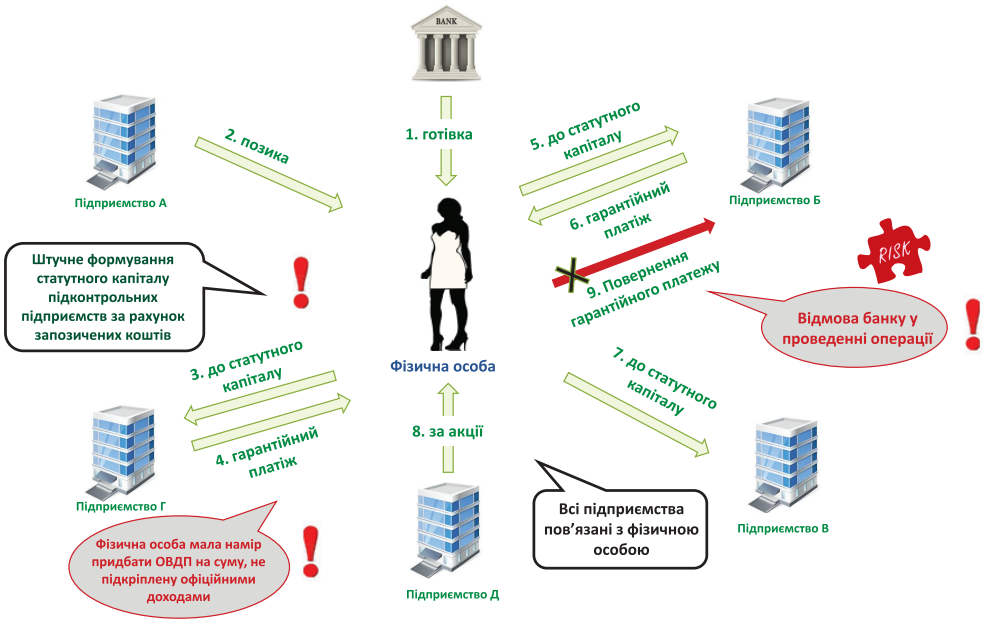
Держфінмоніторингом виявлено схему фальсифікації правочинів, пов'язану з купівлею - продажем облігацій внутрішньої державної позики з подальшим зарахуванням коштів на рахунки фізичної особи.

Встановлено, що **Фізична особа** та підконтрольні їй підприємства відкрили рахунки в декількох банківських установах. На один з таких рахунків зазначена особа отримала позику від **Підприємства А**, внесла кошти готівкою та перерахувала на рахунок **Підприємства Б** як внесок до статутного капіталу, яке, своєю чергою, повернуло кошти на її рахунок як гарантійний внесок по договору купівлі-продажу ОВДП. При цьому, для проведення подібних операцій у **Фізичної особи** не вистачало офіційно задекларованих доходів. За аналогічною схемою протягом короткого проміжку часу були проведені операції на значні суми в різних банках ще з декількома підприємствами.

Надалі **Фізична особа** надала в одну з банківських установ додаткову угоду про розірвання договору купівлі-продажу ОВДП і здійснила спробу повернення коштів на користь **Підприємства Б**, проте банк відмовив у проведенні такої операції. Джерелом коштів для проведення такої операції були надходження за продані акції **Підприємству Д**.

Таким чином, **Фізичною особою** організована схема проведення циклічних фінансових операцій з метою приховування незаконного походження коштів та подальшим поверненням їх на рахунки **Фізичної особи**.

Правоохоронним органом здійснюється досудове розслідування.



3.6. Відмивання доходів, отриманих від торгівлі зброєю

Правоохоронні органи систематично викривають та припиняють злочинну діяльність осіб, які здійснюють незаконну торгівлю зброєю та особливо небезпечними хімічними речовинами.

Як правило організаторами таких схем торгівлі є учасники злочинних угрупувань, раніше судимі громадяни та інші особи з відповідними навичками.

Типові приклади розслідувань щодо відмивання злочинних доходів, отриманих від торгівлі зброєю наведено нижче.

Приклад 3.6.1.

Організація схеми відмивання доходів, одержаних від продажу зброї та комплектуючих

Держфінмоніторингом, з врахуванням інформації отриманої від банківської установи, виявлено фінансові операції, проведені по рахунках/платіжних картках та за участю **групи фізичних осіб**, які можуть бути пов'язані із продажем зброї та комплектуючих з тимчасово окупованої території Донецької та Луганської областей.

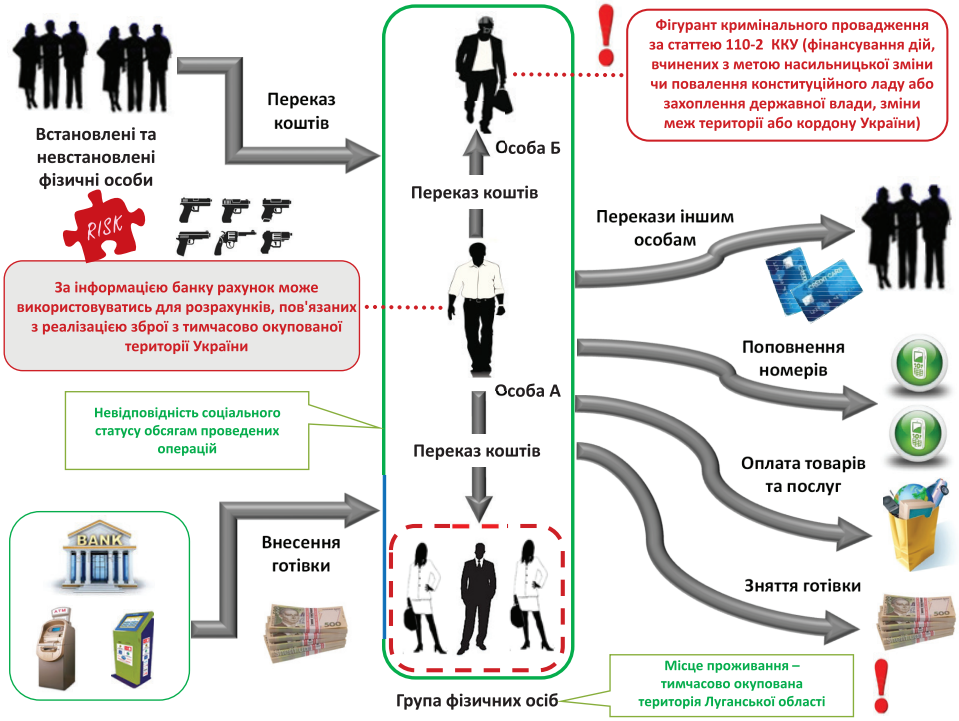
В ході фінансового розслідування встановлено, що на картковий рахунок **фізичної особи А**, щодо якої була інформація про причетність до продажу зброї з тимчасово окупованої території України, зараховувались безготівкові перекази, в тому числі з використанням ряду платіжних сервісів онлайн-платежів.

В подальшому, отримані кошти у день їх надходження, спрямовувались на платіжні картки **групи фізичних осіб**, місцем проживання яких є тимчасово окупована територія Луганської області. Кошти зокрема спрямовувались на користь **фізичної особи Б**, яка є фігурантом кримінального провадження за ознаками вчинення кримінального правопорушення, передбаченого статтею 110^2 Кримінального кодексу України – фінансування дій, вчинених з метою насильницької зміни чи повалення конституційного ладу або захоплення державної влади, зміни меж території або кордону України.

Надалі, отримані кошти вищезазначеною **групою фізичних осіб** використовувались для: поповнення рахунків інших осіб, поповнення значної кількості номерів мобільних телефонів, придбання товарів/послуг, переведення в готівку.

Слід зазначити, що відсутня будь-яка інформація щодо участі вищезазначених осіб у діяльності юридичних осіб, реєстрації їх як суб'єктів підприємницької діяльності, отриманих та задекларованих доходів, а також сплачених податків.

Правоохоронним органом здійснюється досудове розслідування.



3.7. Відмивання доходів отриманих від торгівлі наркотичними та психотропними речовинами

Проблема протидії наркозлочинності є однією з найгостріших соціальних проблем України. За статистичними даними Національної поліції питома вага наркозлочинів становить 16% від загальної кількості зареєстрованих злочинів.

При цьому кожен 9 зареєстрований тяжкий та особливо тяжкий злочин скоєно у сфері обігу наркотичних засобів та психотропних речовин, їх аналогів і прекурсорів.

За 10 місяців 2021 року органами Національної поліції задокументовано 272,4 тис. кримінальних правопорушень у сфері незаконного обігу наркотичних засобів, серед яких понад 97 тис відносяться до категорії тяжких та особливо тяжких злочинів.

Залишається актуальним питання злочинів, пов'язаних з незаконним обігом наркотиків, скоєних організованими злочинними утвореннями.

За даними різних джерел зростає міжнародний наркобізнес. Третина всіх міжнародних організованих злочинних груп займається збутом наркотичних засобів.

За останніми оцінками, третину доходів транснаціональні організовані злочинні групи в усьому світі отримують від незаконного обігу наркотичних засобів.

Організовані злочинні наркоугруповання швидко вдосконалюють свої методи роботи, використовуючи останні інноваційні технології, можливості інтернет-зв'язку, транзакції з криптовалютою, тим самим розширюючи ринок наркообігу.

Наркобізнес як форма організованої злочинної діяльності сам породжує корупцію, втягуючи у свою діяльність представників органів влади, у тому числі працівників правоохоронних органів.

Злочинна організація у сфері незаконного обігу наркотиків відрізняється високим рівнем управління й організації. Між керівництвом та виконавцями з'явилися проміжні, структурно-функціональні підрозділи: радників, консультантів, логістів, розвідників, охоронців, корумпованих посадових осіб державних органів та інші.

За даними Держприкордонслужби обсяги виявлених наркотиків на державному кордоні України та рівень ризику їхньої контрабанди залишаються високими.

Типові приклади розслідувань щодо відмивання злочинних доходів, отриманих від торгівлі наркотичними та психотропними речовинами, наведено нижче.

Приклад 3.7.1.

Виявлення міжнародних каналів контрабандного переправлення наркотиків і прекурсорів

Служба безпеки України заблокувала два міжнародні канали контрабандного переправлення в Україну наркотиків і прекурсорів. Зловмисники ввозили оптові партії «товару» під виглядом лікарських засобів і косметичної продукції. Середньомісячні «прибутки» наркоділків становили десятки тисяч доларів.

На території митного посту Міжнародного аеропорту «Бориспіль» правоохоронці викрили двох наркокур'єрів. Зловмисники намагалися провезти до країни партію псевдоефедрину – прекурсору, який у підпільних нарколабораторіях використовують для виготовлення метамфетаміну.

Щоб приховати протиправну діяльність, ділки декларували багаж як лікарські засоби. Після переправлення «товару» зловмисники планували реалізувати його через власну мережу дилерів.

Встановлено, що затримані входять до складу міжнародного злочинного угруповання, яке спеціалізується на збуті оптових партій наркотиків з однієї з африканських країн.

Крім того, у Києві затримано ще одного організатора контрабандного каналу наркотиків до України. Зловмисники переправляли концентрований канабіс з однієї з країн Північної Америки під виглядом косметичної продукції.

Для переправлення «товару» вони використовували сервіси міжнародного поштового зв'язку.

Правоохоронці затримали організатора наркотрафіку під час отримання чергової «посилки».

Приклад 3.7.2.

Виявлення міжнародних каналів контрабандного переправлення кокаїну

Правоохоронні органи виявили у порту «Південний» прихований від митного контролю наркотичний засіб «кокаїн», контрабандно переміщений в Україну.

Наркотик прибув з Республіки Еквадор через контейнерний термінал одного з портових операторів у технологічних порожнинах морських рефрижераторних контейнерів з вантажем бананів у 50 брикетах вагою брутто майже 60 кг. Вартість вилученої партії кокаїну на «чорному ринку» складає орієнтовно 10 млн доларів США.

Приклад 3.7.3.

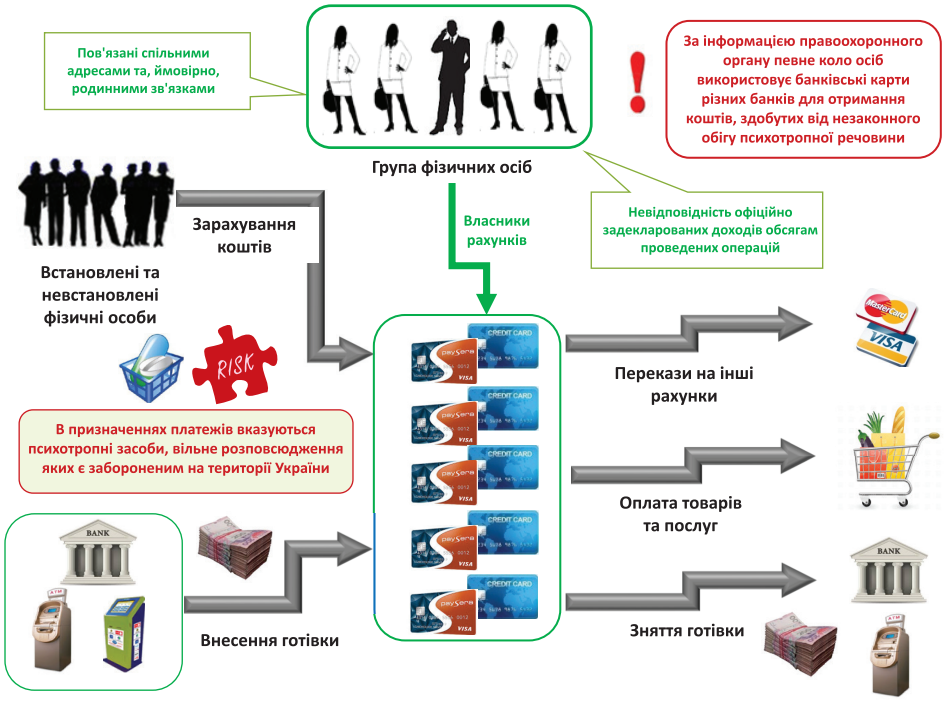
Відмивання доходів, одержаних від незаконного обігу психотропних речовин

Держфінмоніторингом від правоохоронного органу отримано інформацію щодо проведення досудового розслідування за ознаками кримінального правопорушення, передбаченого ч. 2 ст. 307 КК України. У ході проведення досудового розслідування установлено, що певне коло осіб використовує банківські карти різних банків для отримання коштів, здобутих від незаконної реалізації психотропної речовини.

За результатами аналізу, Держфінмоніторингом встановлено, що на рахунки **групи з п'яти фізичних осіб**, відкриті у різних банківських установах, зараховувались кошти в готівковій і безготівковій формі від значної кількості встановлених та невстановлених фізичних осіб, в тому числі у якості розрахунків за медичні препарати. Надалі кошти перераховувались на інші рахунки, знімались готівкою або використовувались для оплати товарів та послуг.

В призначеннях платежів вказувались психотропні засоби, вільне розповсюдження яких є забороненим на території України. Фізичні особи, учасники фінансових операцій, пов'язані спільними адресами та, ймовірно, родинними зв'язками. Більшість учасників не зареєстровані як фізичні особи – підприємці. Крім того, обсяги фінансових операцій не відповідають офіційно задекларованим доходам.

Правоохоронним органом здійснюється досудове розслідування.



3.8. Відмивання доходів отриманих, від торгівлі людьми та розповсюдження відеозображень порнографічного характеру

Торгівля людьми та розповсюдження порнографії є глобальним злочинним бізнесом, сучасною формою рабства, яка залишається однією з найбільш актуальних проблем сучасних правових та економічних систем національного та міжнародного рівня. Протидія зазначеному виду злочинності потребує посилення спроможності уповноважених органів державної влади.

Значна частка даного виду злочинів пов'язана із трудовою та сексуальною експлуатацією.

В цілому, за 7 місяців 2021 року працівники поліції виявили понад 760 кримінальних правопорушень, пов'язаних з торгівлею людьми.

Разом із зазначеним видом злочинів, правоохоронним органом виявлено факти продажу немовлят за кордон.

Викрито та ліквідовано діяльність 26 організованих злочинних груп, до яких входило 139 учасників. 328 торгівцям людьми повідомлено про підозру.

Типові приклади розслідувань щодо відмивання злочинних доходів, отриманих від торгівлі людьми та розповсюдження відео зображень порнографічного характеру, наведено нижче.

Приклад 3.8.1.

Продаж немовлят за кордон

За інформацією Департаменту міграційної поліції, до складу організованої злочинної групи входило п'ятеро осіб, які здійснювали продаж дітей за кордон під виглядом сурогатного материнства.

Зловмисники створили **Товариство з обмеженою відповідальністю** для надання посередницьких послуг у межах програми сурогатного материнства.

Рекламу про свої послуги фігуранти розміщували на інтернет-платформах різних країн. Діяли зловмисники за відпрацьованою схемою:

підшукували жінок, які за грошову винагороду - від 300 до 1 000 доларів США погоджувались на фіктивні шлюби з іноземцями.

Лікар, який входив до складу організованої злочинної групи, оформлював фальшиві довідки щодо протипоказань для планування та виношування вагітності «дружинами». Це ставало підставою для офіційного застосування допоміжних репродуктивних технологій.

Відтак «сімейним парам» підшукували сурогатних матерів.

За виношування дитини жінкам платили від **6-8 тисяч доларів США**.

Після народження немовляти мати оформлювала довіреність на право вивозу батьком-іноземцем дитини за кордон. За послуги зловмисників громадяни іншої держави платили близько **70 тисяч доларів США**.

Наразі поліцейські встановили 16 фактів продажу дітей. Під час проведення обшуків правоохоронці вилучили чорнові записи. У них зазначена інформація щодо ще 160 замовлень від іноземців.

Приклад 3.8.2.

Фіктивне працевлаштування громадянина на роботу

За інформацією Національної поліції, до складу злочинної групи входило п'ятеро осіб, які ввели в оману 192 особи та привласнили півтора мільйона гривень.

Організатори злочинної схеми створили кілька юридичних компаній для надання посередницьких послуг із працевлаштування за кордоном. У ході досудового розслідування співробітники національної поліції встановили, що ліцензії на такий вид діяльності фірми не мали.

Правоохоронним органом повідомлено фігурантам схеми про підозру за ч. 4 ст. 190 (Шахрайство) КК України.

Приклад 3.8.3.

Розповсюдження відео зображень порнографічного характеру

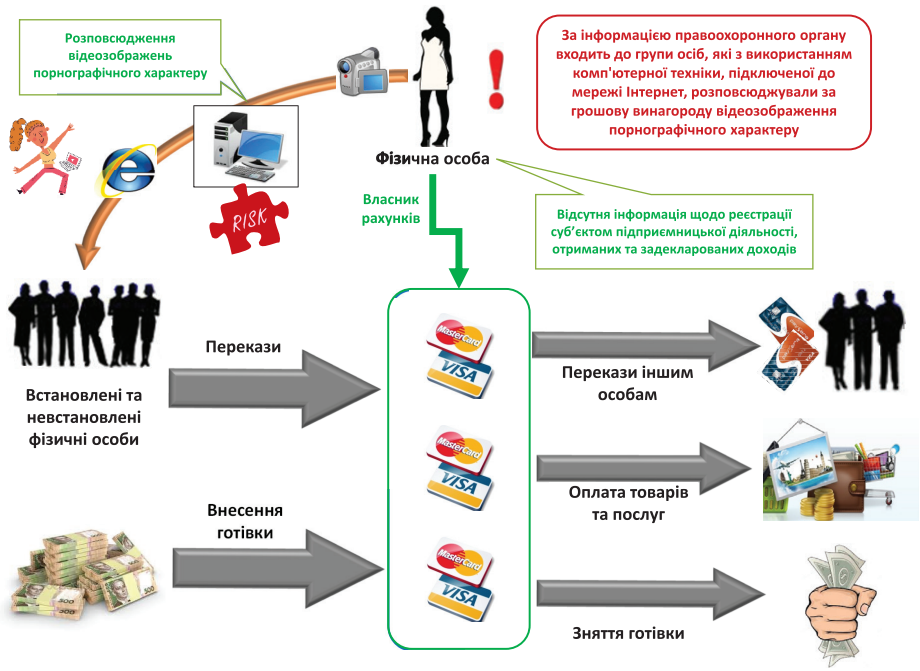
Держфінмоніторингом від правоохоронного органу отримано інформацію щодо проведення досудового розслідування за ознаками кримінального правопорушення, передбаченого ч. 3 ст. 301 та ч. 2 ст. 209 КК України. У ході проведення досудового розслідування встановлено групу фізичних осіб, які з використанням комп›ютерної техніки, підключеної до мережі Інтернет, розповсюджували за грошову винагороду відеозображення порнографічного характеру.

Держфінмоніторингом встановлено, що на карткові рахунки **фізичної особи** зараховувались безготівкові та готівкові кошти від значної кількості встановлених та невстановлених фізичних осіб.

Надалі, отримані кошти **фізичною особою** використовувались для придбання товарів/послуг, поповнення рахунків інших осіб, переведення в готівку. Значна частина готівкових операцій по внесенню/зняттю готівки проводилась **фізичною особою** – власницею карткових рахунків.

При цьому, вищезазначена **фізична особа** не входить до посадово-засновницького складу підприємств. Інформація про реєстрацію суб'єктом підприємницької діяльності, отримані та задекларовані доходи відсутня.

Правоохоронним органом здійснюється досудове розслідування.



3.9. Відмивання доходів від вчинення шахрайських дій

Згідно з даними Держфінмоніторингу, а також виходячи з відкритих джерел інформації, злочинці намагаються отримати вигоду з пандемії COVID-19 шляхом активізації шахрайської діяльності.

Згідно з даними Офісу Генерального прокурора, шахрайство займає значну частку у загальній структурі злочинів. Водночас з огляду на надзвичайно високу латентність цього злочинного діяння (особливо побутового шахрайства), є підстави вважати, що цей показник є значно вищим.

Проблематика шахрайства не втрачає своєї актуальності протягом останніх декількох десятиліть.

Згідно з положеннями чинного КК України, шахрайство можна розглядати в трьох розуміннях – вузькому (власному), широкому та найбільш широкому, а саме:

- шахрайство у вузькому (власному) розумінні включає заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою й кваліфікується за ст. 190 «Шахрайство» КК України;
- шахрайство в широкому розумінні включає також заволодіння спеціальним майном та іншими предметами спеціального призначення, зокрема:

  ст. 262 «Викрадення, привласнення, вимагання вогнепальної зброї, бойових припасів, вибухових речовин чи радіоактивних матеріалів або заволодіння ними шляхом шахрайства або зловживанням службовим становищем» КК України;

  ст. 289 «Незаконне заволодіння транспортним засобом» КК України;

  ст. 308 «Викрадення, привласнення, вимагання наркотичних засобів, психотропних речовин або їх аналогів чи заволодіння ними шляхом шахрайства або зловживання службовим становищем» КК України;

  ст. 312 «Викрадення, привласнення, вимагання прекурсорів або заволодіння ними шляхом шахрайства або зловживання службовим становищем» КК України;

  ст. 313 «Викрадення, привласнення, вимагання обладнання, призначеного для виготовлення наркотичниах засобів, психотропних речовин або їх аналогів, чи заволодіння ним шляхом шахрайства або зловживання службовим становищем та інші незаконні дії з таким обладнанням» КК України;

  ст. 357 «Викрадення, привласнення, вимагання документів, штампів, печаток, заволодіння ними шляхом шахрайства чи зловживання службовим становищем або їх пошкодження» КК України;

  ст. 410 «Викрадення, привласнення, вимагання військовослужбовцем зброї, бойових припасів, вибухових або інших бойових речовин, засобів пересування, військової та спеціальної техніки чи іншого військового майна, а також заволодіння ними шляхом шахрайства або зловживання службовим становищем» КК України;
- шахрайство в найбільш широкому розумінні включає також шахрайство з фінансовими ресурсами, яке кваліфікується за ст. 222 «Шахрайство з фінансовими ресурсами» КК України.

Типові приклади розслідувань щодо відмивання злочинних доходів, отриманих від шахрайських дій, наведено нижче.

3.9.1. Шахрайство з використанням банкомату, термінальних мереж, систем дистанційного обслуговування, соціальної інженерії

Фінансова сфера завдяки різноманітності інструментів для надання послуг є привабливим об'єктом для застосування різних шахрайських схем.

Дане питання не втрачає своєї актуальності, а лише змінюється кількість випадків шахрайства в розрізі різних інструментів.

Основними факторами трансформації сучасного шахрайства є перехід світової економіки до нового технологічного укладу, інформатизація суспільства у всіх сферах, глобалізація.

Але разом з цими можливостями з реального світу у віртуальний світ також проникають і такі соціальні явища, як шахрайство.

Підсумовуючи викладене вище, можемо зазначити, що існують наступні види шахрайської діяльності:

Шахрайство з використанням банкомату:

- зняття готівки з використанням «білого» пластику;
- використання скіммінгових інструментів (копіювання даних платіжних карток, у т.ч. з магнітної смуги, запис ПІН-коду тощо);
- зняття коштів із використанням банкомату без відбиття цієї операції на рахунку (Transaction Reversal Fraud);
- зняття готівки власником платіжної картки без її фізичного отримання (Cash Trapping);
- фізичні атаки на банкомати.

Шахрайство в термінальній мережі:

- здійснення операцій із використанням підробленої/викраденої/втраченої платіжної картки;
- отримання готівки через касу банку за підробленими документами та платіжною карткою;
- проведення дублюючих операцій касиром/оператором;
- проведення несанкціонованого/неточного списання (коли сума на чеку та сума, яка включена до розрахунку, відрізняються);
- компрометація касиром даних платіжної картки під час розрахунків у торговельно-сервісній мережі з метою їх подальшого несанкціонованого використання;
- використання накладок (скімерів) на термінальному обладнанні, яке дозволяє під час здійснення розрахунку зчитувати та передавати дані платіжної картки (протиправна домовленість з касирами);
- встановлення шкідливих програм, які пошкоджують програмне забезпечення терміналів.

Шахрайство в системах дистанційного обслуговування:

- несанкціоноване втручання та/або встановлення шкідливих програм (вірусів), які пошкоджують програмне забезпечення персональних комп'ютерів та перехоплюють паролі доступу до рахунків, інформацію з секретних ключів/токенів тощо.

Соціальна інженерія:

- виманювання шахраями, які входять в довіру до власників рахунків/власників карток, їх персональних даних, реквізитів платіжних карток або спонукання власників рахунків до здійснення переказу коштів на користь шахраїв.

3.9.2. Використання цифрових технологій для шахрайства

Останні роки в Україні фіксується стрімкий розвиток цифрової економіки.

Поширення он-лайн сервісів, перехід на електронну взаємодію суспільства та держави є логічним наслідком технологічного прогресу.

Під час пандемії COVID-19 багато хто користується Інтернет-банкінгом, отримує виписки-баланси на свої мобільні телефони, замовляє товари та послуги через мережу Інтернет.

Вказане привертає увагу злочинців, які прагнуть заволодіти доступом до сервісів жертви для вчинення шахрайських дій. Одним із важливих елементів отримання чи відновлення доступу до різних девайсів та електронних послуг є номер мобільного телефону.

За даними Комітету з питань цифрової трансформації Верховної Ради України більша частина абонентів в Україні отримають послуги мобільного зв'язку анонімно, тобто, проблема набуває характеру загальнонаціональної.

Але фактично, більшість абонентських номерів сьогодні вже «прив'язані» до конкретних осіб через банківські послуги.

Реєстрація абонентських номерів у постачальників електронних комунікаційних послуг створює умови для захисту абонентів від шахрайських схем.

Мають місце непоодинокі ситуації, коли внаслідок викрадення телефонів, у пам'ять яких було внесено персональні дані, виникали прикрі непорозуміння з банківськими рахунками. Використовуючи довірливість потерпілих зловмисники також отримують дані банківських карток, CVV та PIN-код.



Приклад 3.9.2.1.

Шахрайства з викраденням телефонних карт

Заволодівши номером телефону, шахрай отримує доступ до акаунта жертви в онлайн-банкінгу і, відповідно, до управління коштами.

Основні дії шахраїв щодо заволодіння фінансовим номером.

Крок 1: Формування журналу останніх дзвінків. Шахрай телефонує жертві з різних номерів телефонів. Очікує, що на деякі з них ви будете віддзвонювати. Таким чином він формує для себе список вхідних та вихідних дзвінків.

Крок 2: Сума поповнення рахунку. Паралельно шахрай поповнює ваш рахунок на невелику суму.

Крок 3: Звернення до оператора. Маючи інформацію з перших двох пунктів, шахрай звертається до мобільного оператора, щоб перевипустити сім-картку. Інформації про останні дзвінки та суму поповнення номера телефону часто достатньо для того, щоб оператор перевипустив «сім-карту».

Крок 4: Доступ до вашого профілю в онлайн-банкінгу. Маючи номер телефону, шахрай має можливість увійти в особистий акаунт жертви в онлайн-банкінгу. Шахрай також отримуватиме всі SMS-повідомлення з кодами підтвердження, які надсилає банк при трансакціях, доступу до мобільних застосунків тощо.

Приклад 3.9.2.2.

Заволодіння клієнтським профілем мобільного оператора

Шахраї намагаються «зламати» клієнтський профіль жертви у застосунку мобільного оператора з метою налаштування переадресації на підконтрольний номер телефону.

Основні дії шахраїв щодо заволодіння фінансовим номером.

Крок 1: Шахраї використовуючи номер телефону жертви пробують скинути пароль входу до клієнтського профілю. На номер телефона жертви приходить SMS з новим кодом для входу в клієнтський профіль або код для скидання пароля.

Крок 2: Злочинці телефонують жертві та в розмові виманюють код отриманий від мобільного оператора. Знаючи, що жертва є клієнтом певного оператора, шахраї можуть застосовувати різні техніки соціальної інженерії, прикидаючись працівниками банку або мобільного оператора тощо.

Крок 3: Шахраї змінюють налаштування в клієнтському профілі: встановлюють переадресацію на підконтрольний номер телефону, змінюють паролі та вживають інші дії необхідні для реалізації злочину.

3.9.3. Шахрайство з кредитами

Згідно з публікаціями правоохоронних органів збільшується кількість випадків із незаконним оформленням кредитів на громадян.

Встановлені факти масштабних механізмів вимагання грошей з громадян через незаконне оформлення онлайн-кредитів.

Учасники схем адмініструють бази «клієнтів» та здійснюють облік псевдоборгів. Для анонімізації телефонних номерів під час дзвінків з погрозами злочинці використовують спеціальне програмне забезпечення.

Приклад 3.9.3.1.

Незаконне оформлення онлайн-кредитів на громадян

За інформацією Національної поліції України, Фізична особа використовуючи методи соціальної інженерії, оформлювала онлайн-кредити на громадян у різних фінансових та мікрокредитних організаціях.

Фізична особа за допомогою комплексної соціальної інженерії незаконно отримувала доступи до фінансового мобільного номера, електронних скриньок та акаунтів у соціальних мережах громадян.

У скомпрометованих облікових записах вона вишукувала необхідну інформацію для ідентифікації осіб та оформлення на них онлайн-кредитів, зокрема паспортні та інші дані.

Надалі, підробивши паспортні дані та змінивши фінансові номери потерпілих на свій, фігурантка отримувала доступ до онлайн-банкінгу громадян. Це дозволило їй не лише «виводити» кредитні гроші, але й оформлювати нові кредити на потерпілих.

В рамках розслідування правоохоронним органом також був встановлений випадок, коли фігурантка через підбір паролю отримала доступ до електронної скриньки потерпілої, де зберігалися копії документів та особисті фото. Надалі з використанням цих даних правопорушниця отримала доступ до онлайн-банкінгу, далі видавши себе за клієнта банку, ініціювала передачу даних через BankID та увійшла до мобільного застосунку «Дія».

Фізичній особі вручено повідомлення про підозру у вчиненні кримінального правопорушення, передбаченого ч. 3 ст. 190 «Шахрайство» КК України.

3.9.4. Шахрайство через крадіжку ідентичності

Злодії, які займаються викраденням даних, зазвичай, отримують особисті дані (інформацію) жертви (паролі, паспортні дані, дані кредитних карток тощо), використовують їх для власних потреб, виступаючи від імені жертви.

Викрадена конфіденційна інформація (наприклад, у Facebook, Viber чи WhatsApp) може бути використана для різних незаконних цілей. Також, злодії можуть скопіювати профіль знайомого, так і викрасти його, або заволодіти чужим номером телефону і далі вже звертатись до знайомих.

Приклад 3.9.4.1.

Викрадення ідентичності в соціальній мережі

Фізична особа, яка здійснила крадіжку ідентичності в Facebook, використовуючи месенджер Facebook звертається до друзів у соціальній мережі та просить позичити грошей на термінові витрати.

Після отримання згоди від друзів позичити кошти, **Фізична особа – шахрай** надає банківські реквізити для переказу коштів.

3.9.5. Шахрайство з лотереями, призами, виграшами

Схема шахрайства з лотереями, призами чи виграшем, як правило, починається з того, що потенційна жертва отримує електронний лист, телефонний дзвінок або текстове повідомлення, в якому йдеться про виграш великої суми грошей, цінного призу або інших дій.

Як правило, користувачеві повідомляється про обмеженість часу для отримання виграшу й необхідності сплатити податковий збір, витрати на доставку або інші вигадані внески.

Оскільки такі повідомлення про лотереї, призи чи виграш є фальшивими, після сплати коштів зловмисникам, жертва не отримує очікуваних «призів».

Приклад 3.9.5.1.

Шахрайство під виглядом винагороди за участь у соцопитуваннях

За інформацією Національної поліції України, у різних соцмережах зловмисники поширюють відео, де від імені української телеведучої розповідається про виплати за участь у проходженні соціального опитування в галузі споживчого ринку.

В описі до відео шахраї розміщують посилання на ресурс, де нібито можна пройти опитування та гарантовано отримати грошову винагороду.

Разом із цим у коментарях зловмисники розміщують фейкові відгуки про успішне зарахування грошей.

Після проходження псевдоопитування громадянам пропонується ввести дані банківської картки для сплати «комісії» та зарахування грошей. Однак у разі виконання таких дій громадяни не лише переказують гроші аферистам, але й передають їм свої банківські дані, які шахраї використовують у власних інтересах.

3.9.6. Шахрайські дії з використанням фіктивних посадових осіб

Одним зі способів вчинення шахрайських дій є представлення злодіїв у якості представників органів влади та банківських установ.

Злочинці зв'язуються з потенційними жертвами (особисто, електронною поштою, телефонний дзвінок або текстове повідомлення) та видають себе за офіційних посадових осіб різних установ та організацій з метою отримати особисту банківську інформацію або готівкові грошові кошти.

У деяких випадках злочинці видають себе за співробітників правоохоронних органів, лікарень чи банківських установ.

Інформують потенційних жертв про неправдиві дані щодо подій з родичами, яким терміново необхідна допомога, чи про загрозу кримінального переслідування, або блокування банківської картки.

Також, для здійснення шахрайства під виглядом блокування банківських карток, зловмисники маскуються під працівників банківської установи для отримання конфіденційної фінансової інформації від жертв.

Приклад 3.9.6.1.

Шахрайство під виглядом блокування банківських карток

За інформацією Департаменту кіберполіції Національної поліції України, **Фізична особа** видавала себе за працівника банку і розсилала громадянам повідомлення про блокування їхніх банківських карток.

У повідомленнях зазначався телефон для зворотного зв'язку, за яким консультували з приводу «розблокування». **Фізична особа** переконувала потерпілих повідомити їй повні реквізити картки. Отримавши платіжні дані – привласнювала гроші.

За даним фактом відкрито кримінальне провадження за ч. 3 ст. 190 «Шахрайство» КК України.

Приклад 3.9.6.2.

Шахрайське заволодіння грошовими коштами юридичних осіб з використанням підроблених документів

Держфінмоніторингом встановлено використання невідомими особами банківського рахунку приватного виконавця з метою шахрайського заволодіння грошовими коштами ряду юридичних осіб фармацевтичної галузі, які територіально знаходяться в різних містах України, шляхом надсилання до банківських установ України платіжних вимог щодо списання боргу.

Встановлено, що здійснені спроби списання коштів з рахунків **трьох підприємств** фармацевтичної галузі, які відкриті у двох банківських установах, на рахунок **приватного виконавця**, відкритий в іншій банківській установі, у якості стягнення боргу згідно з виконавчими написами. Фінансові операції було зупинено банківською установою.

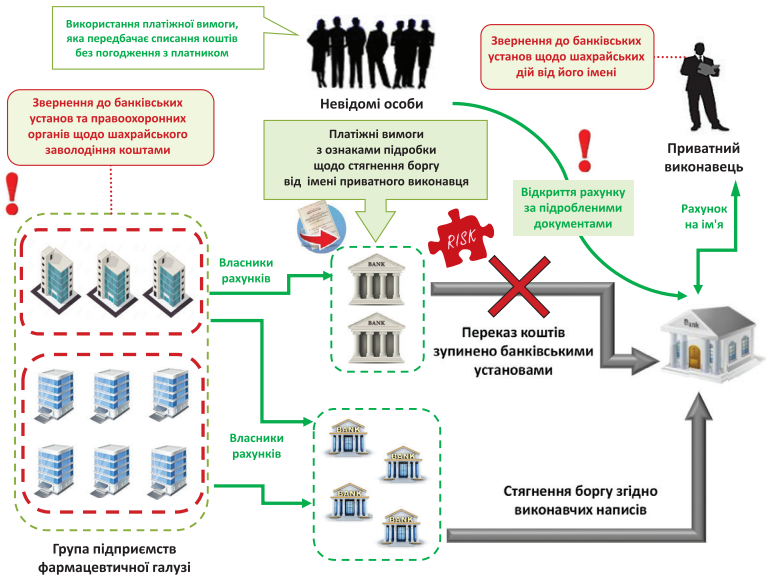
Спроби списання коштів здійснювались на підставі платіжних вимог, які передбачають переказ коштів на рахунок отримувача без погодження з платником.

Підприємства звернулись до банківської установи та правоохоронних органів щодо шахрайських дій невідомих осіб від імені **приватного виконавця**. Справжнім **приватним виконавцем** повідомлено, що вищезазначений рахунок ним не відкривався та платіжні вимоги не направлялись.

При аналізі документів з різних банківських установ виявлено, що підписи **приватного виконавця** відрізняються між собою, що свідчить про підробку документів.

Також встановлено, що в цей же період на рахунок, відкритий від імені приватного виконавця, зараховувались кошти від іншої групи підприємств фармацевтичної галузі з аналогічними призначеннями.

Правоохоронним органом здійснюється досудове розслідування.



3.9.7. Шахрайство під час онлайн-шопінгу

Один з популярних способів шахрайства в інтернеті – це афери при покупці товарів онлайн.

У зв'язку з пандемією кількість таких випадків зросла, зокрема, через нестачу певних категорій продуктів.

Злодії створюють фальшиві сайти, маскуючись під авторитетного продавця, для продажу дорогих товарів від відомих брендів за дуже низькими цінами.

Однак після замовлення покупець отримує або продукт-підробку, або взагалі нічого, а в гіршому випадку зловмисники можуть викрасти усі активи, маючи персональні дані особи (дані банківської карти).

З метою зниження ймовірності втрати грошей в результаті такого шахрайства доцільно отримати інформацію про діяльність продавця.

Приклад 3.9.7.1.

Привласнення коштів за допомогою фішингових інтернет-магазинів[3]

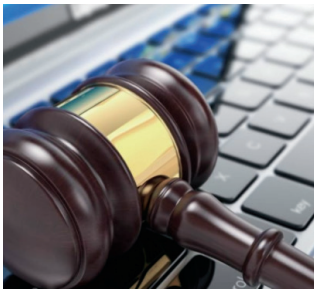
За інформацією Департаменту кіберполіції Національної поліції України, **Фізичні особи** створили ряд фішингових інтернет-магазинів, де пропонували людям електронну, мобільну, комп'ютерну та іншу техніку зі знижкою на умовах передоплати.

Створюючи враження реальних менеджерів, зловмисники, щойно отримували замовлення від клієнтів, передзвонювали їм нібито з call-центру і переконували: товар у наявності в якомусь іншому місті, тому його доставка можлива лише певною поштою і за умови повної попередньої оплати.

Ошукані громадяни вводили дані своїх банківських карток у форму на сайті або перераховували кошти на реквізити, що надавали злочинці, а ті знімали їх і більше на зв'язок не виходили.

3 Режим доступу: https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-zhyteliv-odesy-v-internet-shaxrajstvi-z-prodazhu-elektronnoyi-ta-orgtexniky-3473

3.9.8. Шахрайство через аукціони



Злочинці також маскують свої шахрайські дії шляхом створення підроблених аукціонів або через зламані акаунти Інтернет-аукціонів, де пропонують певний товар.

Після виграшу в аукціоні покупець платить призначену ціну, однак він ніколи не отримує цей продукт.

Приклад 3.9.8.1.

Привласнення коштів через зламані акаунти Інтернет-аукціонів[4]

За інформацією Департаменту кіберполіції Національної поліції України, **Фізичні особи** використовуючи скомпрометовані облікові записи отримували платіжні дані користувачів і використовували їх для онлайн-шопінгу.

Так, злочинці зламували облікові записи користувачів онлайн-аукціонів з продажу товарів. У скомпрометованих акаунтах фігуранти отримували

авторизовані дані платіжних систем (платіжні реквізити). Використовуючи ці відомості, зловмисники здійснювали покупки в Інтернеті.

Крім цього, **Фізичні особи** у DarkNet купували скомпрометовані облікові записи соціальних мереж. Після – несанкціоновано втручалися в їх роботу та налаштовували рекламу, сплата за яку стягувалася з банківських карток потерпілих. За такі дії зловмисники отримували прибуток від посередників рекламодавців.

Під час попереднього огляду вилученої комп›ютерної техніки правоохоронці виявили скомпрометовані дані доступу до персональних комп›ютерів та соціальних мереж декількох тисяч громадян Чехії, Італії, Франції, Німеччини, Естонії, Іспанії, Великої Британії, Польщі тощо.

4 Режим доступу: https://cyberpolice.gov.ua/news/policzejski-bukovyny-vykryly-zlovmysnykiv-u-zlami-akauntiv-internet-aukczioniv-dlya-pryvlasnennya-groshej-gromadyan-1341

3.9.9. Шахрайські схеми з інвестиціями

Актуальним питанням також є збільшення кількості шахрайських схем з інвестиціями, в яких повідомляють про те, що продукція або послуги належать певним особам.

Фактично злочинці здійснюють крадіжку ідентичності відомих компаній для реалізації шахрайських схем та поширення неправдивої інформації.

Дуже розповсюдженою шахрайською схемою є обкрадання людей під виглядом залучення інвестицій через спеціально створені вебресурси. Сайти нібито дозволяють отримувати прибуток через проведення операцій з купівлі-продажу банківських металів, іноземної валюти, криптовалюти, цінних паперів та інших активів. «Інвесторів» вводять в оману, імітуючи через програмний інтерфейс сайтів угоди купівлі-продажу та фіктивне зростання у 100 і більше разів прибутку від вкладених коштів. При подачі заявок на виведення прибутку у готівку до вкладників телефонують працівники шахрайських кол-центрів як представники торговельних платформ та вимагають внесення збору за обслуговування та комісії за переведення коштів в готівку. Додатково фізична особа повинна сплати ще 15-20% від суми «отриманих коштів».

Після оплати акаунти «інвесторів» блокуються, а кошти з них організатори шахрайської схеми забирають собі.

Приклад 3.9.9.1.

Підроблення документів з метою приховування джерел походження готівкових коштів

Держфінмоніторингом виявлено схему підроблення документів, наданих клієнтом до обслуговуючого банку як підтвердження джерел походження готівкових коштів.

В ході фінансового розслідування встановлено, що **Фізичною особою А** було здійснено внесення готівкових коштів на власний рахунок у значній сумі. В якості документів, що підтверджують джерела походження цих коштів, **Фізичною особою А** до **Банку А** було надано договір продажу власної квартири **Фізичній особі Б**, при цьому ціна продажу в декілька разів була вищою за ринкову вартість такої нерухомості.

В якості підтвердження джерел походження коштів у **Фізичної особи Б**, які було використано для придбання квартири, було надано договори купівлі-продажу цінних паперів, згідно з якими **Фізична особа Б** продала **Фізичній особі В** належні їй цінні папери, які обліковувались на рахунках у цінних паперах, відкритих у **Банку Б**.

Разом з цим, за інформацією, отриманою від **Банку Б**, встановлено, що **Фізична особа Б** ніколи не відкривала рахунки у цінних паперах, які було вказано у договорах купівлі-продажу. Крім того, встановлено, що зазначена особа працює за робітничою спеціальністю

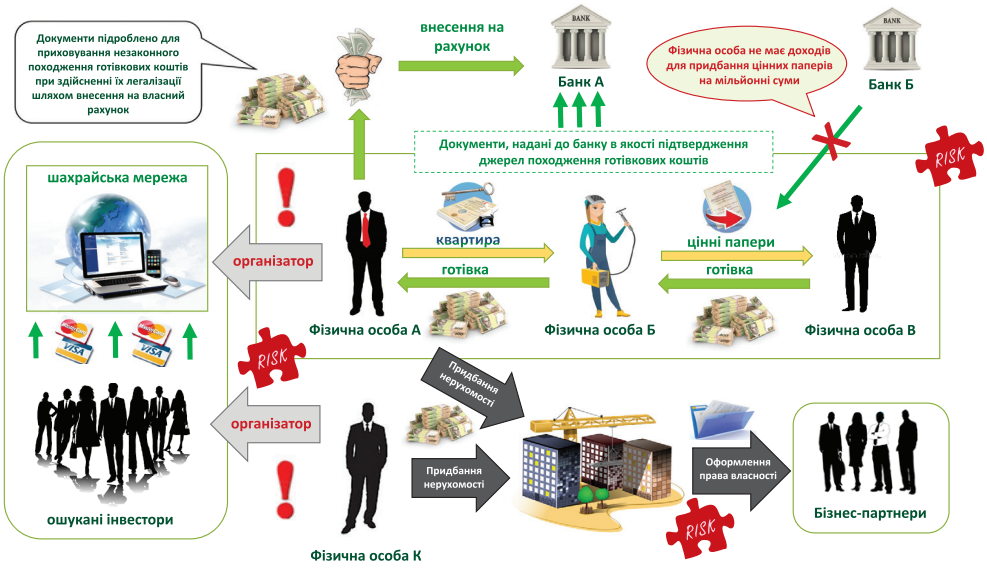
на одному із заводів, що не передбачає отримання доходу в сумі, достатній для придбання цінних паперів на мільйонні суми.

За інформацією правоохоронного органу **Фізична особа А** є одним з організаторів шахрайської схеми, яка полягає у залученні коштів фізичних осіб з різних країн через вебресурси, які, нібито, дозволяють отримувати надприбутки шляхом купівлі-продажу різних активів (банківських металів, криптовалют, акцій тощо), та в подальшому привласненні залучених коштів через ланцюг підконтрольних підприємств.

Надані до банківської установи документи було сфальсифіковано **Фізичною особою А** для приховування незаконного походження готівкових коштів при здійсненні їх легалізації шляхом внесення на власний рахунок.

Привертає увагу, що на квартиру, яку **Фізична особа Б** придбала у **Фізичної особи А**, накладено обтяження у вигляді іпотеки, яку, начебто, **Фізична особа Б** отримала від іншої особи, яка є бізнес-партнером **Фізичної особи А**. Внаслідок цього, **Фізична особа Б** не може розпоряджатись нерухомістю, оформленою на власне ім'я, що може свідчити про фіктивність зміни власника нерухомості та укладання угоди виключно для легалізації коштів.

Крім того, в ході розслідування встановлено, що **Фізична особа А** разом з іншим організатором шахрайської схеми – **Фізичною особою К** використовуючи привласнені кошти ошуканих інвесторів придбали велику кількість нерухомості, частину якої через фіктивні договори іпотеки переоформили на своїх бізнес-партнерів для уникнення розпізнавання.



Приклад 3.9.9.2.

Шахрайство з використанням торгової марки банку

За інформацією, служби безпеки банку виявлено нову схему шахрайства, яка використовує зареєстрований невідомими особами у США сайт та незаконно використовує логотип та айдентику банку.

Даний сайт є шахрайським, використовує посилання на вигадані інвестиційні проєкти та компанії без їхньої згоди, а також незаконно використовує айдентику банку та інших юридичних осіб.

Зазначається, що шахраї заманюють у шахрайський проєкт пропозицією високого доходу за схемою, яка притаманна виключно шахрайській фінансовій піраміді із застосуванням соціальної інженерії та ймовірного хакерства. Про злочинний характер схеми говорить й односторонній канал зв'язку в проєкті: після того, як людина заповнить форму, оператор шахрайського центру виходить на зв'язок для введення в оману клієнтів.

3.10. Відмивання доходів від кіберзлочинів

Кіберзлочинці постійно шукають нові способи вчинення злочинів через шкідливе програмне забезпечення.

Серед найвідоміших форм шкідливого програмного забезпечення можна виділити трояни, програми вимагачі, віруси, черв'яки та банківські шкідливі програми. Об'єднують всі ці види шкідливих програм – зловмисні наміри їх авторів чи операторів.

Спеціально розроблені електронні листи з небезпечними вкладеннями виявились ефективним та дешевим способом проникнення в комп'ютери та облікови записи жертв. Для цього зловмисникам потрібен лише один невірний клік користувача.

Непоодинокі випадки коли користувачі також стають жертвами підроблених сайтів, випадково компрометують власні реквізити електронних платіжних засобів та/або логіни/паролі доступу до систем Інтернет/мобільного банкінгу.

У подальшому злочинці здійснюють пакетне розповсюдження (продаж, поширення) інформації щодо скомпрометованих даних.

До кіберзлочинів (інформаційних злочинів) можна віднести злочини, скоєні за статтями, які входять до **Розділу 16 «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» КК України**, зокрема:

- ст. 361 «Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку» КК України;
- ст. 361[1] «Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут» КК України;
- ст. 361[2] «Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації» КК України;
- ст. 362 «Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї» КК України;
- ст. 363 «Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється» КК України;
- ст. 363[1] «Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку» КК України.

Типові приклади розслідувань щодо відмивання злочинних доходів, отриманих від кіберзлочинів, наведено нижче.

Приклад 3.10.1.

Заволодіння коштами компаній-нерезидентів через хакерську атаку

Держфінмоніторингом, з врахуванням інформації, отриманої від іноземного підрозділу фінансової розвідки, виявлено схему шахрайського заволодіння коштами компаній-нерезидентів.

В результаті хакерської атаки кошти **компанії-нерезидента А** були списані на рахунок **компанії Ю** в **банку 1**. По рахунку клієнта спостерігалось незвично швидке проходження коштів «транзитом». Валютні кошти зараховані від **компанії-нерезидента А** після продажу одразу перераховано на рахунки групи компаній в інших банках.

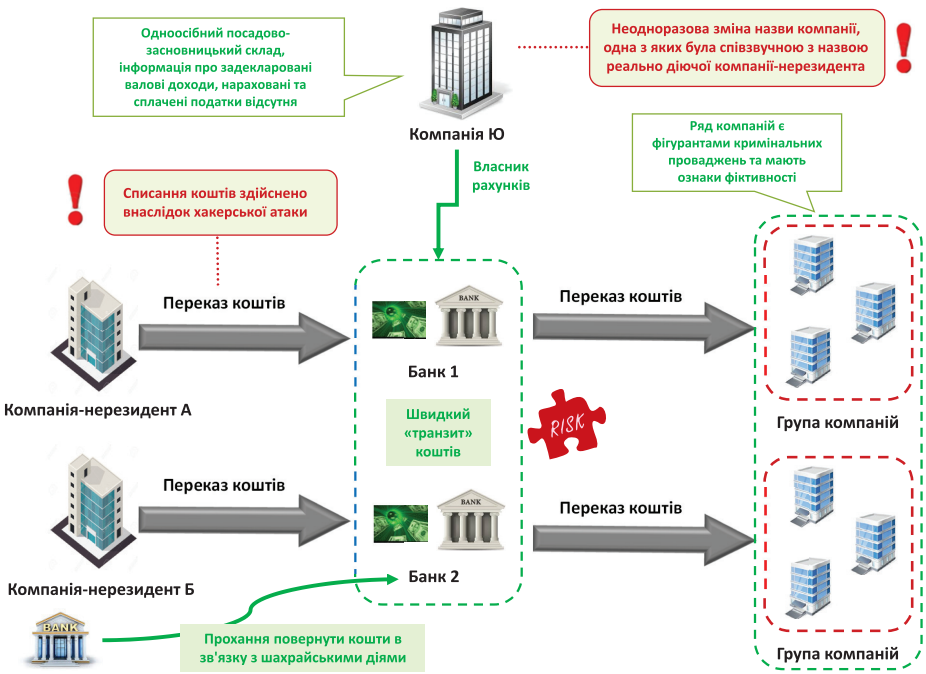
Відносини банку з клієнтом встановлено нещодавно (менш ніж три місяці), при цьому банк не міг зв'язатися з ним за наданими контактними даними.

Крім того, на рахунок **компанії Ю** в **банку 2** зараховано валютні кошти від **компанії-нерезидента Б**. Водночас, від іноземного банку отримано запит про шахрайські дії **компанії Ю**. Надалі отримані кошти виведені на групу компаній з ознаками фіктивності. Ряд компаній є фігурантами кримінальних проваджень.

Слід зазначити, що **компанія Ю** декілька разів змінювала назву, одна з яких була співзвучною з назвою справжньої компанії-нерезидента.

Компанія Ю має одноосібний посадово-засновницький склад, інформація про задекларовані валові доходи, нараховані та сплачені податки відсутня.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 3.10.2.

Незаконне заволодіння активами компанії-нерезидента шляхом несанкціонованого списання коштів

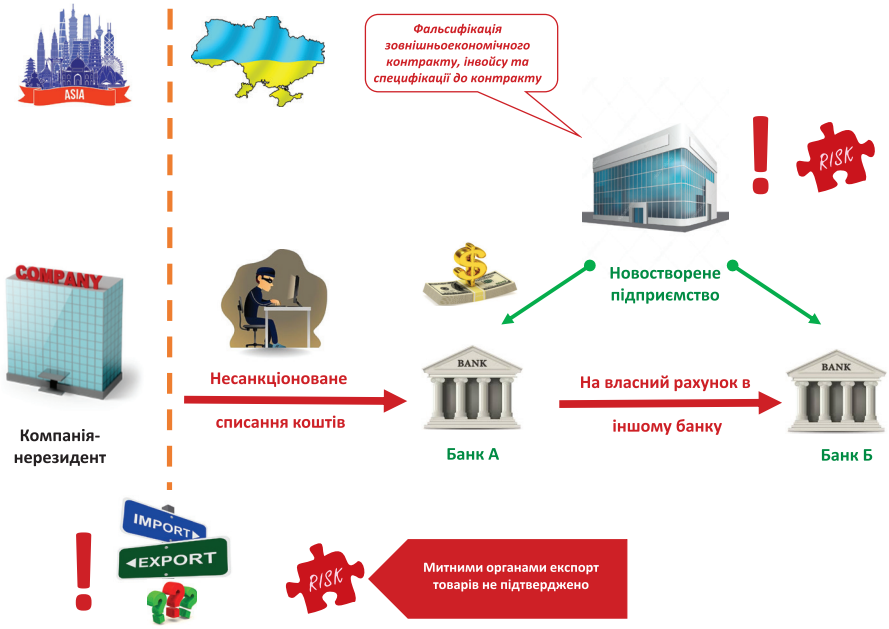
В ході фінансового розслідування, Держфінмоніторингом виявлено шахрайську схему спрямовану на незаконне заволодіння грошових активів **Новоствореним підприємством**, шляхом несанкціонованого списання коштів з рахунку **Компанії-нерезидента**.

Новостворене підприємство спробувало здійснити перерахування коштів з власного рахунку, відкритого в **Банку А** на інший власний рахунок, відкритий в **Банку Б**. При цьому до **Банку А** було надано сфальсифікований зовнішньоекономічний контракт, інвойс та специфікацію до контракту як джерело походження коштів на рахунку **Новоствореного підприємства**.

Слід зазначити, що митними органами експорт товару не підтверджено.

Привертає увагу, що **Новостворене підприємство** не є виробником товарів, зазначених у специфікації, та під час державної реєстрації використало назву відомого бренду іноземної компанії для здійснення шахрайських дій та привласнення коштів доброчесних юридичних та фізичних осіб.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 3.10.3.

Привласнення коштів підприємств за допомогою шкідливого програмного забезпечення

За інформацією Національної поліції України, викрито злочинну групу, яка викрадала грошові кошти з банківських рахунків юридичних осіб, використовуючи шкідливі програмні засоби.

В ході фінансового розслідування встановлено, що зловмисники створили та модифікували шкідливе програмне забезпечення, за допомогою якого отримували доступ до банківських програм електронних платежів «Клієнт-банк» та «Інтернет клієнт-банк». Вірусне програмне забезпечення надсилали на електронні скриньки різних підприємств.

Після його потрапляння на техніку – відстежували надходження грошей на банківські рахунки, здійснювали втручання в роботу програм і несанкціоновано перерахували гроші на підконтрольні рахунки.

За даним фактом відкрито кримінальне провадження за ч. 5 ст. 185 (Крадіжка), ч. 2 ст. 361-1 (Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів), ч. 2 ст. 361 (Несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем,комп'ютерних мереж чи мереж електрозв›язку), ч. 3 ст. 209 (Легалізація (відмивання) майна, одержаного злочинним шляхом) КК України.

3.11. Вчинення злочинів та відмивання доходів з використанням віртуальних активів

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

Віртуальні активи використовують інноваційні технології для швидкої передачі вартості по всьому світу та мають багато потенційних переваг, включаючи швидше та дешевше здійснення платежів.

Засновані на віртуальних валютах платіжні продукти та послуги створюють ризики відмивання грошей і фінансування тероризму в значних обсягах. Ця технологія дозволяє здійснювати анонімні перекази коштів в міжнародному масштабі.

Переваги криптовалюти:

- відкритий код алгоритму дає змогу добувати криптовалюту кожному;
- анонімність транзакцій (інформація про власника крипто гаманця відсутня, є тільки номер гаманця;
- відсутність єдиного цифрового банку;
- відсутність контролю за транзакціями та платежами.
- гроші зберігаються децентралізовано, тобто на гаманцях мільйонів користувачів у всьому світі - є одночасно і її недоліками та сприяють значній вразливості цього фінансового інструменту у сфері спекуляцій та використання для злочинних операцій, таких як торгівля людьми, контрабанда наркотиків, фінансування тероризму тощо.

Віртуальні валюти, що забезпечують анонімність як користувачів, так і операцій, дозволяють швидко переводити незаконні доходи з однієї країни до іншої, широко використовуються у кримінальному світі та мають попит.

Віртуальна валюта може бути або конвертованою в національну (або «фіатну») валюту або ж неконвертованою.

Валюти, що видаються низкою адміністраторів комп'ютерних ігор, є неконвертованими, оскільки можуть використовуватися лише в контексті гри (наприклад, гри Warhammer).

Віртуальні валюти на зразок біткоїна можуть конвертуватися у фіатні валюти. Тому саме конвертовані віртуальні валюти зазвичай потрапляють до поля зору злочинців та як наслідок правоохоронців.

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

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

15 Рекомендація FATF вимагає, що з метою протидії ВК/ФТ/ЗМЗ ринок надання віртуальних послуг повинен мати належний рівень регулювання, надавачі віртуальних послуг мають бути зареєстровані та отримати ліцензії, а також щодо них впроваджено належний рівень нагляду (моніторингу).

Євросоюз вживає різні масштабні заходи для боротьби з відмиванням коштів та фінансуванням тероризму, зокрема щодо більш ретельного контролю транзакцій в криптовалюті.

Традиційною технологією відмивання коштів в цій сфері є придбання за «злочинні» кошти різних видів віртуальних активів (криптовалют) та на наступному етапі за допомогою різних бірж та спеціальних сервісів-міксерів подрібнити початкові монети та конвертувати їх в інші криптовалюти.

Таким чином кошти можуть пройти сотні адрес, ускладнюючи відстеження початкового власника. Принцип роботи подібних сервісів простий, вони беруть криптовалюту у різних клієнтів, «перемішують» її, в кінцевому результаті виходить «мікс», який не дозволяє відстежити власника грошей.

У 2021 році британська поліція конфіскувала рекордну кількість криптовалюти на загальну суму $408 мільйонів у рамках розслідування про відмивання коштів.

Один з майданчиків торгів криптовалютою був причетний до відмивання коштів.

Віртуальні валюти можуть бути пов'язані зі злочинами:

- віртуальна валюта сама по собі може бути викрадена або одержана шахрайським способом;
- віртуальна валюта може бути використана для забезпечення анонімності під час купівлі таких речей, як наркотики або вогнепальна зброя;
- віртуальна валюта може застосовуватися в ході шантажу, наприклад, коли від компанії або установи вимагають сплатити викуп у віртуальній валюті за видалення шкідливого програмного забезпечення з комп'ютерної системи;
- віртуальну валюту можуть застосовувати для відмивання доходів від організованої злочинності та корупції, зокрема, в цілях швидкого переміщення активів через кордони.

Типові приклади розслідувань щодо відмивання злочинних доходів через віртуальні активи наведено нижче.

Приклад 3.11.1.

Проведення підозрілих транзакцій з використанням віртуальних валют

Держфінмоніторингом, з врахуванням інформації, отриманої від іноземного ПФР, банківських установ та баз даних, виявлено групу громадян України, які проводили підозрілі транзакції з використанням віртуальних валют.

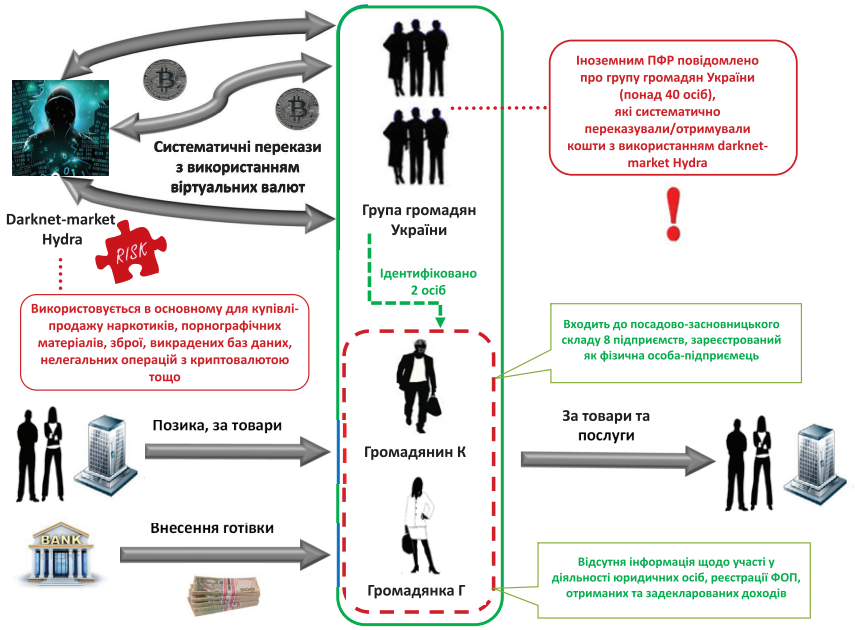
Так, іноземним ПФР повідомлено про **групу громадян України** (понад 40 осіб), які систематично переказували/отримували кошти з використанням **darknet-market Hydra**.

Привертає увагу, що зазначений інтернет-ресурс використовується в основному для купівлі-продажу наркотиків, порнографічних матеріалів, зброї, викрадених баз даних, нелегальних операцій з криптовалютою тощо.

В ході фінансового розслідування ідентифіковано **дві особи** з даної групи громадян. Слід заначити, що **громадянин К** входить до посадово-засновницького складу 8 підприємств, а також зареєстрований як фізична особа-підприємець. Водночас стосовно **громадянки Г** відсутня будь-яка інформація щодо участі у діяльності юридичних осіб, реєстрації як суб'єкта підприємницької діяльності, отриманих та задекларованих доходів, а також сплачених податків.

Держфінмоніторингом від банківських установ отримано ряд повідомлень про фінансові операції проведені за участю **громадянина К** та **громадянки Г**, в тому числі пов'язані з використанням готівкових коштів, які, не виключено, отримані від незаконних операцій протизаконного інтернет-ресурсу.

Правоохоронним органом здійснюється досудове розслідування.



Приклад 3.11.2.

Вчинення кіберзлочинів з використанням послуг користуванні крипто біржі Binance[5]

За інформацією правоохоронного органу, виявлена транснаціональна злочинна діяльність групи осіб, які використовуючи віддалене кероване шкідливе програмне забезпечення, отримали доступ до «AD» (ActiveDirectory – віддалене керування комп'ютером в операційній системі «Microsoft») серверів корейських компаній.

У подальшому злочинці встановили програму-вимагач «Clop» для блокування інформації та подальшого витребування викупу за розблокування інформації. Внаслідок кібератаки на чотирьох корейських компаніях було заблоковано 810 внутрішніх серверів та персональних комп'ютерів.

В ході розслідування встановлено, що вказана кібератака здійснювалась із сервера, який закріплений за IP-адресою, яка фактично знаходиться у м. Харків.

Встановлено, що до вчинення кримінального правопорушення причетна Фізична особа, яка має у користуванні криптогаманці на біржі Binance, та на які надходили кошти за розблокування інформації.

В ході розслідування встановлено, що Фізична особа має відношення до вчинення фінансових операцій та інших угод з грошовими коштами та іншим майном, здобутих завідомо злочинним шляхом, та не маючи офіційних доходів, які співрозмірні з його видатками, купує у свою приватну власність транспортні засоби, цінне нерухоме майно, земельні ділянки та інше.

За даним фактом відкрито кримінальне провадження за ч. 2 ст. 209 (Легалізація (відмивання) майна, одержаного злочинним шляхом), ч. 2 ст. 361 (Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) КК України.

Приклад 3.11.3.

Заволодіння ідентичності аккаунту на крипто біржі «Binance»[6]

Правоохоронним органом встановлено, що Фізична особа здійснила несанкціоноване втручання в роботу персонального комп'ютера потерпілого, що призвело до втрати грошових коштів.

Так, злочинці використовуючи аккаунт потерпілого на крипто біржі «Binance», заволоділи криптовалютою на суму 60 000 доларів США.

5 Режим доступу: https://reyestr.court.gov.ua/Review/98093620
6 Режим доступу: https://reyestr.court.gov.ua/Review/89612547

Приклад 3.11.4.

Створення онлайн-ресурсів для відмивання коштів та фінансування тероризму (сепаратизму) через віртуальні активи

Служба безпеки України заблокувала діяльність злочинного угруповання, яке займалося відмиванням та незаконним переведенням коштів, у тому числі з використанням криптовалют.

Так, організатори створили низку онлайн-ресурсів (сайти, телеграм-канали), які дозволяли користувачам конвертувати криптовалюту у готівку в особливо великих розмірах (на понад 240 млн грн).

Даним сервісом користувались також особи, які підтримують тероризм та сепаратизм. Дані транзакції здійснювались через заборонені іноземні електронні платіжні системи. Для відмивання коштів злочинці інвестували в нерухомість, земельні ділянки та дорогоцінні метали.

Приклад 3.11.5.

Використання криптовалюти як розрахунок за наркотичні засоби

В Одеській області Службою безпеки України виявлено функціонування нарколабораторії, яка займалась виготовленням амфетаміну. **Злочинці** також здійснювали контрабандне постачання МДМА (напівсинтетична психоактивна сполука амфетамінового ряду) з Нідерландів.

Для проведення розрахунків злочинці активно використовували криптовалюту Bitcoin.

Необхідна сума в Bitcoin розміщувалась в електронний гаманець продавця, якому за допомогою системи знеособлених чатів «Джаббер» повідомлявся електронний код для отримання доступу для коштів.

Для купівлі Bitcoin клієнти, які мали намір придбати наркотичні засоби або психотропні речовини, з використанням банківських карт українського банку за допомогою різноманітних іноземних сайтів придбавали криптовалюту.

Приклад 3.11.6.

Використання криптовалюти для сепаратистських акцій, терористичних, диверсійних та екстремістських актів

У Хмельницькій області в рамках кримінального провадження, розпочатого за ст. 110 «Посягання на територіальну цілісність і недоторканність України» КК України, Службою безпеки України викрито факт отримання винагороди у вигляді криптовалюти Bitcoin жителем регіону за виконання злочинних доручень співробітників спецслужб іноземної держави.

РОЗДІЛ IV. ОСНОВНІ ІНСТРУМЕНТИ, ІНДИКАТОРИ ТА СПОСОБИ ВІДМИВАННЯ ЗЛОЧИННИХ ДОХОДІВ ТА ФІНАНСУВАННЯ ТЕРОРИЗМУ (СЕПАРАТИЗМУ)

Різноманітність злочинних організаційних структур, постійна адаптація злочинців до методів та заходів протидії ВК/ФТ/ЗМЗ, які вживаються міжнародною спільнотою, а також високий ступінь пристосування злочинців до навколишніх змін дозволяє стверджувати, що інструменти, способи та методи вчинення злочинів постійно змінюються.

За результатами аналізу проведеного дослідження, Держфінмоніторингом було узагальнено найбільш поширені індикатори, які дозволяють виявляти схеми, пов'язані з відмиванням доходів та фінансуванням тероризму (сепаратизму).

Для здійснення належного підходу до впровадження ризик-орієнтованого підходу, суб'єкти, які залучені до ПВК/ФТ можуть розширювати коло індикаторів для виявлення підозрілих фінансових операцій (діяльності).

Основні інструменти у виявлених схемах відмивання злочинних доходів

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

- використання готівки;
- завищення/заниження вартості товарів/робіт/послуг;
- здійснення транзитних операцій;
- проведення безтоварних операцій;
- підміна (заміна) номенклатури товарів;
- неповернення валютної виручки;
- відсутність розрахунків за імпортними контрактами;
- використання фіктивних контрактів;
- надання/повернення фінансової допомоги;
- здійснення операцій з цінними паперами, в тому числі з так званими «сміттєвими»;
- придбання корпоративних прав;
- відступлення прав вимог (факторинг);
- страхування фінансових ризиків;
- здійснення пайової участі у будівництво;
- переведення активів на бізнес-партнерів;
- використання підроблених документів;
- придбання нерухомості та авто VIP класу;
- використання електронних грошей та системи миттєвих переказів;
- використання торговельних операцій для відмивання коштів;
- надання незаконних послуг через професійні мережі з відмивання коштів;
- операції з криптовалютою;
- використання механізму «зустрічних потоків»;
- виплата агентських винагород;
- використання шкідливих програм;
- проведення дублюючих операцій касиром;
- викрадення даних;
- злом акаунтів користувачів;
- використання накладок (скімерів) на термінальному обладнанні;

- створення компаній-клонів;
- використання підставних осіб;
- використання сміттєвих цінних паперів;
- соціальна інженерія;
- використання складних умов виплати страхового відшкодування.

Індикатори підозрілості учасників

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

- незначний досвід роботи (період діяльності), дата та місце реєстрації;
- відсутність найманих працівників або незначна кількість працюючих;
- одноосібний посадово-засновницький склад;
- засновником/керівником є особа, яка належить до соціально вразливих верств населення (студенти, пенсіонери, особи, які отримують соціальну допомогу тощо), особи зі спеціальним статутом (малозабезпечені, жебраки), особи молодого віку (до 20 років) або похилого (після 75 років);
- засновником/керівником є особа яка зареєстрована та проживає на непідконтрольній Україні території (тимчасова окупована територія у Донецькій та Луганській областях, Автономна Республіка Крим та місто Севастополь);
- компанії з реєстрацією в офшорних зонах, зонах бойових дій;
- юридична особа часто здійснює зміну назви або засновницько-посадовий склад;
- фізичні особи є кінцевими бенефіціарними власниками чи входять до посадово-засновницького складу великої кількості юридичних осіб;
- незначний статутний капітал;
- відсутність основних засобів/виробничих потужностей/складських приміщень/інших активів;
- ліквідація суб'єкта господарювання одразу після здійснення платежу;
- не є виробником товарів;
- відсутність нарахувань та виплати заробітної плати працівникам;
- відсутність ліцензій/дозволів на окремі види діяльності;
- відсутність задекларованих доходів та сплачених податків;
- відсутність орендних платежів;
- клієнт або його контрагенти є фігурантами кримінальних проваджень;
- документи містять суттєві помилки, суперечності або ознаки підробки;
- невідповідність КБВ;
- участь директора, бухгалтера, засновника в значній кількості юридичних осіб;
- у більшості тендерних закупівель в аукціонах приймає одна й та ж група осіб;
- відносно осіб, які входять до засновницько-посадового складу, наявні ухвали суду про подання підробних документів при реєстрації;
- назва юридичної особи збігається з назвою відомих міжнародних компаній;
- наявність податкового боргу;
- реєстрація за місцем масової реєстрації;
- по рахунках не сплачуються платежі, притаманні звичайній господарській діяльності;
- не відповідність штатної чисельності працівників юридичної особи взятим зобов'язанням;
- наявність негативної інформації у відкритих джерелах.

Індикатори підозрілості фінансових операцій (діяльності)

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

- необґрунтоване в значних розмірах використання готівки для розрахунків;
- транзитне проходження безготівкових коштів за рахунком (протягом короткого проміжку часу);
- учасник фінансової операції не надає пояснення щодо фінансових операцій та наявні ознаки щодо приховування джерел походження коштів;
- невідповідність отриманих доходів з обсягами проведених фінансових операцій;
- наявність фактів щодо підробки офіційних документів;
- звернення постраждалих осіб до правоохоронних органів;
- наявність інформації про відкрите кримінальне провадження чи судове переслідування учасника фінансової операції;
- проведення фінансових операцій, які не мають очевидної мети;
- проведення фінансових операцій зі значною кількістю контрагентів (невідповідність діяльності, розпорошення активів з метою приховування фінансових потоків);
- проведення фінансових операцій з поповнення значної кількості номерів мобільних телефонів;
- здійснення фізичною особою господарських (торгових) операцій без декларування підприємницької діяльності в органах державної влади;
- відсутність обов'язкових платежів на рахунках суб'єктів підприємницької діяльності та юридичних осіб, які притаманні звичайній господарській діяльності (оренда, комунальні послуги, податки, збори тощо);
- не розкриття інформації в призначенні платежу щодо підстав та мети переказу коштів;
- спонтанні обороти по рахунках юридичної особи (значні за обсягами обороти або повна відсутність оборотів);
- застосування суб'єктів господарювання з ознаками «фіктивності»;
- створення компанії «клона» відомої іноземної компанії;
- регулярні перекази коштів на рахунки юридичних осіб у якості оплати за договором факторингу, відступлення права вимоги та позик;
- проведення фінансових операцій за договорами страхування, які мають ознаки удаваних;
- фінансові операції з цінними паперами з ознаками «сміттєвих»;
- великі щоденні обороти коштів з незначним сальдо на початок та кінець дня;
- зарахування/списання коштів на/з рахунки/рахунків фізичної особи від значної кількості осіб, за відсутності реєстрації як суб'єкта господарювання;
- структуровані платежі;
- платежі без найменування конкретного товару/послуги;
- проведення сумнівних фінансових операцій між групою юридичних осіб, які розташовані за адресами масової реєстрації;
- учасником фінансової операції є особа, яка брала участь у діяльності незаконних збройних формувань;
- очевидна невідповідність призначень прибуткових та видаткових операцій за фінансовими операціями клієнта;
- проведення фінансових операцій пов'язаних з торгівлею корисними копалинами без наявності дозволів та ліцензій на їх видобуток або не підтвердження джерела таких копалин;
- придбання високовартісних активів із непідтверджених джерел;
- здійснення операцій з готівкою на мільйонні суми, за відсутності офіційно задекларованих доходів.

Способи легалізації (відмивання) злочинних доходів

За результатами дослідження встановлено наступні основні способи легалізації (відмивання) злочинних доходів та фінансування тероризму (сепаратизму):

- внесення готівкових коштів з використанням декількох рахунків у різних банківських установах та наданням одних і тих же документів та інформації про власні доходи для підтвердження джерела походження коштів;
- легалізація коштів шляхом придбання коштовного майна;
- надання фінансової допомоги пов'язаній компанії, яка через деякий час повертається та знімається готівкою;
- перерахування отриманих бюджетних коштів переможцем тендеру на користь ряду фізичних осіб – підприємців з призначенням платежу виплата доходу, при цьому діяльність підприємців обмежується періодом отримання бюджетних коштів;
- перерахування державним підприємством (бюджетною установою) коштів на користь суб'єкта господарювання без фактичного постачання товарів та надання послуг;
- отримання державних коштів суб'єктами господарювання, які не мають найманих працівників та виробничих потужностей, з подальшим перерахуванням частини коштів на користь посередників для виконання умов тендеру. Інша частина переводиться в готівку або перераховується на рахунки підприємств з ознаками фіктивності у якості надання фінансової допомоги/купівлі цінних паперів/переведення боргу з кінцевим отриманням готівки, або перераховується на рахунки підприємств, які здійснюють транзитні операції;
- підроблення документів, з метою підтвердження джерел походження готівкових коштів;
- здійснення експортних операцій без здійснення розрахунків;
- здійснення імпортних операцій без проведення розрахунків;
- виведення коштів за межі України шляхом підроблення імпортних контрактів та здійснення фіктивного імпорту;
- використання механізму «зустрічних потоків» для приховування обготівковування підприємствами, що здійснюють оптово-роздрібну торгівлю;
- зарахування коштів на користь фізичних осіб-суб'єктів підприємницької діяльності з подальшим обготівковуванням;
- виведення коштів з підприємства реального сектору економіки шляхом укладання фіктивних договорів страхування із страховою компанією;
- фінансування тероризму та сепаратизму за рахунок контрабандних поставок вугілля з тимчасово окупованих територій Донецької та Луганської областей;
- перерахування коштів на користь громадських організацій у вигляді грантів та допомог для можливого фінансування тероризму (сепаратизму);
- заволодіння шахрайським способом грошовими коштами юридичних осіб шляхом надсилання до банківських установ України платіжних вимог, з ознаками підробки, щодо списання боргу;
- заволодіння компаніями-клонами відомих виробників шахрайським способом коштами компаній-нерезидентів, з подальшим швидким перерахуванням коштів на користь компаній з ознаками фіктивності;
- використання карткових рахунків фізичних осіб для отримання коштів, здобутих від незаконного обігу наркотичних та психотропних речовин, зброї та відеозображень порнографічного характеру, з подальшим переведенням в готівку, а також переказами на користь інших встановлених та невстановлених осіб.

Найпоширеніші способи фінансування тероризму та сепаратизму

- перерахування грошових коштів за допомогою міжнародних електронних платіжних систем (Золота корона, Yandex гроші, Гроші@mail.ru QIWI, WesternUnion, MoneyGram, PayPal, Webmoney), електронних та Web гаманців;
- кеш-кур'єри;
- матеріальне забезпечення терористичних угрупувань, шляхом надання такого забезпечення неприбутковими (благодійними) організаціями, підконтрольними таким угрупуванням чи особам;
- здійснення міжнародних постачань з подальшим розрахунком на території інших країн;
- фінансування тероризму нерезидентами під виглядом законної діяльності;
- добровільна передача власних готівкових коштів фізичними особами представникам терористичних та/або сепаратистських організацій;
- перерахування грошових коштів на карткові рахунки членів терористичних угрупувань;
- використання фіктивних фінансових структур для отримання готівкових коштів;
- використання третіх осіб для збору коштів;
- використання банкоматів для зняття грошових коштів з банківських рахунків третіх осіб;
- використання дебетових карток;
- отримання кредитів без наміру їх повернення;
- використання взаємозаліків для прикриття грошових потоків;
- передача майна та інших активів безпосередньо особам, які причетні до тероризму;
- вимагання фінансової допомоги у суб'єктів господарської діяльності для подальшого фінансування тероризму та сепаратизму, у т.ч. ватажками збройних формувань, які діють на території ОРДЛО;
- вчинення грабежів, розбоїв, викрадення людей з метою отримання грошових коштів за їх викуп;
- несанкціоноване списання грошових коштів із рахунків юридичних осіб з подальшим перерахуванням на рахунки фізичних та юридичних осіб.

ВИСНОВОК

Результати проведеного типологічного дослідження вказують на зростання в умовах пандемії COVID-19 загроз в області шахрайства, кіберзлочинності, привласнення державних коштів.

При збільшенні кількості фінансових операцій, що проводяться віддалено, збільшується попит на використання онлайн торговельних платформ та віртуальних активів для здійснення платежів, а також проведення фінансових операцій поза межами фінансової системи країни.

Вразливості, що виникають пов'язані головним чином з відсутністю або майже неможливим контролем фінансових операцій, зокрема: неефективність у виявленні злочинів осіб, які причетні до надання послуг поза межами фінансової системи країни, необізнаність, недосвідченість та довірливість громадян в користуванні онлайн сервісами, а також використанні новітніх технологій, неврегульованість ринку віртуальних активів.

Використання типологічного дослідження під час аналізу фінансових потоків дозволяє встановити цілісну картину та алгоритм відмивання злочинних доходів або іншого злочину. Для встановлення таких схем потрібно мати широкий доступ до різного роду інформації та визначити перелік невідповідностей з відомими даними, а також систематизувати дані такого аналізу.

ДОДАТОК. АНАЛІТИЧНІ ІНСТРУМЕНТИ ДЛЯ КОНТРОЛЮ ТА МОНІТОРИНГУ

1. Аналітичні інструменти

У своїй діяльності суб'єкти для здійснення первинного фінансового моніторингу використовують наступні джерела інформації:

- дані з державних реєстрів;
- дані з відкритих публічних джерел;
- повідомлення правоохоронних органів;
- онлайн-сервіси перевірки компаній;
- результати журналістських розслідувань;
- офіційні документи Держфінмоніторингу та суб'єктів державного фінансового моніторингу;
- тощо.

З метою проведення належної перевірки клієнта на етапі встановлення ділових відносин, а також більш детального поглибленого аналізу протягом обслуговування задля моніторингу фінансових операцій клієнтів суб'єкти первинного фінансового моніторингу також використовують:

- власні скорингові моделі задля запобігання встановлення ділових відносин із клієнтами, що мають ознаки сумнівності;
- власні скорингові моделі оцінки ризику ділових відносин з клієнтом відповідно до типу клієнта (юридична особа, фізична особа, фізична особа-підприємець);
- розроблені матриці розрахунку рівня ризику публічних осіб;
- скринінгові моделі виявлення потенційно високоризикових клієнтів;
- різноманітні звіти та власні сценарії відбору підозрілих фінансових операцій (діяльності).

Суб'єкти первинного фінансового моніторингу з метою виявлення підозрілих фінансових операцій створюють відповідні правила відбору операцій за наступними полями: дата здійснення операцій, призначення платежу, сума, рівень ризику, країна, інформація щодо типу рахунку тощо.

Також, такі суб'єкти здійснюють сценарний аналіз, що включає дослідження обігу активів в цілому та окремих фінансових операцій клієнтів в динаміці.

Суб'єкти первинного фінансового моніторингу додають до власних аналітичних систем додаткову інформацію щодо учасників операцій та іншу інформацію, яка може значно розширити перелік даних для аналізу.

Виявлення фінансових операцій, що підлягають фінансовому моніторингу, з використанням автоматизованих систем, які включають зокрема аналіз критеріїв ризику та індикаторів підозрілості фінансових операцій, є дуже важливим для виконання завдань суб'єктом первинного фінансового моніторингу.

Приклад реквізитів для встановлення сценарію відбору підозрілих фінансових операцій (діяльності)

Щодо профілю клієнта:

- розмір статутного капіталу суб'єкта господарювання;
- вид діяльності суб'єкта господарювання;
- кількість працюючих суб'єкта господарювання;
- розмір доходів та сплачені податки суб'єкта господарювання;
- період діяльності юридичної особи/вік фізичної особи;
- інформація про кінцевого бенефіціарного власника, посадово-засновницький склад суб'єкта господарювання та їх участь в інших юридичних особах;
- інформація про зміни кінцевого бенефіціарного власника та посадово-засновницького складу суб'єкта господарювання;
- наявність інформації про відкриті кримінальні провадження з розслідування злочинів у сфері господарської діяльності щодо власника істотної участі/контролера або юридичної особи, її керівників та/або представників;
- наявність виробничих потужностей/торговельно-складських приміщень, інших активів, необхідних для ведення задекларованої господарської діяльності суб'єкта господарювання;
- потенційна сума (оборот) коштів, що може бути використаний суб'єктом господарювання за допомогою послуги (продукту).

Щодо фінансових операцій клієнта:

- кількість рахунків або платіжних карток суб'єкта господарювання;
- порівняння щодо обсягу дебетових та кредитових фінансових операцій за рахунком суб'єкта господарювання протягом одного дня/періоду;
- наявність змін в обсягах фінансових операцій, що здійснюються за рахунками клієнта суб'єкта господарювання;
- характер проведених фінансових операцій;
- інформація щодо використання сейфа суб'єктом господарювання;
- IP-адреси для здійснення фінансових операцій суб'єктом господарювання.

2. Публічні інформаційні ресурси контролюючих (державних) органів та приватних організацій

Використання автоматизованих процедур збирання та аналітичної обробки інформації з відкритих джерел є важливим кроком для підтримки прийняття управлінських рішень, підвищення рівня протидії ВК/ФТ/ЗМЗ.

Одержання додаткової інформації з публічних інформаційних ресурсів контролюючих (державних) органів та приватних організацій є важливим кроком для аналізу схем ВК/ФТ/ЗМЗ.

Держфінмоніторинг систематично проводить роботу щодо виявлення публічних інформаційних джерел для отримання додаткової інформації. Корисні посилання зазначаються відповідно до тематики дослідження.

Деякі корисні посилання наведені у типологічних дослідженнях Держфінмоніторингу за минулі періоди, які розміщені у відкритому доступі для користування.

Актуальні відкриті джерела що стосуються широкого кола питань наведено нижче.

2.1. Тероризм

Тероризм

Держфінмоніторинг	Перелік осіб, пов'язаних з провадженням терористичної діяльності або стосовно яких застосовано міжнародні санкції
https://fiu.gov.ua/pages/dijalnist/protidija-terorizmu/perelik-teroristiv	

Сайт «Миротворець»	Центр дослідження ознак злочинів проти національної безпеки України, миру, безпеки людства та міжнародного правопорядку.
https://myrotvorets.center	

Державний департамент США	Перелік країн, що підтримують тероризм.
https://www.state.gov/ country-reports-on-terrorism-2/	

2.2. Списки РБ ООН

Зведений список Ради Безпеки ООН

Рада Безпеки ООН	
https://www.un.org/securitycouncil/content/un-sc-consolidated-list https://scsanctions.un.org/search/	Зведений перелік фізичних і юридичних осіб, до яких застосовуються заходи, введені Радою Безпеки ООН.

2.3. Дані щодо фізичних осіб

Дані щодо фізичних осіб

Міністерство внутрішніх справ України	
http://wanted.mvs.gov.ua/searchperson	Особи, які переховуються від органів влади.

2.4. Публічні діячі

Публічні діячі

Пунктом 6 Додатку 9 до Положення, яке затверджено постановою Правління Національного банку України № 65, визначено джерела інформації, які можуть використовуватися банком для визначення належності клієнта до категорії PEP за умови, якщо рівень ризику ділових відносин (разової фінансової операції на значну суму) з клієнтом є вищим, ніж низький, а саме:

- бази даних сервіс-провайдерів, що надають безоплатно або платно інформаційні послуги;

- публічні джерела даних у мережі Інтернет, включаючи офіційні інтернет-представництва органів державної влади;
- офіційні інтернет-представництва систем декларування доходів публічними особами, включаючи Єдиний державний реєстр декларацій осіб, уповноважених на виконання функцій держави або місцевого самоврядування.

Відкритий реєстр національних публічних діячів України	Пошук національних публічних діячів та пов'язаних з ними осіб.
https://pep.org.ua/uk/	

Довідник «Офіційна Україна сьогодні»	Містить інформацію про органи державної влади та біографічні довідки урядовців.
http://dovidka.com.ua/user/	

Офіційний веб-портал Верховної Ради України	Інформація про народних депутатів України.
http://w1.c1.rada.gov.ua/pls/site2/p_deputat_list	

2.5. Декларації уповноважених осіб

Декларації осіб, уповноважених на виконання функцій держави або місцевого самоврядування

Єдиний державний реєстр декларацій	Єдиний державний реєстр декларацій осіб, уповноважених на виконання функцій держави або місцевого самоврядування.
https://public.nazk.gov.ua/	

Проєкт «Декларації»	База декларацій чиновників.
https://declarations.com.ua/	

2.6. Перевірка чинності документів

Перевірка чинності документів

Державна міграційна служба України (ДМСУ) https://nd.dmsu.gov.ua/	База даних недійсних, викрадених або втрачених документів, що посвідчують особу.

Міністерство внутрішніх справ України (Єдиний державний веб-портал відкритих даних) https://wanted.mvs.gov.ua/passport	Інформація про викрадені/втрачені/ недійсні паспорти громадянина України.

2.7. Фінансові санкції

Фінансові санкції

Міністерство фінансів США https://home.treasury.gov/ policy-issues/financial-sanctions/specially-designated-nationals-list-data-formats-data-schemas https://sanctionssearch.ofac.treas.gov/	OFAC публікує список осіб і компаній, які належать, контролюються або діють за чи від імені цільових країн.
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.	

2.8. Санкції України

Застосовані Радою національної безпеки і оборони України санкції

Рада національної безпеки і оборони України	Перелік фізичних та юридичних осіб стосовно яких застосовані обмежувальні заходи (санкції).
https://sanctions-t.rnbo.gov.ua/	

2.9. Реєстри Міністерства юстиції

Автоматизовані системи Єдиних та Державних реєстрів, що створюються відповідно до наказів Міністерства юстиції України

Реєстри Міністерства юстиції України	Оприлюднено дані з Єдиних та Державних реєстрів, що створюються відповідно до законодавства України.
https://nais.gov.ua/registers	

Кабінет електронних сервісів	Оприлюднено дані з Єдиних та Державних реєстрів, що створюються відповідно до законодавства України.
https://kap.minjust.gov.ua	

2.10. Будівництво

Портал державної електронної системи у сфері будівництва

https://e-construction.gov.ua/	Портал Єдиної системи в сфері будівництва є публічною частиною самої Системи та має на меті забезпечення безкоштовного безперешкодного доступу до інформації, що створюється в системі для всіх типів користувачів.

Портал забезпечує зручний пошук інформації з можливістю проектування даних на карту, а також базові аналітичні інструменти. Також на порталі доступні корисні онлайн сервіси, які стануть в нагоді для пошуку інформації. Функціональність Порталу розширюється по мірі розвитку Єдиної системи в сфері будівництва.

2.11. Цінні папери

Інформація щодо професійних учасників ринку цінних паперів

Агентство з розвитку інфраструктури фондового ринку України https://smida.gov.ua/	Інформація емітентів цінних паперів.

2.12. Судові органи

Реєстр судових рішень

Реєстр судових рішень	Єдиний державний реєстр судових рішень
https://reyestr.court.gov.ua/	

2.13. Власники банківських установ

Інформація про власників істотної участі у банках України.

Національний Банк України	Інформація про власників істотної участі у банках України.
https://bank.gov.ua/control/uk/publish/article?art_id=6738234&cat_id=51342	

2.14. Компанії України

Реєстраційні дані щодо компаній України

Інтернет адреси	Актуальні відомості та інформація щодо діяльності та даних суб'єктів господарювання, зареєстрованих в Україні.
https://youcontrol.com.ua https://opendatabot.ua https://clarity-project.info https://vkursi.pro https://zaparkanom.com.ua https://ca.ligazakon.net https://ring.org.ua	

2.15. Компанії, зареєстровані в іноземних юрисдикціях

Інформаційні ресурси щодо компаній нерезидентів

OpenOwnership https://opencorporates.com/	Найбільша відкрита база даних компаній в світі.
OpenOwnership – громадська технологічна ініціатива, яка розширює доступ до інформації про бенефіціарну власність. Наразі OpenOwnership містить дані по більш ніж 4,2 млн компаній. OpenOwnership також надає технічну допомогу урядам та компаніям, які прагнуть активно розкривати інформацію.	

Список Forbes Global 2000 http://www.forbes.com/global2000/list/#search	Найбільші компанії світу.

Центр по дослідженню корупції і організованої злочинності OCCRP https://www.occrp.org/ru/investigations	Центр по дослідженню корупції і організованої злочинності (англ. Organised Crime and Corruption Reporting Project, OCCRP) – 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.

База даних офшорних витоків ICIJ https://offshoreleaks.icij.org	База містить інформацію щодо понад 800 000 офшорних компаній, фондів і трастів із розслідувань Pandora Papers, Paradise Papers, Bahamas Leaks, Panama Papers та Offshore Leaks.

 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.

Dato Capital	Он-лайн база про компанії та їх директорів.
en.datocapital.com	

База містить інформацію про компанії зареєстрованих в Нідерландах, Великій Британії, Гібралтарі, Іспанії, Панамі, Каймановых Островах, Люксембурзі, Британських Віргінських Островах, Мальті, Кюрасао.

База має платний та безкоштовний контент.

Безкоштовно: організаційно-правова форма компанії, дата реєстрації, номер, юридична адреса, активна/неактивна, інформація про дату останніх змін.

Платно: реєстраційні та статутні документи, призначення/звільнення директорів, сплата податків, фінансова звітність.

Розширений платний звіт: реєстраційні документи, довіреності, повний перелік змін до статуту, перелік поданих документів, реєстраційна інформація з переліком директорів та секретарів, новини про компанію, інформація про директорів та секретарів компанії в інших компаніях.

Bureau van Dijk Electronic Publishing	Масштабна реєстраційна база про компанії, що зареєстровані у різних юрисдикціях по всьому світу.
https://www.bvdinfo.com/en-gb	

Незначну інформацію можна отримати безкоштовно (організаційно-правова форма, місце розташування, активна/неактивна), скориставшись он-лайн сервісом пошуку.

Відкритий портал даних Європейського союзу	Безкоштовно: доступ до відкритих даних, опублікованих установами та органами ЄС.
http://data.europa.eu/euodp/en/home	

Відкриті реєстри щодо реєстраційних даних компаній нерезидентів

Регіон (країна)	Опис	Адреса
Європейський Союз	Відкритий портал даних Європейського союзу. Безкоштовно: доступ до відкритих даних, опублікованих установами та органами ЄС.	http://data.europa.eu/euodp/en/home
Європейський Союз	Реєстр країн ЄС (включаючи Ісландію, Ліхтенштейн, Норвегію).	https://e-justice.europa.eu/content_find_a_company-489-en.do?clang=en
Європейський Союз	Офіційний список бізнес реєстрів країн ЄС.	https://e-justice.europa.eu/content_business_registers_in_member_states-106-en.do?clang=en
Європейський Союз	Офіційний список земельних реєстрів країн ЄС.	https://e-justice.europa.eu/content_land_registers_in_member_states-109-en.do
Європейський Союз	Консолідований реєстр неплатоспроможних компаній з країн ЄС.	https://e-justice.europa.eu/content_interconnected_insolvency_registers_search-246-en.do
Австрія	Реєстр та дані фінансової звітності компаній з Австрії. Містить платний контент.	https://www.firmenbuchgrundbuch.at/fbgb/easy/fb/search
Британські Віргінські острови	Дані про компанії Британських Віргінських островів	http://www.bvifsc.vg
Велика Британія	Судовий реєстр Верховного суду Великої Британії.	https://www.supremecourt.uk/current-cases/index.html
Велика Британія	Судовий реєстр адміністративних апеляцій Високого суду.	https://www.judiciary.gov.uk/about-the-judiciary/who-are-the-judiciary/judicial-roles/tribunals/tribunal-decisions/osccs-decisions/
Велика Британія	Реєстр компаній Великобританії	https://beta.companieshouse.gov.uk/
Велика Британія	Інформація про компанію в Сполученому Королівстві Великої Британії та Північної Ірландії, що, поміж іншим, охоплює: (адреса, дата заснування); поточні та колишні посадові особи компанії; сканкопії документів (реєстрація, зміни посадових осіб, річні звіти тощо); інформація про обтяження; попередні назви компанії.	https://www.gov.uk/government/organisations/companies-house

Регіон (країна)	Опис	Адреса
Велика Британія	Інформація про нерухомість, що, поміж іншим, охоплює: відомості про майно, включно з реєстрацією права власності, номером документа про реєстрацію права власності, відомості про власника, ціну купівлі, будь-які права проходу чи проїзду через територію, а також дані про те, чи «погашена», тобто виплачена, іпотека. Аналогічні реєстри нерухомості є в Північній Ірландії (https://www.nidirect.gov.uk/articles/searching-the-land-registry) та Шотландії (https://www.ros.gov.uk/).	https://www.gov.uk/search-property-information-land-registry
Велика Британія	Інтерактивна мапа та база даних власників іноземних компаній	http://www.private-eye.co.uk/registry
Велика Британія	У Великій Британії поліція має право встановлювати право власності на транспортний засіб через Національну базу даних поліції (Police National Database – PND). Державне агентство Великої Британії з реєстрації транспортних засобів і видачі посвідчень водія (UK Driver and Vehicle Licensing Agency – DVLA) веде облік зареєстрованих «тримачів» автомобілів, інформацію про яких надає за «достатніх підстав», навіть якщо особа, яка потребує такої інформації, не офіцер поліції.	https://www.gov.uk/request-information-from-dvla
Велика Британія	Судна	http://discovery.nationalarchives.gov.uk/browse/r/h/C3770037.
Велика Британія	Реєстрація повітряних суден у Великій Британії передбачає ведення реєстру та застосування засобів ідентифікації для британських власних та експлуатованих комерційних і приватних повітряних суден, до того ж реєстраційні позначення починаються з ідентифікаційного префікса «G». Реєстр веде Управління цивільної авіації Великої Британії.	http://www.caa.co.uk/Aircraft-register/G-INFO/Guidance-on-using-the-G-INFO-Database/

Регіон (країна)	Опис	Адреса
Велика Британія	Суд Корони – це загальнонаціональний суд, що проводить засідання за округами, центри яких розташовані в найбільших містах Англії та Уельсу. У ньому розглядають усі серйозні кримінальні справи, передані від магістратських судів. Справи розглядає суддя за участю 12 присяжних. В Англії та Уельсі діє близько 90 Судів Корони, серед яких Центральний кримінальний суд міста Лондона, відомий як «Олд-Бейлі». Рішення Суду Корони розглядає Відділ у кримінальних справах Апеляційного суду під головуванням Лорда головного судді. Апеляції від Апеляційного суду розглядають у Верховному суді.	http://www.nationalarchives.gov.uk/help-with-your-research/research-guides/criminal-courts-england-wales-from-1972/
Велика Британія	Судові документи. Пошук справ можливий за ім'ям обвинуваченого, назвою суду, правопорушенням або ім'ям адвоката. Після виконання пошуку буде показано загальну інформацію, але для перегляду вироків потрібно зареєструватися. Однак послугу надають безкоштовно.	http://www.thelawpages.com/court-cases/court-case-search.php?mode=1
Велика Британія та Північна Ірландія	У цій реєстраційній базі Сполученого Королівства безкоштовно можна отримати наступну інформацію: - інформацію про компанію (адреса, дата заснування); - про діючих та колишніх посадових осіб компанії; - сканкопії документів (реєстрації, зміни посадових осіб, річна звітність тощо); - відомості про обтяження; - попередні назви компанії; - відомості щодо неплатоспроможності; - відомості про бенефіціарів.	https://www.gov.uk/government/organisations/companies-house

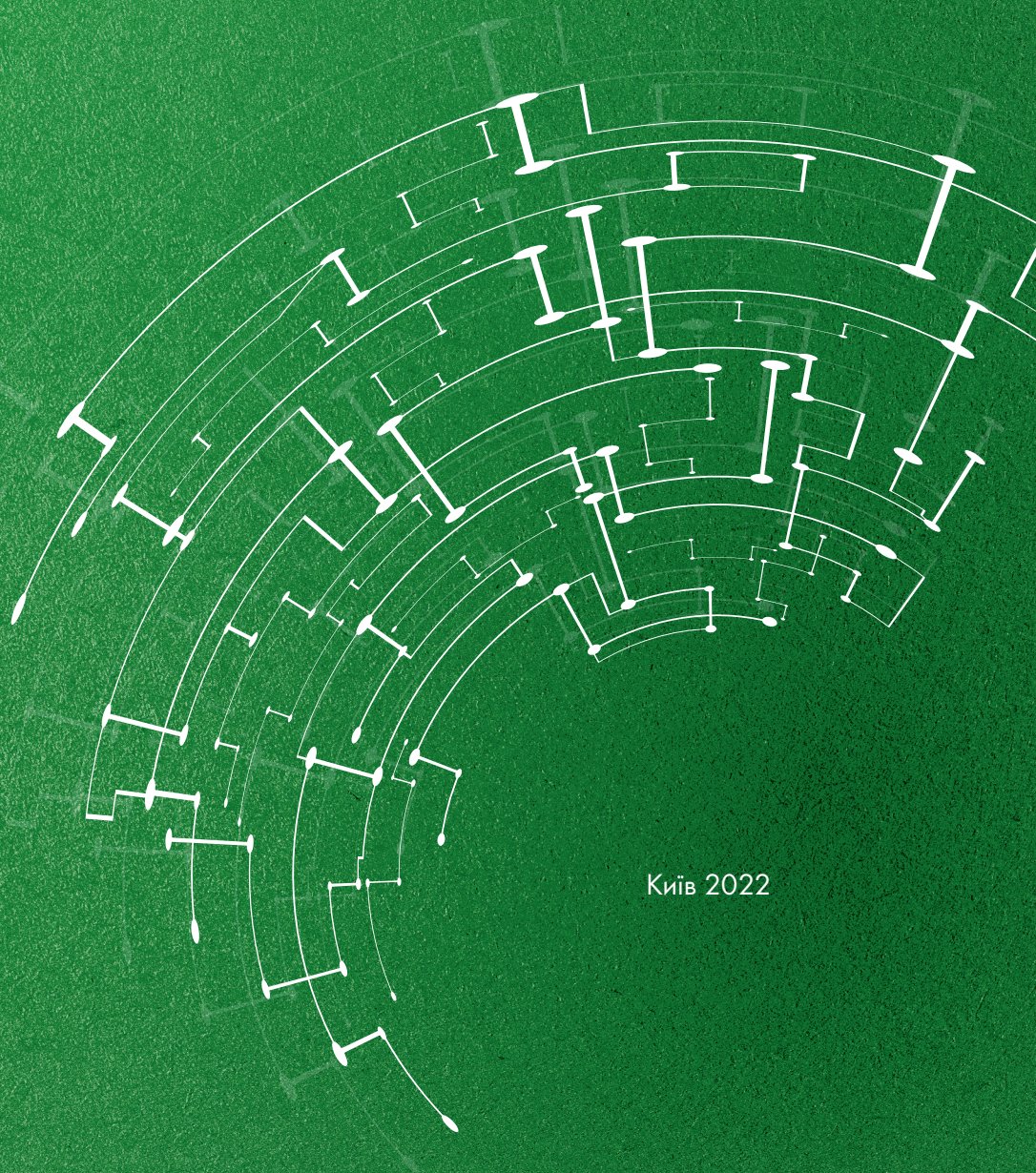
Регіон (країна)	Опис	Адреса
Велика Британія та Північна Ірландія	У цій реєстраційній базі Сполученого Королівства безкоштовно можна отримати наступну інформацію: - інформацію про компанію (адреса, дата заснування); - про діючих та колишніх посадових осіб компанії; - сканкопії документів (реєстрації, зміни посадових осіб, річна звітність тощо); - відомості про обтяження; - попередні назви компанії; - відомості щодо неплатоспроможності; - відомості про бенефіціарів.	https://beta.companieshouse.gov.uk/
Естонія	Безкоштовно: назва та організаційно-правова форма компанії, реєстраційний номер компанії, юридична адреса, розмір статутного капіталу, дата реєстрації та затвердження уставу, активна/неактивна, дати подання звітностей до реєстру.	https://ariregister.rik.ee/lihtparing
Естонія	Відкритий економічний реєстр Естонії	www.mtr.mkm.ee

2.16. Дані щодо активів

Повітряне судно	База даних реєстрації повітряних суден
http://www.airframes.org/	
Безкоштовно: за реєстраційним номером борту літака отримується інформація щодо моделі літака, типу, власника, дати виготовлення, історії. За кодом ICAO/IATA можна отримати інформацію щодо оператора авіаліній.	

Повітряне судно	Бази фотографій повітряних суден
https://www.planespotters.net/ https://www.jetphotos.com	
Безкоштовно: за реєстраційним номером борту літака видаються фотографії літака із вказанням дати та місця фотографування.	

Відстеження польотів	Глобальна служба відстеження польотів, яка надає інформацію про літальні апарати у всьому світі в режимі реального часу
https://www.flightradar24.com https://www.marinetraffic.com/	
Безкоштовно: за реєстраційним номером борту літака відстежується пересування літака в режимі реального часу. Платно: історія пересувань літака.	



Київ 2022