РИЗИКИ ВІДМИВАННЯ КОШТІВ ТА ФІНАНСУВАННЯ ТЕРОРИЗМУ У СВІТІ ВІРТУАЛЬНИХ АКТИВІВ

www.coe.int/moneyval

ТИПОЛОГІЧНИЙ ЗВІТ

2023

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Комітет Експертів з Оцінки Заходів Протидії Відмиванню Коштів та Фінансуванню Тероризму - MONEYVAL – є постійним моніторинговим органом Ради Європи, на який покладено завдання з оцінки відповідності міжнародним стандартам з протидії відмиванню коштів і фінансуванню тероризму, ефективності їх імплементації, а також завдання з розробки рекомендацій для національних органів влади в контексті необхідних покращень в їхній системі ПВК/ФТ. Через динамічний процес взаємних оцінок та регулярних звітів про прогрес, MONEYVAL має на меті покращити можливості національних органів влади протидіяти відмиванню коштів та фінансуванню тероризму більш ефективно.

Неофіційний переклад здійснено Державною службою фінансового моніторингу України

Типологічний Звіт щодо ризиків відмивання коштів та фінансування тероризму у світі віртуальних активів було прийнято Комітетом MONEYVAL на його 65-ому Пленарному Засіданні (Страсбург, 26 травня 2023).

Дизайн обкладинки: Рада Європи
Фото: Shutterstock

ЗМІСТ

Список скорочень

AMLD	Директива з протидії відмиванню коштів
ATM	Банкомат
CDD	Належна перевірка клієнта
CEPOL	Європейський поліційний коледж
DeFi	Децентралізовані фінанси
DLT	Технологія розподіленої мережі
ECOFEL	Центр Егмонтської Групи з питань досконалості та лідерства
EDD	Посилена належна перевірка
FATF	Група розробки фінансових заходів з протидії відмиванню коштів
FUR	Звіт про Прогрес
IT	Інформаційні технології
MER	Звіт про Взаємну Оцінку
MONEYVAL	Комітет експертів з оцінки заходів протидії відмиванню коштів
NFT	Невзаємозамінний токен
PEP	Політично значуща особа
SAR	Повідомлення про підозрілу діяльність
SNRA	Наднаціональна оцінка ризиків ЄС
STR	Повідомлення про підозрілу операцію
SWIFT	Товариство всесвітніх міжбанківських фінансових телекомунікацій
VASP	Постачальник послуг з віртуальних активів
ВА	Віртуальний актив
ВК/ФТ	Відмивання коштів / фінансування тероризму
ВНУП	Визначені нефінансові установи та професії
ВПД	Взаємна правова допомога
Егмонт	Егмонтська Група підрозділів фінансової розвідки
ЄАГ	Євразійська Група з протидії відмиванню коштів та фінансуванню тероризму
Європол	Агентство Європейського Союзу з питань співпраці правоохоронних органів
Євроюст	Агентство Європейського Союзу з питань співпраці у сфері кримінальної юстиції
ЄЕЗ	Європейська Економічна Зона
ЄС	Європейський Союз
НОР	Національна оцінка ризиків
НПО	Неприбуткова організація
ПВК/ФТ	Протидія відмиванню коштів / фінансуванню тероризму
ПО	Правоохоронні органи
ПФР	Підрозділ фінансової розвідки
РЄ	Рада Європи
РОП	Ризикоорієнтований підхід
ФУ	Фінансова установа

1. Вступ

Цей звіт має на меті представити комплексний огляд ризиків відмивання коштів і фінансування тероризму у світі віртуальних активів та їхніх постачальників послуг у країнах-членах MONEYVAL. Звіт містить горизонтальний аналіз рівня дотримання країнами-членами MONEYVAL Рекомендації 15, огляд заходів, вжитих для регулювання та нагляду за сектором постачальників послуг з віртуальних активів (VASP), а також деякі особливості виявлених ризиків використання VASP та віртуальних активів (VA) для відмивання злочинних доходів (тобто біржі, обмінні пункти, агрегатори та інші платформи криптовалют, включаючи електронні ігри, ставки на спорт і NFT).

Звіт був підготовлений командою під головуванням керівника проекту пана Девіда Бейкера (острів Мен) за підтримки експертів з Гібралтару, Мальти, Князівства Монако, Словацької Республіки та Словенії. Естонія та Відділ боротьби з кіберзлочинністю Ради Європи переглянули проект звіту.

Під час підготовки звіту командою проекту:

a) Підготовлено та розповсюджено опитувальник, до якої долучилися 15[1] країн-членів MONEYVAL.
b) Проведено літературний огляд опублікованих звітів і документів, включно з документами Групи розробки фінансових заходів з протидії відмиванню коштів, Егмонтської групи, Ради Європи та приватного сектору.
c) Проведено дві зустрічі проектної команди та одну розширену зустріч по типологіям[2], де всі країни-члени та спостерігачі MONEYVAL були запрошені для коментарів та обговорення.

Дослідження об'єднує та аналізує дані, отримані від країн-членів MONEYVAL, щодо кількох питань, що стосуються: 1) того, як члени регулюють діяльність з емісії ВА та функціонування VASP; 2) чи мають ПО достатні повноваження та інструменти для розслідування, визначення місцезнаходження та застосування тимчасових заходів щодо ВА, 3) типів платформ ВА, які використовуються для фінансової підтримки злочинної діяльності; 4) прикладів кейсів, розслідуваних відповідними органами, з описом злочинних схем із залученням елементів віртуальних активів, які були виявлені; 5) інші дані, що стосуються цілей дослідження.

Враховуючи вищезазначене, звіт структуровано у чотири розділи; Горизонтальна перевірка відповідності Р.15; оцінка ризиків ВА та VASP; ризикоорієнтований нагляд за сектором VASP; правоохоронні та операційні питання.

[1] Албанія, Андорра, Азербайджан, Боснія та Герцеговина, Болгарія, Німеччина, Гібралтар, Угорщина, Острів Мен, Латвія, Литва, Мальта, Сербія, Словаччина, Словенія

[2] Зустріч щодо Типологій відбулася 22 березня 2023 року

2. Ключові висновки

- Країни-члени MONEYVAL перебувають на різних етапах впровадження Рекомендації 15. Більшість членів потребують серйозних або помірних покращень. Кращих результатів було досягнуто в тих сферах, де VASP були включені до національного Закону про ПВК/ФТ як підзвітні суб'єкти. Деякі члени досягли кращого прогресу, ніж інші.
- Оцінка ризиків ВА та VASPs на національному рівні часто починається з перевірки зареєстрованих організацій у юрисдикції та визначення суттєвості сектора. Країни-члени повідомили, що було важко точно визначити суттєвість сектора.
- Під час оцінки ризику, вищий або нижчий ризик, який становлять установи, залежить від низки факторів, включаючи продукти, послуги, клієнтів, географію, бізнес-моделі та якість програми комплаєнсу установи. У більш розвинених юрисдикціях аналіз ризиків також враховує результати наглядових дій.
- Використання технологій під час виявлення та оцінки ризиків у цьому секторі виглядає хорошою практикою. Для кращого розуміння та пом'якшення ризику деякі країни придбали інструменти оцінки ризику блокчейну, а наглядовий орган навчив співробітників блокчейн-аналізу.
- Ліцензування, реєстрація та регулювання залишаються викликом, головним чином через здатність призначеного наглядового органу повністю розуміти ризики та особливості сектора.
- Різниця між реєстрацією в цілях нагляду з ПВК/ФТ та отриманням ліцензії може мати значний вплив на запобігання злочинності та управління галуззю. Деякі країни-члени повідомляють, що реєстрації все ще недостатньо, оскільки фірми з меншою репутацією використовують реєстрацію як штамп легітимності, а їхні клієнти рідко розуміють різницю між реєстрацією та регулюванням.
- Країни-члени MONEYVAL повідомляють про труднощі з виявленням незареєстрованих VASP або VASP без ліцензії на практиці.
- У нагляді за сектором VASP більшість країн-членів MONEYVAL знаходяться на початку етапу впровадження. Не всі наглядові органи мають вичерпні ресурси з точки зору персоналу та знань, і РОП рідко пристосований до оцінки ризиків, яка має секторальні особливості.
- Збір статистичних даних, що стосуються ВА та VASPs, покращить оцінку ризику, особливо в юрисдикціях, яким необхідно виявити незареєстровані національні VASPs або іноземні VASPs, що діють на території юрисдикції.
- Моніторинг транскордонних транзакцій все ще є проблематичним питанням (наприклад, проблема із застосуванням Travel Rule).
- Більшість країн-членів MONEYVAL отримують незначну кількість STR від VASP. Очевидно, що регулювання та нагляд за VASP позитивно впливає на обізнаність та обсяги STR.
- Відзначено занепокоєння щодо якості звітів VASP. Фактори, що сприяють цьому, включають (i) надмірну залежність від технологічних інструментів для виявлення потенційних підозрілих операцій, які можуть допомогти у виявленні червоних прапорців, але не можуть повністю замінити людський аналіз і досвід; (ii) надсилання захисних STR; (iii) перекладання зобов'язань щодо ПВК/ФТ, включаючи моніторинг транзакцій на аутсорс; (iv) брак досвіду у сфері ПВК/ФТ; та (v)

неправильне розуміння зобов'язань щодо звітності в ситуаціях, коли VASP працюють у кількох юрисдикціях.

- Шахрайство та сексуальна експлуатація дітей були виділені як поширені предикатні злочини, виявлені VASPs
- Відповідальність за розслідування ВК/ФТ найчастіше визначається не на підставі modus operandi справи (наприклад, чи включає вона ВА), а на основі типу основного злочину. Менші країни, як правило, мають один центральний правоохоронний орган, відповідальний за всі розслідування ВК/ФТ.
- Джерела фінансової розвідки значною мірою залежать від визначення VASP як підзвітних суб'єктів. Країни-члени здебільшого повідомляли, що законні повноваження щодо збору доказів під час розслідувань ВК/ФТ також охоплюють інформацію, яка зберігається у VASP.
- Існують труднощі зі збором доказів від VASP, розташованих в іноземних юрисдикціях, а канали ВПД не є ефективними для забезпечення своєчасного вилучення ВА, розташованих за кордоном.
- Більшості ПФР та ПО не вистачає відповідних технологічних інструментів і досвіду для ефективного аналізу та розслідування випадків ВК/ФТ, пов'язаних з ВА. Однак очевидно, що є інвестиції в навчання та співпрацю з VASP для накопичення досвіду.
- Можливість конфіскувати та заморожувати ВА залежить від присутності посередника VASP та/або володіння приватними ключами, які забезпечують контроль над ВА.
- Лише невелика частина розслідувань ВК/ФТ стосується доходів, отриманих злочинним шляхом, які є ВА. Це вказує на труднощі у виявленні та розслідуванні випадків ВК/ФТ, пов'язаних із ВА. Вартість заморожених і конфіскованих злочинних доходів, які є ВА, є незначною.

3. Відповідність країн-членів MONEYVAL Стандартам FATF з питань ВА та VASP: сучасний стан

Глобальні стандарти з ПВК/ФТ щодо ВА та VASP викладені в Рекомендації 15[3]. FATF опублікувала документи, спрямовані на те, щоб допомогти юрисдикціям і приватному сектору виконати нові вимоги з ПВК/ФТ щодо ВА та VASP[4].

Через особливості сектору та (відносно) нещодавнє прийняття стандарту переважна більшість країн-членів MONEYVAL ще не повністю імплементували ці вимоги. З 23 юрисдикцій, які були оцінені з червня 2021 року на відповідність Р.15, більшість потребують значних або помірних покращень. Зокрема, необхідні подальші вдосконалення щодо оцінки ризиків ВК/ФТ, нагляду та застосування превентивних заходів з ПВК/ФТ. У розділі нижче наведено детальний аналіз дотримання країнами-членами MONEYVAL конкретних зобов'язань, викладених у кожному відповідному критерії Р.15.

MER та FUR наступних 23 юрисдикцій-членів (які оцінював тільки MONEYVAL[5]) станом на квітень 2023 року були проаналізовані: Албанія, Андорра, Болгарія, Хорватія, Кіпр, Чеська Республіка, Естонія, Грузія, Гібралтар, Святий Престол (включаючи державу-місто Ватикан), Угорщина, Острів Мен, Ліхтенштейн, Литва, Мальта, Республіка Молдова, Князівство Монако, Польща, Сан-Марино, Сербія, Словацька Республіка, Словенія та Україна. Двоє членів (Латвія та Вірменія) не були оцінені на відповідність новим вимогам Р.15 у процесі звітів про прогрес.

Одна країна-член MONEYVAL – Святий Престол (включаючи державу-місто Ватикан) – заборонив ВА. В цілях цього горизонтального перегляду їх відповідність критеріям 15.1, 15.2, 15.3(a), 15.3(b), 15.5 та 15.11 було відображено в аналізі. Оскільки критерії 15.4, .15.6 – 15.10 не застосовуються до цієї юрисдикції, таблиці горизонтального аналізу відображають в якості присвоєного підрейтингу - N/A.

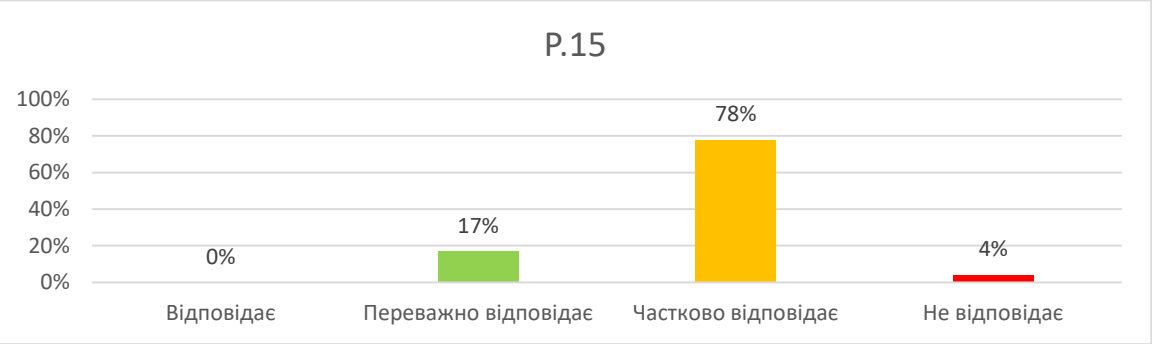
Близько 80% оцінених країн-членів не відповідають або лише частково відповідають вимогам Р.15. І жодна країна-член не відповідає повністю вимогам FATF щодо ВА та VASP.

[3] Критерії 15.1 і 15.2 не були детально оцінені, оскільки вони не охоплюють виключно зобов'язання щодо ВА та VASP.

[4] Оновлені Керівні Настанови з Ризикоорієнтованого Підходу до Віртуальних Активів та Постачальників Послуг з Віртуальних Активів (жовтень 2021) https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html; Індикатори Червоних Прапорців Відмивання Коштів та Фінансування Тероризму щодо Віртуальних Активів (вересень 2020) https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html; Цільове Оновлення в Контексті Імплементації Стандартів FATF щодо ВА та VASP (червень 2022) https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Targeted-update-virtual-assets-vasps.html

[5] Відповідність Ізраїлю, Німеччини та Великобританії вимогам Р.15 не було враховано в цілях цього горизонтального огляду

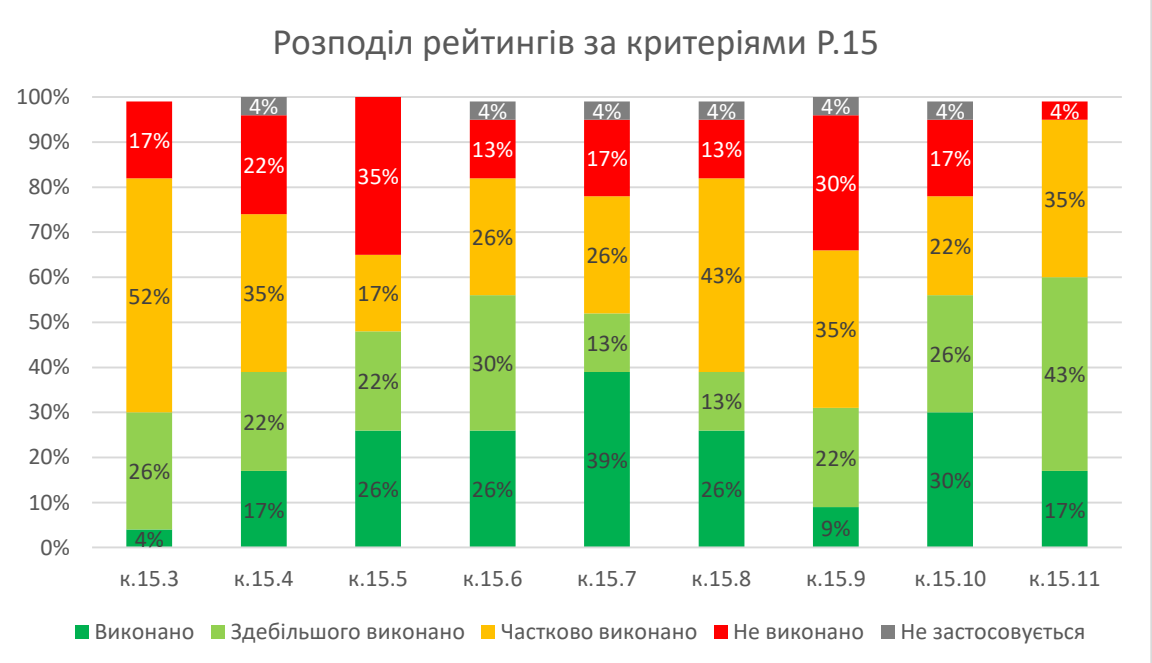
Рисунок 1 – Відповідність P.15 серед оцінених країн-членів MONEYVAL



* Таблиця показує підрейтинги 23 країн-членів MONEYVAL, отриманих під час процесу взаємних оцінок та звітів про прогрес
* Деякі цифри (%) були округлені

Незважаючи на те, що недоліки різняться в кожній юрисдикції, горизонтальний аналіз показує, що кращі результати були досягнуті щодо тих критеріїв, де національне законодавство таке, що включення VASP до підзвітних суб'єктів в Законі про ПВК/ФТ автоматично призведе до запровадження : нагляду і моніторингу, зобов'язання наглядових органів видавати керівні настанови, включення зобов'язань щодо цільових фінансових санкцій та міжнародної співпраці. Вимоги щодо проведення спеціальних оцінок ризиків і впровадження превентивних заходів (здебільшого через проблеми з Travel Rule та відсутність можливості моніторингу джерел/пунктів призначення) виявилися – навіть на технічному рівні – більш складними.

Рисунок 2 – Порівняння рівнів відповідності за різними критеріями P.15



* Таблиця показує підрейтинги 23 країн-членів MONEYVAL, отриманих під час процесу взаємних оцінок та звітів про прогрес
* Деякі цифри (%) були округлені

Аналізуючи результати відповідності країн-членів MONEYVAL вимогам P.15, слід зазначити, що перші два підкритерії не мають прямого відношення до питань ВА та VASP,

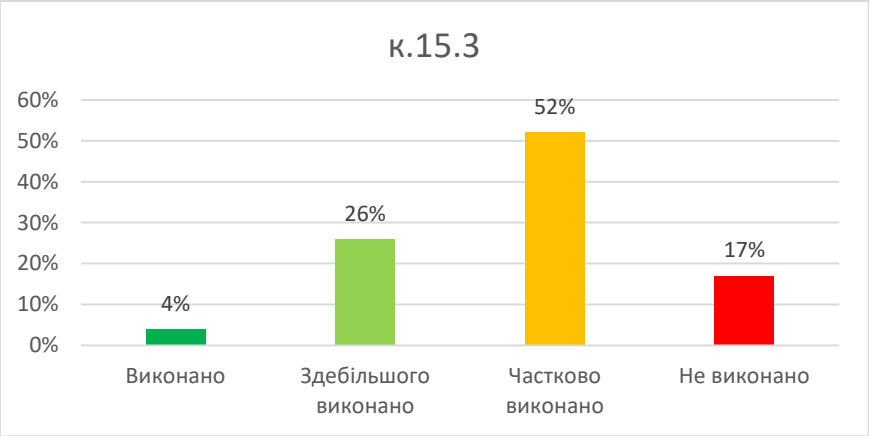
однак, вони все ще можуть впливати на загальний рейтинг технічної відповідності позитивно або негативно.

3.1 Оцінка та розуміння ризиків – виглядає як ризикована справа (к.15.3)

Оцінка конкретних ризиків, пов'язаних з ВА, виявилася однією з найпроблемніших сфер: лише 30% країн-членів досягли високих рівнів відповідності. При проведенні, оцінка ризиків може бути як самостійною, так і частиною НОР. Вимоги до самих VASP щодо виявлення, оцінки та управління ризиками часто вирішуються шляхом розширення зобов'язань з ПВК/ФТ, які вже діють для ФУ та ВНУП.

Цікавим спостереженням щодо відповідності країн-членів MONEYVAL к.15.3 є те, що оцінка ризику не була вичерпною, а інформація, використана для проведення оцінки ризику (якісна та кількісна), не була актуальною. Країни, які або тільки почали регулювати ВА та VASP, або мають невеликий сектор VASP, як правило, схильні до більш академічної оцінки ризиків, які значною мірою покладаються на інформацію (публікації) міжнародних організацій.

Рисунок 3 – Відповідність критерію 15.3

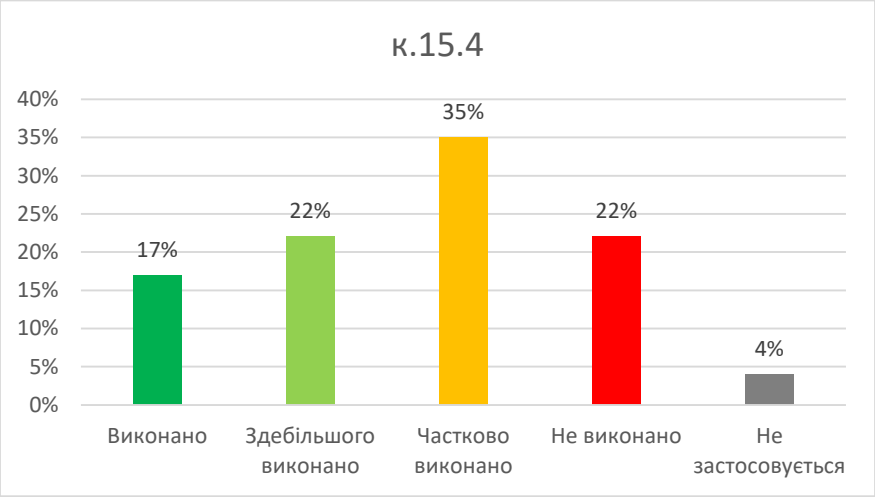


* Таблиця показує підрейтинги 23 країн-членів MONEYVAL, отриманих під час процесу взаємних оцінок та звітів про прогрес
* Деякі цифри (%) були округлені

3.2 Ліцензування та реєстрація – залишається викликом (к.15.4)

Серед оцінених країн-членів близько 39% отримали високу оцінку за зобов'язання реєструвати або ліцензувати VASP. Однак, навіть коли така вимога існує, виникають труднощі з її застосуванням, оскільки через свою природу VASP можуть працювати в різних юрисдикціях, не реєструючись та не маючи фізичної присутності. Рішення для подолання цієї проблеми включали ідентифікацію VASP, які рекламують себе офіційною мовою країни або які надають послуги, доступні для резидентів. Місцеві посередники, які шукають клієнтів або відвідують потенційних клієнтів-резидентів, можуть стати причиною застосування вимог щодо реєстрації. Деякі країни-члени не поширили реєстраційні чи ліцензійні режими на фізичних осіб, які здійснюють підприємницьку діяльність VASP.

Рисунок 4 – Відповідність критерію 15.4

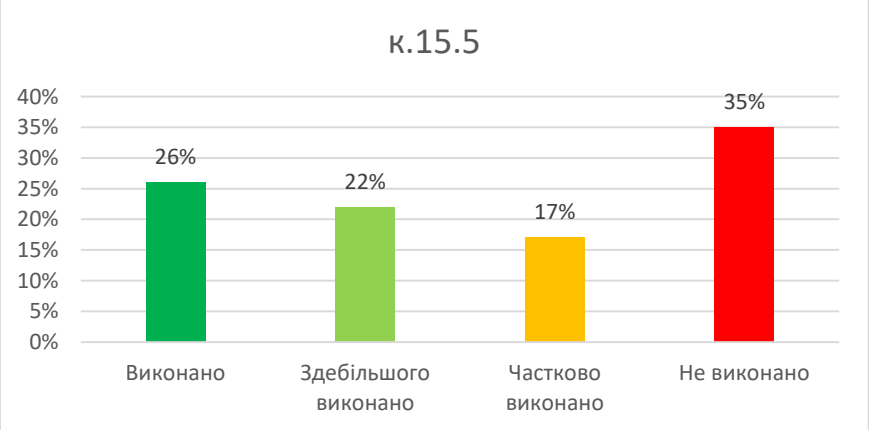


* Таблиця показує підрейтинги 23 країн-членів MONEYVAL, отриманих під час процесу взаємних оцінок та звітів про прогрес
* Деякі цифри (%) були округлені

3.3 Виявлення неліцензованих та незареєстрованих VASP – падіння ефективності в технічній відповідності (к.15.5)

Виявлення незареєстрованих або неліцензованих VASP здійснюється здебільшого за допомогою моніторингу засобів масової інформації, включаючи блоги у сфері фінансових технологій, і звітів третіх сторін. Іншим способом виявлення незареєстрованих VASP є онсайт перевірки органом, що реєструє. Першим кроком для досягнення відповідності на цьому фронті є прийняття положень, що забороняють діяльність незареєстрованих або неліцензованих VASP, що супроводжується суттєвим режимом санкцій за випадки невідповідності. Відсутність помітності та обмежене розуміння того, як VASP можуть працювати у їхній юрисдикції, є проблемою для виявлення неліцензованої діяльності. Крім того, якщо режим ліцензування/реєстрації не поширюється на фізичних осіб, органи влади не зобов'язані виявляти наявність неліцензованої/незареєстрованої діяльності з їх боку.

Рисунок 5 – Відповідність критерію 15.5

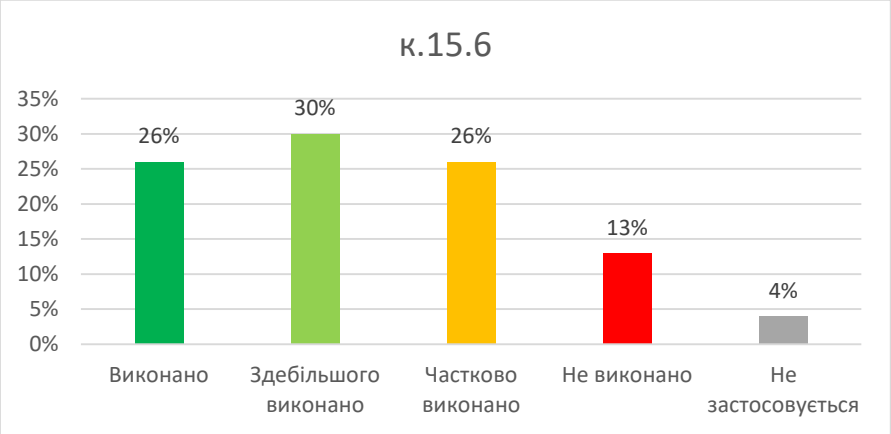


* Таблиця показує підрейтинги 23 країн-членів MONEYVAL, отриманих під час процесу взаємних оцінок та звітів про прогрес
* Деякі цифри (%) були округлені

3.4 Нагляд та моніторинг – якщо плисти за течією, це окупається (к.15.6)

Розподіл повноважень нагляду та моніторингу є однією з вимог, яка має найвищий рівень відповідності в загальному контексті Р.15. У багатьох випадках відповідальність за нагляд за VASP покладалася на вже створений наглядовий орган, як правило, Управління з фінансового регулювання та нагляду, ПФР або інший досвідчений компетентний орган влади, що здається хорошим рішенням. Однією з головних проблем у нагляді за VASP є розподіл персоналу, який мало коли відповідає суттєвості сектора. Інша виявлена проблема стосується рівня знань і навичок персоналу щодо функціонування ВА, а також застосування ризикоорієнтованого нагляду, якого неможливо досягти за відсутності високого рівня відповідності першому критерію, проаналізованому вище (15.3). Просте застосування однакових методів нагляду між секторами не працює.

Рисунок 6 – Відповідність критерію 15.6



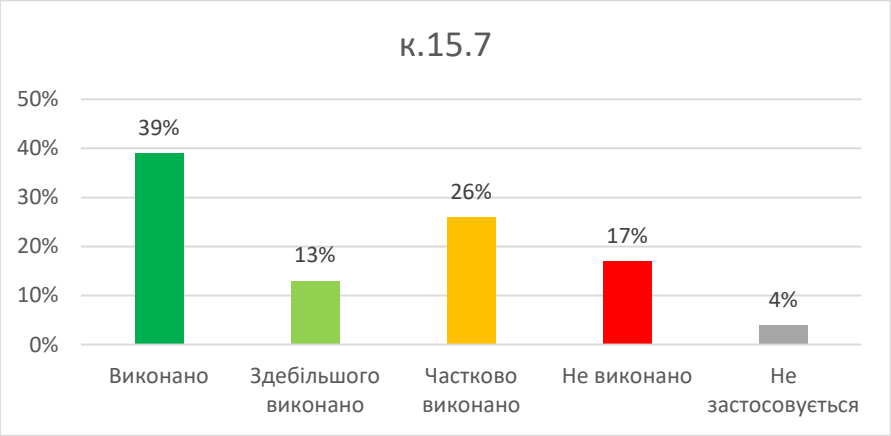
* Таблиця показує підрейтинги 23 країн-членів MONEYVAL, отриманих під час процесу взаємних оцінок та звітів про прогрес
* Деякі цифри (%) були округлені

3.5 Керівні настанови та фідбек – що посієш – те й пожнеш (к.15.7)

Інший досить позитивний висновок стосувався спроможності компетентних і наглядових органів влади розробляти керівні настанови та надавати зворотний зв'язок, щоб допомогти VASP застосовувати заходи з ПВК/ФТ для протидії ВК/ФТ, зокрема, для виявлення та повідомлення до ПФР про підозрілі операції. При включенні VASP до числа підзвітних суб'єктів будуть застосовуватись всі вимоги, що стосуються керівних настанов та фідбеку. Крім того, країни, які повністю виконали вимогу, опублікували спеціальні інструкції та рекомендації, що стосуються безпосередньо сектору VASP.

Рушійною силою сектору є ентузіасти, які, як правило, мають технічний досвід завдяки тісним зв'язкам між ВА та сектором інформаційних технологій. Це призводить до того, що члени команд з комплаєнсу часто мають досвід роботи у сфері ІТ, а не комплаєнсу. З цієї причини зворотний зв'язок дуже важливий для підвищення рівня відповідності вимогам з ПВК/ФТ.

Рисунок 7 – Відповідність критерію 15.7

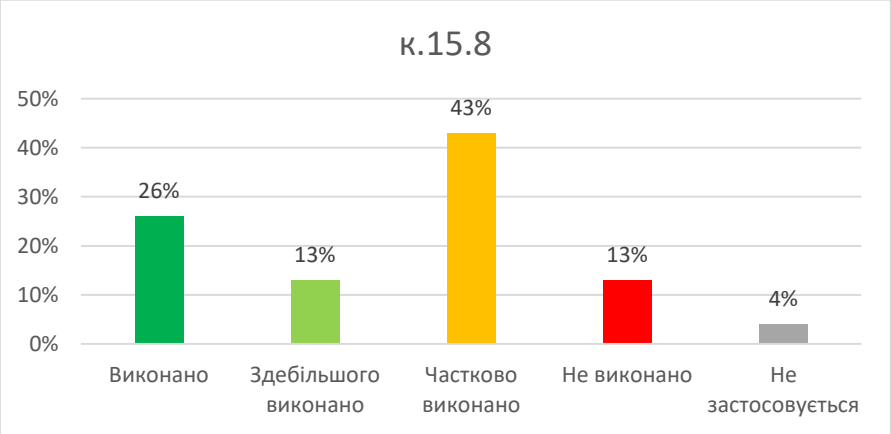


* Таблиця показує підрейтинги 23 країн-членів MONEYVAL, отриманих під час процесу взаємних оцінок та звітів про прогрес
* Деякі цифри (%) були округлені

3.6 Санкційний режим у випадку неспроможності відповідати вимогам – принцип батога та пряника (к.15.8)

Режим санкцій застосовує той самий підхід, що й механізми нагляду, а саме шляхом включення VASP до переліку підзвітних суб'єктів, що розширює наглядові повноваження на цей сектор. Цей підхід відносить цей критерій до тих, які мають високий рівень відповідності. Проблеми з дотриманням цього критерію полягають в обмеженому обсязі (наприклад, неможливість вилучити ліцензію) та діапазоні санкцій, які не були ані пропорційними, ані переконливими.

Рисунок 8 – Відповідність критерію 15.8



* Таблиця показує підрейтинги 23 країн-членів MONEYVAL, отриманих під час процесу взаємних оцінок та звітів про прогрес
* Деякі цифри (%) були округлені

3.7 Застосування превентивних заходів до VASP (к.15.9)

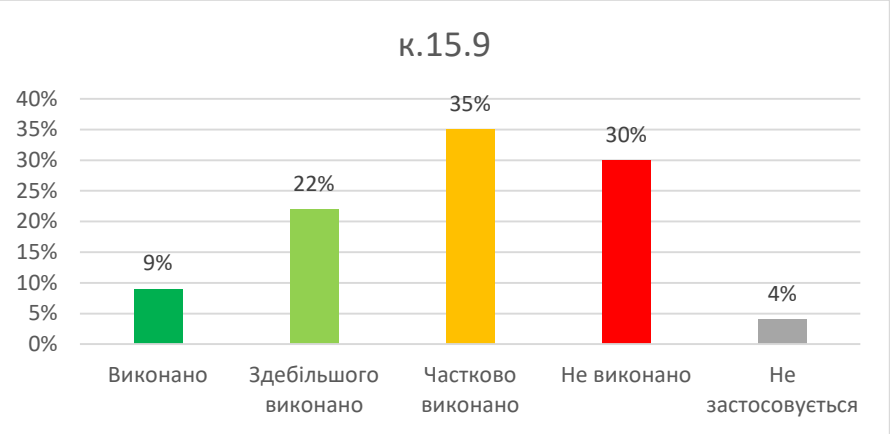
Попри те, що може здатися, що вимоги щодо запобіжних заходів можна легко реалізувати шляхом простого включення VASP до підзвітних суб'єктів нарівні з ФУ та ВНУП, рейтинги

показують обмежену відповідність вимогам: лише 9% країн-членів виконали вимоги цього критерію та 22% здебільшого виконали.

Деякі з труднощів у досягненні високого рівня відповідності у застосуванні превентивних заходів зумовлені системними недоліками, які однаково стосуються ФУ та ВНУП (наприклад, CDD, EDD, режим звітності, ведення документації тощо).

Також окремі проблемні питання стосуються вимог Travel Rule та надання інформації про отримувачів переказів.

Рисунок 9 – Відповідність критерію 15.9

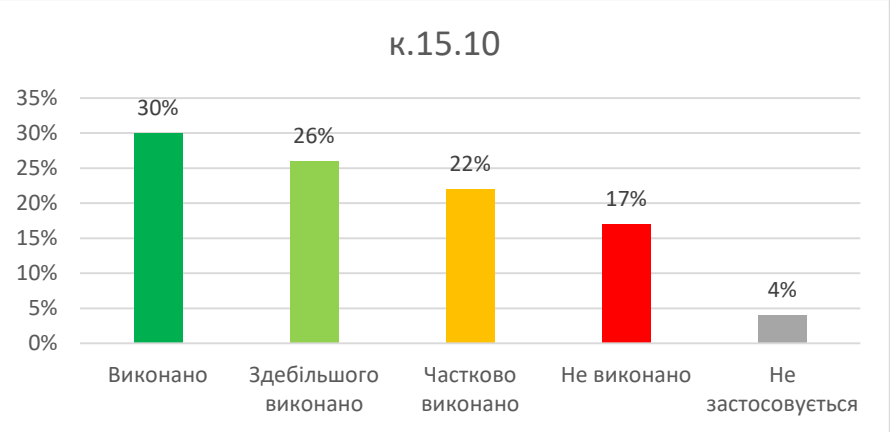


* Таблиця показує підрейтинги 23 країн-членів MONEYVAL, отриманих під час процесу взаємних оцінок та звітів про прогрес
* Деякі цифри (%) були округлені

3.8 Цільові фінансові санкції є ...цільовими (к.15.10)

Дотримання вимог забезпечується за рахунок застосування тих самих правил та механізмів, які використовуються для ФУ та/або ВНУП. Недоліком, який спостерігається в учасників, які не відповідають даному критерію, є те, що зобов'язання з ЦФС не поширюються на VASP.

Рисунок 10 – Відповідність критерію 15.10

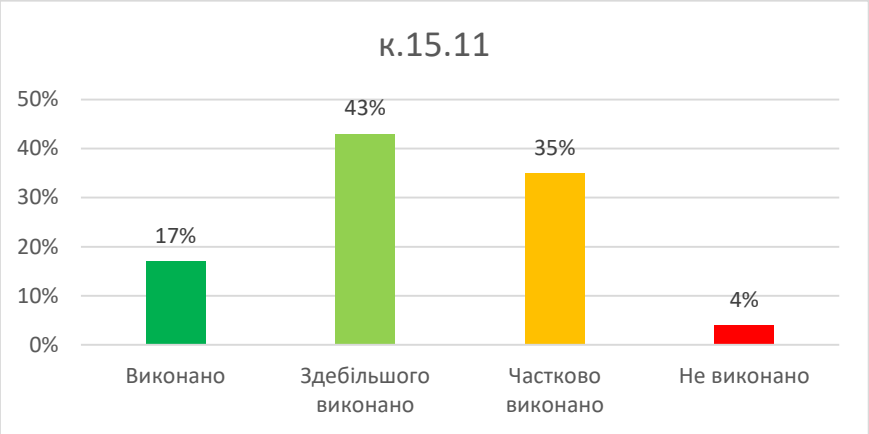


* Таблиця показує підрейтинги 23 країн-членів MONEYVAL, отриманих під час процесу взаємних оцінок та звітів про прогрес
* Деякі цифри (%) були округлені

3.9 Міжнародна співпраця – тісний зв'язок (к.15.11)

Найвищий рівень дотримання вимог Р.15 відзначається щодо спроможності органів влади забезпечувати максимально широке сприяння міжнародній співпраці з іноземними партнерами, коли йдеться про ВА. Цей позитивний результат зумовлений широкими повноваженнями органів влади щодо обміну інформацією, незалежно від типу залучених активів. Недоліки, виявлені у зв'язку з к.15.11, стосуються більше системних проблем і випливають з Р.36-Р.40.

Рисунок 11 – Відповідність критерію 15.11



* Таблиця показує підрейтинги 23 країн-членів MONEYVAL, отриманих під час процесу взаємних оцінок та звітів про прогрес
* Деякі цифри (%) були округлені

4. Розуміння ризиків, які походять від неправомірного використання ВА та VASP з метою ВК/ФТ

Як описано в горизонтальному огляді Р.15 вище, не всі учасники оцінили ризик ВК/ФТ, який становлять ВА та VASP, а якщо така оцінка ризику і проводилася, то в багатьох випадках вона була недостатньо поглибленою.

Кейс 1: Оцінка ризику ВА та VASP – Андорра

Андорра провела свою другу НОР, що завершилася у грудні 2020 року, використовуючи результати дворівневого дослідження (як національного, так і секторального) і незалежної оцінки ризиків як НПО, так і сектору ВА.

Дослідження сектору ВА включало розділ, присвячений основним застосовним визначенням (включаючи визначення «віртуальний актив», «постачальник послуг віртуальних активів», «цифрові валюти», «віртуальні валюти», а також «криптовалюти»). Виявлені ризики ВА та VASP включають: (i) анонімність; (ii) транскордонний характер операцій, (iii) відсутність однорідного регулювання у глобальному масштабі; та (iv) потреба в подальшому навчанні та підвищенні кваліфікації на тему ВА та VASP.

НОР також розглянула ризик крізь призму чинних міжнародних стандартів, включаючи Рекомендацію 15 FATF, пояснювальну записку до неї, зміст 5-ї AMLD, а також деякі інші аспекти.

Окремий розділ присвячений присутності ВА та VASP у Князівстві Андорра. Цей розділ охоплює не лише чинну законодавчу базу, а й вплив на інші сектори економіки. Також були розглянуті існуючі державно-приватні ініціативи з використанням технології блокчейн в Андоррі.

У висновку НОР було зроблено основні висновки, визначено ризики та заходи щодо їх зниження. Загальний рівень ВК, пов'язаний із сектором VASP в Андоррі, було визначено як високий.

Опитування показало, що оцінка ризиків на національному рівні починається з перевірки зареєстрованих суб'єктів у юрисдикції та з визначення суттєвості сектору VASP. Ця перевірка є простим процесом, коли VASP повинні мати ліцензію або бути зареєстрованими, а перед органами влади стоїть завдання оцінити, чи обслуговують ще незареєстровані організації клієнтів у відповідній юрисдикції та в якому обсязі. Однак на практиці юрисдикції стикаються з проблемами при виявленні незареєстрованої або неліцензованої діяльності VASP у своїй юрисдикції.

У тих випадках, коли реєстрація не вимагається, країни повинні покладатися на інформацію, внесену юридичними особами у комерційний реєстр щодо виду діяльності (або об'єкту діяльності), яку вони здійснюють. На основі цієї інформації органи влади застосовують фільтр для ідентифікації юридичних осіб, які пропонують послуги, пов'язані з ВА. Такий підхід є менш надійним для оцінки кількості VASP, які діють у країні, оскільки можуть виникнути помилки (ненавмисні) при декларуванні об'єкта діяльності або коли об'єкт діяльності надто широкий, щоб визначити точний вид діяльності, що надається певними операторами, які б могли кваліфікувати компанію як VASP.

Після першої перевірки VASP проводиться більш глибокий аналіз сектору, який зазвичай починається з розсилки опитувальника суб'єктам, зареєстрованим (ліцензованим) як VASP, або тим, хто потенційно може надавати послуги, схожі на VASP. Існує ризик того, що в результаті проведеної юрисдикцією роботи буде встановлено, що в країні не існує підприємств, які мають бути зареєстровані, тоді в такому випадку ВА та VASP випадуть з поля зору юрисдикції. Оцінка щодо використання ВА у країні має бути проведена навіть якщо не існує зареєстрованих VASP (наприклад, з'ясувати чи отримують клієнти національної юрисдикції послуги в іншій юрисдикції).

У разі виявлення підприємств, які підлягають реєстрації, різні установи всередині сектору можуть становити високий або низький ризик залежно від низки факторів, включаючи продукти, послуги, клієнтів, географічне положення, бізнес-моделі та міцність програми з комплаєнсу установи. При проведенні секторального стратегічного аналізу щодо VASP країнами було оцінено:

- скільки та які зареєстровані установи діють як оператори віртуальних валютних гаманців та пунктів обміну віртуальної валюти;
- хто є їх клієнтами: кількість фізичних та юридичних осіб; кількість громадян країни, громадян ЄС та третіх країн;
- скільки клієнтів VASP віднесено до клієнтів з високим ризиком (кількість та відсоток від загальної кількості клієнтів);
- сфера діяльності: вартість операцій, країна походження та призначення отриманих та надісланих коштів.

У більш розвинених юрисдикціях під час аналізу ризиків враховуються також результати наглядових заходів, наприклад рівень дотримання VASP вимог CDD для операцій, що перевищують 1000 євро. Фінансова розвідувальна інформація, отримана з STR, також є важливим джерелом інформації для визначення потенційних ризиків ВК/ФТ в секторі, де подаються відповідні STR пов'язані з ВА та VASP. Якщо говорити про менш позитивні моменти огляд показує, що надмірне використання технологій для виявлення STR негативно впливає на їх якість (див. розділ 6.1.2).

Кейс 2: Постачальники послуг віртуальних фінансових активів (VFASP), віртуальні фінансові активи та нові технології, що розвиваються – Мальта

У березні 2021 року Мальта розпочала оновлення національної оцінки ризиків. Прийнята методологія була зосереджена на конструктивних обговореннях у межах створених робочих груп та обговорень з представниками приватного сектору. Мета оновлення НОР полягала в тому, щоб отримати (у тому числі і в результаті обговорень у робочих групах) досить детальну оцінку реальних загроз і вразливостей, з якими стикаються різні сектори, що аналізуються.

Для оцінки загроз і вразливостей, пов'язаних з конкретним сектором або сферою діяльності, було створено різні робочі групи. Кожна робоча група складалася з тих органів влади, які мають найглибші знання у даному секторі, о один з них очолював групу. Цей процес було значно вдосконалено порівняно з процесом, що передував НОР 2018 року, і призвів до більш детальної та точної оцінки основних загроз, вразливостей і загальних ризиків, з якими стикається Мальта щодо ВК, ФТ та ФР. Однією з таких секторальних робочих груп, яку очолює Управління з фінансового регулювання та нагляду Мальти (MFSA), стала група по роботі з постачальниками послуг віртуальних фінансових активів (VFASPs), віртуальними фінансовими активами та новими технологіями, що розвиваються, до складу якої увійшли представники Підрозділу аналізу фінансової розвідки (FIAU), Бюро з повернення активів (ARB), Генеральної прокуратури (OAG), поліції Мальти (MPF), Національного координаційного комітету з протидії

відмиванню коштів та фінансуванню тероризму (NCC) та представницьких органів приватного сектора (постачальники послуг VFA (VFA – virtual financial assets) та агенти VFA).

Інформація, яка надійшла від наглядових органів, і яка зберігається у MFSA та FIAU, а також дані, які зберігаються у MPF, ARB та OAG, включають:

- Дані, зібрані MFSA під час процесу ліцензування, і наглядові дані, зібрані після видачі ліцензій.
- Дані, отримані з системи FIAU «Платформа з відповідності та нагляду для оцінки ризиків» (CASPAR)[6], і особливо з її секторальних опитувальників щодо оцінки ризиків.
- Дані, отримані в результаті наглядових та правозастосовних дій FIAU та MFSA.
- Більш детальні дані, доступні для відділу аналізу розвідувальних даних FIAU через систему goAML[7], про повідомлення про підозрілі операції (STR), які подаються суб'єктами до FIAU, у тому числі про їх якість та предикатні злочини, виявлені підзвітними установами, а також дані з запитів на інформацію, отриманих FIAU, незалежно від того, чи вони є внутрішніми чи міжнародними.
- Більш точні дані від OAG та MPF щодо запитів про взаємну правову допомогу, європейські слідчі ордери та міжнародну співпрацю.
- Типології STR та розслідування фінансових злочинів.
- Більш точні дані про вилучені активи, включаючи криптоактиви, заморожені та конфісковані з ARB

Аналіз ризиків у секторі VASPs часто доповнюється фактами та даними, зібраними з достовірних досліджень у сфері ВА, проведеих міжнародними організаціями. Тим не менш, на національному рівні аналіз секторальних ризиків значною мірою покладається на відповіді, які отримують органи влади від самого приватного сектору, при цьому дії для перевірки фактів з боку наглядового органу практично не вживаються.

Через залежність ВА та VASP від технологій, країнам важливо використовувати технології при виявленні та при оцінці ризиків у цьому секторі. Для кращого розуміння та зниження ризиків, деякі країни інвестували в інструменти оцінки ризиків блокчейну та навчили співробітників наглядових органів аналізу блокчейну. Загалом це виявилося ефективною практикою.

У більш просунутих ПО створено спеціалізовані підрозділи, які займаються мобільною, комп'ютерною і мережевою криміналістикою, а також розслідуванням блокчейн-технологій та ВА, вони оснащені технічними засобами оцінки та аналізу. Було залучено фахівців з розслідування та кримінального переслідування, пов'язаних з ВА.

Загалом більшість країн-членів провели оцінку ризику злочинного використання або ВА, або VASP з метою ВК, деякі також розглядали ризики ФТ. Однак, більшість цих оцінок, як видається, мають більш академічний характер і значною мірою спираються на джерела та інформацію з міжнародних звітів (включаючи звіти FATF).

[6] У березні 2019 року Відділ з нагляду FIAU у сфері ПВК/ФТ запровадив ефективне, стандартизоване технологічне рішення під назвою CASPAR для динамічної оцінки ризиків суб'єктів, збору даних про ризики та процесу оцінки ризиків. Система CASPAR використовує дані з різноманітних джерел (наприклад, надані підзвітними суб'єктами, наглядовими органами, засобами масової інформації, NRA/SNRA тощо), щоб забезпечити комплексну оцінку ризиків окремих підзвітних суб'єктів.

[7] goAML був представлений у 2020 році.

Юрисдикції MONEYVAL оцінювали ризики сектору VASP по-різному, не маючи єдиної думки про те, які фактори ризику або змінні були враховані. Одна з країн-членів MONEYVAL зазначила, що при оновленні оцінки ризиків VASP були додатково враховані ризики, що виникають у результаті: (i) діяльності з ВА (наприклад, використання токенів для залучення капіталу та роботи торгових платформ ВА); та (ii) діяльності або операції VASP. При оновленні було використано додаткові набори даних, які раніше були відсутні (наприклад, транскордонні операції, зв'язки з країнами, які мають стратегічні недоліки та дані щодо місця знаходження бенефіціарних власників).

Через обмеження, пов'язані зі збором даних, що наведені вище, складається враження, що більшість країн-членів мають обмежене уявлення про типи VASP, які діють на їхній території. Це стосується як іноземних зареєстрованих VASP, які надають послуги національним клієнтам, так і національних незареєстрованих чи неліцензованих VASP. Для поглибленої оцінки ризиків країнам-членам необхідно глибше розуміти сектор та його суттєвість.

5. Нагляд за VASP у країнах-членах Moneyval

У цьому розділі звіту описано різні підходи, які використовують країни-члени для ліцензування або реєстрації національних VASP, а також для впровадження ризик-орієнтовної системи нагляду для сектору VASP.

5.1 Різні типи ВА та VASP

Країни-члени MONEYVAL використовували різні підходи, коли вводили визначення термінів ВА та VASP у своє законодавство, що має каскадний вплив як на технічне дотримання вимог, так і на питання ефективності.

У Глосарії до Методології FATF віртуальні активи визначаються як цифрове вираження вартості, яке може бути предметом торгівлі або переказу у цифровому вигляді та може використовуватися для оплати або інвестиційних цілей. Віртуальні активи не включають цифрове вираження фіатних валют, цінних паперів та інших фінансових активів, які вже охоплені іншими розділами Рекомендацій FATF.

Постачальник послуг віртуальних активів (VASP) – це будь-яка фізична або юридична особа, яка в якості ділової діяльності здійснює одну або декілька з наведених нижче видів діяльності або операцій для іншої фізичної або юридичної особи, або від її імені: i) обмін між віртуальними активами та фіатними валютами; ii) обмін між однією або кількома формами віртуальних активів; iii) переказ[8] віртуальних активів; iv) зберігання та/або управління віртуальними активами або інструментами, що дозволяють контролювати віртуальні активи; та v) участь та надання фінансових послуг, пов'язаних із пропозицією емітента та/або продажем віртуального активу. Термін VASP не стосується конкретної технології, він може охоплювати криптовалютні підприємства, маркетплейси NFT, суб'єктів, що надають послуги ATM, кастодіанів гаманців та децентралізовані біржі.

Аналіз показує, що не всі країни-члени включили фізичних осіб у визначення VASP. У деяких країнах-членах VASP визнаються лише тоді, коли вони діють як юридичні особи, наприклад товариства з обмеженою відповідальністю. Інше обмеження визначення VASP пов'язане з типом послуг, які ці організації або особи можуть надавати. Найчастіше визначення VASP не поширюється на організації або осіб, які здійснюють обмін між однією або декількома формами віртуальних активів, передачу віртуальних активів та участь у фінансових послугах, пов'язаних із пропозицією емітента та/або продажем ВА, і наданням таких послуг.

Юрисдикції, які є країнами-членами ЄС або приводять своє законодавство у відповідність до нормативно-правової бази ЄС, вже перенесли 5AMLD. Охоплення VASP у 5AMLD не таке широке, як у Стандартах FATF. Насправді 5AMLD не охоплює участь та надання послуг, пов'язаних із емісією монет, надання послуг переказу ВА та послуг з обміну між ВА. Проте, деякі країни-члени ЄС і країни, які не входять до ЄС, вирішили вийти за рамки вимог Директиви , визначивши додатковий вид послуг.

[8] У цьому контексті віртуальних активів, переказ означає проведення операції від імені іншої фізичної або юридичної особи, яка переміщує віртуальний актив з однієї адреси або рахунку віртуального активу на іншу адресу або рахунок.

Існують рідкісні випадки, коли країни-члени виходять за рамки стандартів FATF, даючи ширші визначення, які охоплюють навіть однорангові операції. Однак поки що неясно, як це буде реалізовано на практиці.

5.2 Нормативно-правова база

Одним із заходів щодо зниження ризику для діяльності VASP є застосування у цьому секторі заходів контролю за виходом на ринок і відповідного ризик-орієнтованого нагляду з метою ПВК/ФТ. Відповідно до зібраної інформації, більшість країн-членів мають нормативно-правову базу для регулювання ВА та VASP. Одна із країн-учасниць MONEYVAL заборонила будь-які операції з ВА у своїй юрисдикції.

5.2.1. Порядок ліцензування або реєстрації

15 Рекомендація FATF дозволяє країнам вибирати між ліцензуванням або реєстрацією VASP, за умови, що, як мінімум, VASP повинні мати ліцензію або реєструватися в юрисдикції(юрисдикціях), де вони створені. У випадках, коли VASP є фізичною особою, він повинен мати ліцензію або реєструватися у юрисдикції, де розташоване місце його діяльності. Для виконання цієї вимоги, більшість країн-членів MONEYVAL запровадили певну форму ліцензування, реєстрації або повідомлення для VASP. Однак ці режими відрізняються один від одного. Наприклад, деякі країни застосовують вимоги реєстрації до всіх осіб (фізичних і юридичних), які ведуть діяльність VASP на комерційній основі в межах своєї юрисдикції, за винятком тих, хто вже зареєстрований як VASP в інших державах-членах ЄЕЗ.

Суворість реєстраційних або ліцензійних вимог і тип режиму ґрунтується на оцінці різних видів діяльності ВА та VASP та ризиків ВК/ФТ, яким вони піддаються.

У деяких юрисдикціях режим ліцензування вимагає, щоб VASP були зареєстровані, а не ліцензовані в цілях ПВК/ФТ. Встановлені FATF реєстраційні вимоги можуть спричинити різні проблеми. У той час як деякі наголосили на труднощах з реєстрацією або ліцензуванням через характер послуг, що надаються, інші повідомляли, що зареєстровані VASP вважають відсутність механізму ліцензування перешкодою для надання послуг.

Різниця між реєстрацією з метою нагляду в контексті ПВК/ФТ та отриманням ліцензії може мати істотний вплив на запобігання злочинам та управління сектором. Деякі країни-члени повідомили, що простої реєстрації недостатньо, оскільки менш авторитетні фірми використовують реєстрацію як знак законності, а їхні клієнти рідко розуміють різницю між реєстрацією та регулюванням. Без режиму ліцензування важко довести законність підприємства, особливо якщо підприємство також передбачає надання послуг за кордоном.

У деяких юрисдикціях є закони, що регулюють використання певних технологій. Наприклад, в одній з країн-членів існує поділ між постачальниками технології розподіленої мережі (DLT) та іншими видами діяльності VASP. Існують різні режими регулювання для DLT-провайдерів, уповноважених і контрольованих одним регулюючим органом та інші вимоги для інших видів діяльності VASP.

Недоліки, які досить часто зустрічаються у країнах-членах MONEYVAL, стосуються сфери застосування, наприклад, режими ліцензування або реєстрації не поширюються на

фізичних осіб, які діють як VASP, а лише на юридичних осіб або вони охоплюють не усі види юридичних осіб.

В інших країнах іноземні VASP, які надають послуги в юрисдикції, повинні створити місцеву юридичну особу, щоб контролювати використання іноземних VASP. Проте, як це працює на практиці, невідомо, оскільки, без впровадження більш широкодоступного Інтернету, регулювання було б практично неможливим.

Країни також обмежили можливість для фізичних осіб бути зареєстрованими або отримати ліцензію як VASP через міркування ризику. Якщо фізичним особам заборонено пропонувати послуги, пов'язані з ВА, вони вважаються такими, що не підпадають під ризик-апетит країни.

Розглядаючи процес ліцензування або реєстрації, необхідно вживати необхідних законодавчих або регулятивних заходів, щоб запобігти тому, щоб злочинці або їхні спільники володіли або були бенефіціарними власниками істотної або контролюючої частки чи обіймали керівні посади у VASP. Регулювання виходу на ринкок у країнах-членах MONEYVAL здійснюється по-різному: в одних ці вимоги встановлені, в інших - відсутні. У ході аналізу було виявлено, що вимоги щодо дотримання відповідності та належності іноді виконуються лише частково, коли перевірки охоплюють лише злочини, пов'язані з торгівлею або сферою торгівлі.

У деяких країнах-членах MONEYVAL ВА використовуються для ігрових цілей, наприклад для ставок на спорт/ кіберспорту / азартних ігор. У таких випадках країни-члени намагаються включити спеціальні засоби контролю з ПВК/ФТ, щоб обмежити потенційне зловживання ВА в ігровій сфері. Приклади спеціальних засобів контролю включають: (i) використання лише дозволених моделей ВА, які зберігають платіжний канал для внесення та зняття коштів (ii) вимоги про те, щоб внесення та зняття коштів здійснювалися в одному номіналі, (iii) встановлення порогових значень транзакцій для зняття або внесення та (iv) вимоги використання інструментів аналізу блокчейну для виявлення червоних прапорців високого ризику, з акцентом на схильність до незаконних джерел, кількості переходів із незаконних джерел, використання міксерів, chain hopping (метод ВК, який передбачає часту і швидку зміну криптовалюти для того аби заплутати можливе відстеження коштів, часто із використанням «приватних монет»), блокчейнів з підвищеною анонімністю тощо.

Кейс 3: Ліцензування азартних ігор в Інтернеті – острів Мен

Комісія з нагляду за азартними іграми острова Мен (GSC) здійснює ліцензування та регулює азартні ігри, у тому числі у разі використання ВА. Усі особи, які подають заявки на отримання ліцензії проходять однакові перевірки при подачі заявки на отримання ліцензії незалежно від того, чи використовують вони фіатні валюти, чи ВА, або й те, й інше, включаючи розуміння та ретельне вивчення бенефіціарної власності, проведення належної перевірки власників та контролерів, проведення перевірки джерела статків і посилену належну перевірку, де це необхідно.

Фінансові дані та плани діяльності ретельно перевіряються, з приділенням більшої уваги моделям, які включають використання ВА, у пошуку гарантій щодо використовуваної технології; розуміння ризиків ВК/ФТ під час використання ВА, а також відповідності моделей політиці посиленого контролю та допустимим моделям внесення коштів. На веб-сайті GSC опубліковано додаткові керівні настанови щодо ПВК/ФТ для користувачів ВА,

а для будь-якого власника ліцензії, який використовує ВА, додається умова ліцензії, щоб забезпечити дотримання політики GSC щодо використання ВА.

Усі власники ліцензій, які надають послуги клієнтам, мають вимоги щодо внутрішнього контролю ПВК/ФТ. На додаток до цих заходів контролю, власник ліцензії, який використовує ВА, також повинен вживати додаткові спеціальні заходи контролю, наприклад: використовувати лише дозволені моделі використання ВА, які зберігають платіжний канал для внесення і зняття коштів (тобто не допускається змішування або обмін різних типів криптовалют; або обмін криптовалюти на фіатну валюту), а також порогові значення для CDD і EDD.

Власники ліцензій проводять самооцінку всіх перелічених вище заходів ПВК/ФТ, включаючи додаткові вимоги до використання ВА. Це дозволяє оцінити їх технічну відповідність. Для оцінки ефективності заходів контролю разом із невиїзними перевірками проводяться виїзні перевірки. Для визначення частоти та типу перевірок використовується ризик-орієнтований підхід. Використання ВА є фактором ризику, який додається до оцінки ризиків власників ліцензій, і вони оновлюються щокварталу.

Під час виїзної перевіри проводиться вибіркова перевірка клієнтів, які використовують ВА, включаючи статус ризику клієнтів, моніторинг, транзакції, довічні депозити, способи внесення коштів та діяльність. Перевірки проводяться на відповідність політиці, умовам ліцензії та керівним настановам.

5.3 Нагляд та моніторинг за ПВК/ФТ

5.3.1. Призначення наглядового органу

Рекомендації FATF надають державним органам широкі можливості для свободи вибору моделі нагляду, яка їм найбільше підходить, беручи до уваги ризик і суттєвість сектору VASP, а також особливості інституційної структури органів державної влади. Країни-члени MONEYVAL застосовують різні підходи до нагляду, а це означає, що орган ліцензування або реєстрації не завжди є тим самим органом, який здійснює нагляд у сфері ПВК/ФТ за VASP. Незалежно від того, який підхід застосовує юрисдикція, у випадку нагляду VASP, він має бути ефективним у нагляді за сектором і мінімізовувати ризики ВК/ФТ.

Кейс 4: Реєстрація VASP з боку FMA – Ліхтенштейн

Управління з регулювання фінансового ринку (FMA) є компетентним органом з видачі, внесення змін та відкликання ліцензій для ФУ, TCSP та VASP. За реєстрацію VASP відповідає Виконавча служба (Група лабораторії регулювання/фінансових інновацій).

Перед реєстрацією «концепція» належної перевірки VASP, яка потребує ліцензування, має бути перевірена зовнішнім аудитором, а під час процесу реєстрації FMA збирає детальну інформацію про впровадження превентивних заходів.

Протягом першого року після реєстрації проводиться стандартна перевірка (виїзна перевірка) ліцензованих VASP. FMA має повноваження видавати накази, вказівки та рекомендації для цього сектору.

5.3.2. Повноваження наглядових органів щодо належного моніторингу сектора та ресурсів

Країни-члени MONEYVAL по-різному виконують зобов'язання щодо нагляду та моніторингу. Деякі юрисдикції вирішили застосувати до VASP ті ж самі зобов'язання з ПВК/ФТ, що і для ФУ та ВНУП, з тими самими повноваженнями щодо виконання наглядових функцій, які здійснюються по відношенню до VASP. Таким чином, будь-який новий потенційний VASP підлягатиме тим же ризик-орієнтованим моделі нагляду та інструментам, як й інші підзвітні суб'єкти.

Кейс 5: Повноваження Комісії з фінансових послуг, яка здійснює нагляд за VASP – Гібралтар

Комісія з фінансових послуг є органом, відповідальним за видачу ліцензій та нагляд за VASP, що діють на території Гібралтару, і має такі повноваження:

1) проводити виїзні перевірки;

2) вживати превентивних та коригувальних заходів для забезпечення дотримання вимог;

3) вимагати подання усієї інформації, необхідної для здійснення ефективного нагляду;

4) вимагати подання облікової звітності, інформації та виготовлення документів тощо;

5) вимагати надання звіту кваліфікованих кадрів;

6) вимагати призначення інспекторів;

7) накладати фінансові та адміністративні штрафи;

8) призупиняти або відкликати ліцензію/дозвіл/реєстрацію;

9) тимчасово забороняти обіймати керівні/регульовані посади;

10) видавати розпорядження; та

11) вживати заходи щодо юридичних або фізичних осіб.

Загалом, розглядаючи наглядовий підхід до сектору VASP, більшість країн-членів MONEYVAL тільки починають впровадження. У зв'язку з нещодавніми правилами регулювання з ПВК/ФТ щодо VASP, виявилось, що не всі наглядові органи мають достатньо ресурсів (персоналу та знань).

Аналіз показав цікаву тенденцію на рівні наглядових органів: IT-персонал стає наглядовим персоналом, щоб допомагати в проведенні ефективного нагляду за цим технологічно залежним сектором. У деяких випадках така ж тенденція була помічена на рівні приватного сектору, де IT-фахівці стали відповідальними за комплаєнс і потребують підвищення рівня своїх знань щодо ПВК/ФТ, щоб виконувати зобов'язання та керувати ризиками.

5.3.3. Застосування ризик-орієнтованого підходу до нагляду за VASP

У випадку нагляду, РОП застосовується до того, як наглядові органи розподіляють свої ресурси. Серед країн-членів MONEYVAL, які імплементували нагляд для VASP, не всі запровадили комплексний РОП. РОП не часто використовується в оцінці ризиків у певному секторі, при цьому більшість членів покладаються на висновки більш високого рівня у НОР.

Коли ризик-орієнтований нагляд, покладається на НОР, відповіді на опитувальник показують деякі обмеження, наприклад, країни не розглядають поточний розвиток ВА та VASP. Це негативно впливає на застосування ефективного РОП до нагляду.

У разі ефективного проведення, оцінка ризиків у секторі має бути детальною, та враховувати не лише ризик у секторі VASP загалом, а й ризики на рівні установ. Розглядаючи окремі VASP або конкретні продукти, послуги чи види діяльності з ВА, досвідчені наглядові органи беруть до уваги рівень ризику, пов'язаного з продуктами та послугами VASP, бізнес-моделями, механізмами корпоративного управління, фінансовою та бухгалтерською інформацією, каналами постачання, профілями клієнтів, географічним розташуванням, країною діяльності, рівнем відповідності VASP заходам з ПВК/ФТ, а також ризиків, пов'язаних з окремими продуктами ВА, які підривають прозорість.

Кейс 6. Оцінка ризиків наглядового органу (сектору віртуальних фінансових активів) – Мальта

Наглядовий орган Мальти у сфері ПВК/ФТ, Підрозділ аналізу фінансової розвідки (FIAU), використовує автоматизований інструмент для оцінки ризиків підзвітних установ, за якими він здійснює нагляд. Оцінки ризиків використовуються для різних цілей: у тому числі для визначення річних і багаторічних планів нагляду, для того, щоб уможливити вибір суб'єктів, які піддаються певним ризикам, під час проведення тематичних перевірок, а також для сприяння національним процесам оцінки ризиків.

Оцінка ризиків здійснюється на основі семи основних джерел інформації:

(i) Опитувальники щодо оцінки ризиків ПВК/ФТ (REQ) – це основне джерело інформації про ризики, яка збирається від кожного VASP. Отримується інформація про притаманні ризики та рівень контролю (див. таблицю нижче). Опитувальники розробляються один раз на рік для окремих секторів, зокрема для сектору VASP. У разі неподання такої анкети застосовуються правозастосовні заходи. FIAU також прагне підтвердити інформацію анкети шляхом перехресного порівняння відповідей на різні пов'язані запитання та шляхом порівняння з даними, отриманими під час наглядових перевірок.

(ii) Інформація пруденційного регулятора – Пруденційний регулятор сектору VASP (Управління фінансових послуг Мальти) подає щорічний опитувальник, в якому висвітлюється, чи підлягали певні VASP загальним пруденційним заходам контролю, що були викликані будь-якими занепокоєннями.

(iii) Інформація від ПФР – Департамент фінансової розвідки FIAU щорічно надає інформацію за допомогою опитувальника відділу нагляду тієї самої організації. Ця анкета містить інформацію про кількість та якість STR, поданих кожним VFA.

(iv) Історія нагляду та правозастосування – проблеми та порушення, виявлені під час попередніх наглядових перевірок з ПВК/ФТ. Їх ідентифікують шляхом складання та збору опитувальників після дослідження та інших анкет, заповнених відділом правозастосування, що містять дані про накладені санкції.

(v) SNRA – Ризики сектору VASP, визначені в SNRA ЄС, беруться до уваги для визначення ризику окремих суб'єктів у цьому секторі.

(vi) НОР – аналогічним чином розглядаються ризики, виявлені в НОР.

(vii) Негативна інформація – будь-яка несприятлива інформація, виявлена через публічні чи інші джерела, оцінюється та, якщо це вважається доречним, береться до уваги під час розрахунку ризику окремої організації. Це дозволяє постійно змінювати рейтинг ризику окремих суб'єктів.

Кожному фактору притаманного ризику та контролю в кожному блоці присвоєно певну вагу. Вони збільшують, або зменшують ризик. Ці вагові коефіцієнти калібрувались протягом багатьох років з моменту початку використання системи CASPAR (тобто з 2019 року). Інструмент CASPAR, заснований на цій системі зважування, встановлює оцінку ризику кожному VFA та іншим підзвітним суб'єктам. Ця класифікація потім допомагає сформулювати річні та багаторічні плани, щоб гарантувати, що перевірки VFA відповідають ризику, який вони представляють. За наведеним нижче посиланням можна отримати додаткову інформацію про конкретні дані, які збираються за допомогою щорічного опитувальника для VASP (https://fiaumalta.org/caspar-login/#el-fcfb5f8b).

5.3.4. Виявлення транскордонних потоків

Обсяг і потік транскордонних транзакцій є одним з важливих елементів, який органи нагляду повинні враховувати під час визначення ризику сектору VASP та здійснення наглядової діяльності. Хорошою практикою для наглядового органу є запитувати таку інформацію в секторі, яка може бути використана для формування наглядового підходу та розуміння ризиків.

Аналіз виявив принаймні одну країну-члена, яка збирає дані про вхідні та вихідні транзакції з іншими юрисдикціями. Усі регульовані організації, включаючи DLT-провайдерів/VASP, зобов'язані щорічно подавати цю інформацію наглядовому органу. Після цього кожне повідомлення перевіряється групою нагляду з ПВК/ФТ. Будь-які потенційні червоні прапорці або порушення потім, або запитуються у відповідної підзвітної установи, або використовуються для інформування поточного нагляду за установою.

Аналіз транскордонних потоків також може допомогти визначити, чи існують у вітчизняних VASP іноземні клієнти. Наприклад, згідно з інформацією, наданою одним зареєстрованим VASP своєму наглядовому органу, приблизно 9700 клієнтів (тобто 66%) були місцевими. Іноземні клієнти були переважно з інших країн ЄС та сусідніх країн. Більшість зареєстрованих VASP повідомили, що вони не мали клієнтів, які є PEP, не мали

клієнтів із високоризикових країн, не здійснювали операції, пов'язані з високоризикованими країнами, і не здійснювали операції готівкою. Хоча ці опитування є важливим кроком для оцінки та розуміння діяльності, профілів і ризиків VASP, відсутність перевірок знижує надійність даних. У випадку з Bitcoin, незважаючи на певні успіхи у визначенні гаманців і адрес, важко надійно ідентифікувати країну кожної транзакції, тим більше, коли докладаються зусилля, щоб цілеспрямовано приховати пункт призначення.

Щоб розвинути глибоке розуміння ринку VASP, його структури і ролі у фінансовій системі та економіці країни, наглядові органи інвестують у навчання, персонал або інші ресурси, які дозволяють їм отримати практичні навички та досвід, необхідні для регулювання та нагляду за постачальниками ВА. Деякі країни-члени MONEYVAL співпрацюють з експертами інших секторів та використовують постачальників інструментів блокчейн-аналітики для забезпечення значного рівня навчання, інші створюють спеціальні підрозділи для управління цією сферою. Менші юрисдикції розглядають можливість передачі розслідувань і аналізу ризиків стороннім постачальникам експертних послуг.

5.3.5. Санкції

Можливість накладання санкцій наглядовими органами VASP у країнах-членах MONEYVAL відрізняються за обсягом і сумою, які можуть бути застосовані. Таким чином, не всі члени можуть накласти широкий спектр переконливих та ефективних санкцій на сектор VASP.

У деяких випадках, навіть якщо наглядовий орган VASP має необхідні повноваження накладати санкції за недотримання вимог, повний їх спектр не завжди доступний. Хоча грошові санкції можуть бути переконливими, часто інші покарання в наборі інструментів нагляду відсутні, наприклад можливості обмежити або призупинити ліцензію VASP.

В інших юрисдикціях можливість штрафувати незареєстрованих VASP, або несанкціоновану діяльність VASP та недотримання вимог з ПВК/ФТ входить до повноважень наглядового органу або ПО. Кримінальні та адміністративні суди також можуть заборонити діяльність, на яку подаються скарги. Санкції можуть стосуватися як фізичних осіб, які займаються несанкціонованим бізнесом, так і юридичних осіб, які здійснюють діяльність VASP. Один із прикладів правозастосовних дій щодо VASP за порушення вимог з ПВК/ФТ описано у Кейсі 7.

При роботі з незареєстрованими VASP виникає питання, як їх виявити на практиці. На практиці виявлення незареєстрованих VASP вимагає навчання на всіх рівнях, ПО потребують навчання для виявлення використання незареєстрованих VASP шляхом розслідування предикатних злочинів і паралельних розслідувань відмивання коштів. Традиційним фінансовим організаціям потрібна освіта та рекомендації, щоб визначити потік фіатної валюти в такі VASP.

Кейс 7: Правозастосовні дії – FIAU Мальта

Підрозділ аналізу фінансової розвідки (FIAU) є мальтійським органом, відповідальним за моніторинг і виконання зобов'язань щодо ПВК/ФТ. Це також ПФР Мальти. VASP регулюються в цілях ПВК/ФТ на Мальті з 2018 року.

У 2023 році FIAU наклала штраф у розмірі 463 235 євро на двох VASP, що входили до однієї групи, які надавали численні послуги ВА, включаючи послуги обміну. Цей

правозастосовний захід став результатом наглядової перевірки, проведеної у 2022 році, яка виявила порушення наступних зобов'язань щодо ПВК/ФТ:

(i) Оцінка бізнес-ризику (BRA) – BRA не підходила для виявлення та оцінки ризиків, на які наражалася організація, і не врахувала ризики, пов'язані з використанням VPN, проксі-серверів, міксерів і тумблерів. BRA також була неповною, оскільки вона не проаналізувала сценарії ризику, ймовірність їх реалізації та кінцевий вплив. Чиновники також звернули увагу на те, що BRA була розроблена безпосередньо перед перевіркою і, навіть, не була прийнята керівництвом підприємства.

(ii) Оцінка ризику клієнта (CRA) – під час перевірки установа представила документ із рейтингом ризику, що стосується клієнтів, обраних для перевірки. Не було надано жодних пояснень чи обґрунтувань цих рейтингів. Групі з оцінки також було надано дві різні методології CRA, які не враховували ризик клієнтів, ризики продукту/послуги та ризики інтерфейсу, а аналіз ризику клієнтів базувався на національності та адресі проживання. Юрисдикційний ризик також був недостатнім через неврахування важливих джерел інформації, наприклад індексу сприйняття корупції та списку ЄС юрисдикцій з високим ризиком. У кількох файлах було зазначено недоліки в оцінці ризиків для конкретних клієнтів, що вказувало на системну проблему

(iii) Зобов'язання з CDD – (a) Майже для половини клієнтів не було проведено жодної перевірки особи.

(b) VASP не збирав інформацію про адресу, з якої клієнти отримували або надсилали BA, і не міг визначити, чи був гаманець, який використовувався, приватним, з мультипідписом чи кастодіальним. FIAU очікує від VASP збору інформації про гаманці.

(c) Щодо більш ніж третини своїх клієнтів VASP не зміг зібрати адекватну інформацію про джерело їхнього багатства та очікуваний рівень і характер діяльності, щоб створити відповідний профіль в цілях поточного моніторингу. FIAU також звернула увагу на той факт, що не було фактичних лімітів транзакцій, які могли б пом'якшити транзакційні ризики в таких випадках.

(d) Було відмічено декілька недоліків поточного моніторингу. VASP заявив, що відстежував транзакції на суму понад 10 000 євро за допомогою інструменту блокчейн-аналітики. Враховуючи обсяг транзакцій, що обробляються, і легкість, з якою такі транзакції обробляються, цей підхід не вважався належним. Крім того, така система моніторингу мала включати не лише моніторинг після транзакцій, але й моніторинг у режимі реального часу для ситуацій високого ризику, таких як транзакції на великі суми. Працівники FIAU також виявили транзакції, включно з одною на 1 000 000 доларів США, для яких не було зібрано жодної інформації про мету та джерело коштів.

(iv) Зобов'язання з EDD – FIAU також визначила низку випадків, коли мала бути проведена EDD, але не була здійснений, наприклад, стосовно клієнтів, які проживають у юрисдикціях з високим ризиком, і клієнта, який отримував кошти, що описувалися як позики (включаючи одну трансакцію на 29,4 BTC – понад 1 000 000 євро), для яких не було отримано жодної додаткової інформації чи підтверджуючих документів. Як правило, у таких випадках FIAU, окрім накладення санкцій, вимагає від клієнта вжити заходів для виправлення ситуації. Однак у цьому випадку VASP подала заяву про відмову від своєї ліцензії, і, отже, жодної директиви про вжиття заходів не було видано.

Стосовно того, хто є відповідальним органом для виявлення незареєстрованої/неліцензованої діяльності, аналіз показав, що хоча в одних країнах це завдання чітко покладено на окремий орган (як правило, наглядовий), в інших воно є більш розмитим, і одні органи влади очікують дій з боку «інших». Типовою є ситуація, коли за відсутності конкретних процедур і повноважень наглядові органи прирівнюють незареєстрованих VASP до форм незаконної діяльності та очікують, що поліція (або інший ПО) буде вживати заходів проти них, тоді як ПО не відчувають відповідальності (або не мають обізнаності) і очікують, що наглядовий орган буде вживати заходів.

6. Правоохоронні органи та VASP – Окремі світи?

У цій главі розглядаються можливості та підходи органів влади в країнах-членах MONEYVAL до розслідування випадків ВК/ФТ пов'язаних з ВА, та застосування тимчасових запобіжних заходів.

Розслідування, пов'язані з використанням ВА, викликають кілька проблем, які висвітлюються в цьому звіті. Такі виклики та перешкоди включають: (i) відсутність знань і досвіду щодо того, як проводити аналіз та розслідування ВА; (ii) відсутність юридичної визначеності щодо того, чи застосовуються певні слідчі/тимчасові запобіжні заходи щодо ВА; (iii) відсутність або невідповідність інструментів для ефективного аналізу/розслідування транзакцій з ВА; (iv) неефективне міжнародне співробітництво, яке перешкоджає своєчасному замороженню, вилученню та конфіскації ВА у міжнародних справах; (v) труднощі із застосуванням аналітичних та дослідницьких інструментів щодо нерегульованих VASP.

Тим не менш, технологія, що стоїть за ВА (тобто блокчейн) також має деякі позитивні риси. Інформація (включаючи дані транзакцій), записана в блокчейні, є незмінною та особливо корисною для слідчих, що стежать за грошима. Однак це вимагає розгортання відповідних інструментів (таких як інструменти блокчейн-аналізу), які дозволили б слідчим слідкувати за віртуальними валютами.

Ефективне регулювання VASP також відіграє фундаментальну роль у здатності міжнародного співтовариства протистояти фінансовим злочинам через зловживання VASP. Це пояснюється тим, що регульовані та контрольовані VASP є корисним джерелом інформації, яке може значно допомогти у проведенні розслідувань і відстеженні ВА. Певною мірою цьому кидає виклик поява децентралізації у сфері ВА. Це пов'язано з тим, що децентралізовані моделі не передбачають центрального посередника, який може регулюватися та виступати в якості сполучної ланки з ПО. Швидкий розвиток сектору ВА також вимагає постійного навчання та підвищення кваліфікації ПО, щоб постійно отримувати знання про те, як проводити розслідування з ВА та VASP.

6.1 Повідомлення про Підозрілі Операції з Боку VASP щодо ВА

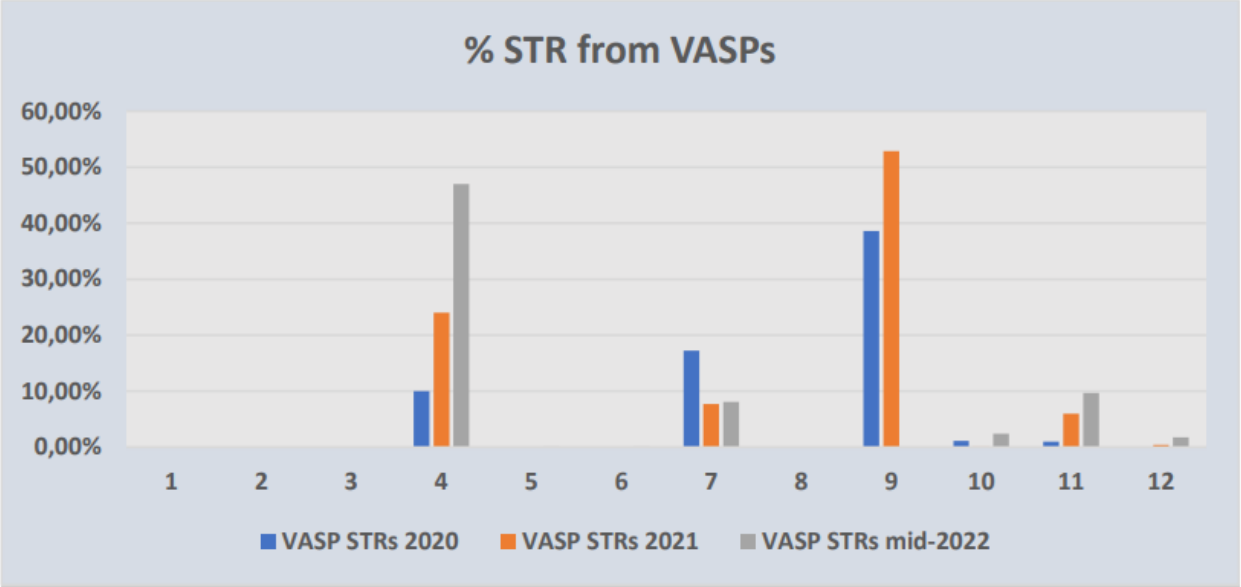
SAR або STR, отримані ПФР, є важливим джерелом розвідувальних даних для виявлення випадків ВК/ФТ. Команда проекту оцінила наявність розвідувальних даних в підозрах пов'язаних з ВА, які надходять через STR. Для висновків були використані дані про загальну кількість STR надісланих VASP у період з 2020 по 2022 рік, надані 12 країнами-членами. Якісні дані щодо змісту отриманих STR також доповнюють опитування.

6.1.1. Обсяг STR, поданих VASP

Відзначається ряд спостережень. З 12 країн-членів, які надали дані про STR, чотири отримали досить значний обсяг STR від VASP, тоді як решта отримують дуже незначну кількість або взагалі не отримують. Очевидно, що ті країни-члени, які намагалися регулювати та контролювати VASP, спонукали до більшої кількості звітів від сектора VASP. На Рисунку 12 представлено відсоток STR, отриманих від VASP, із загального

обсягу STR протягом 2020-2022 років для 12 країн-членів MONEYVAL, які брали участь у цьому аналізі.

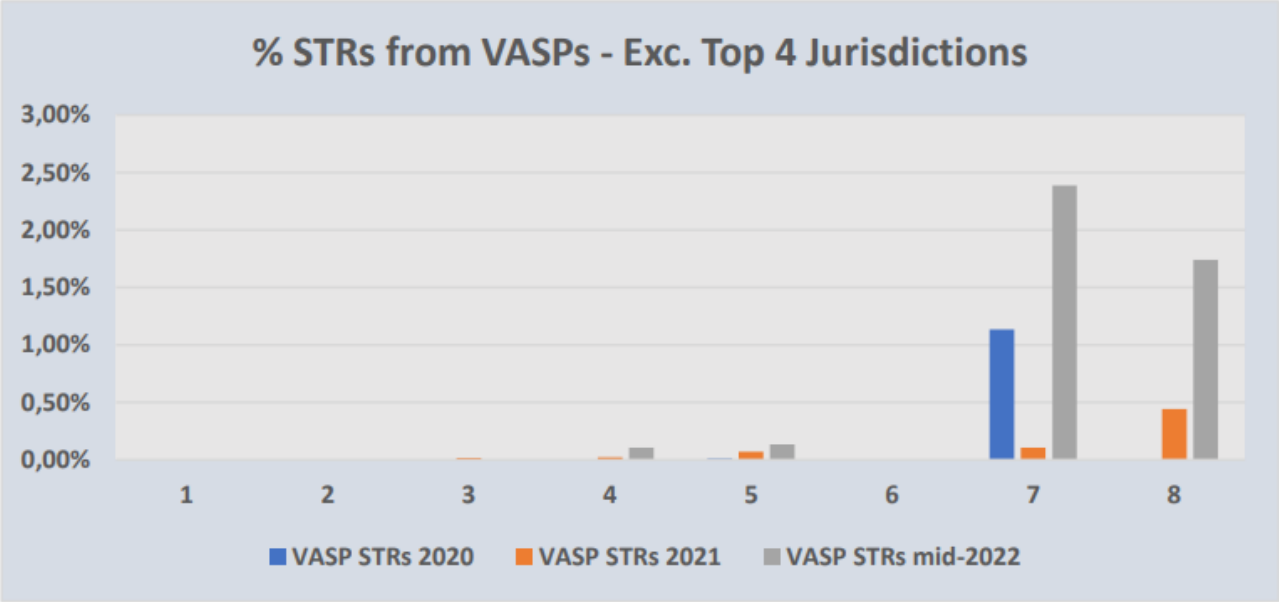
Рисунок 12 – STR, подані VASP



Деякі респонденти відчули збільшення кількості STR, надісланих VASP, порівнюючи 2020 рік з 2022 роком (кінець червня).

Більшість членів-респондентів (шість) отримували менше 1% STR від VASP протягом 2020-2022 років (період на кінець червня), причому три з цих юрисдикцій вказали, що вони ніколи не отримували жодних STR від VASP. Двоє респондентів отримали 2,4% і 1,7% від усіх своїх STR у 2022 році (до середини червня) від VASP. На Рисунку 13 наведено статистичні дані щодо обсягу STR, отримані іншими юрисдикціями, окрім чотирьох найкращих за показниками звітності.

Рисунок 13 – STR, подані VASP (за виключенням 4 топ-юрисдикцій)



Існує припущення, що ВА фігурують у більшій кількості STR, ніж ті, що надходять лише від VASP, і цілком можливо, що справжнє зловживання ВА та VASP можна буде ідентифікувати за допомогою зовнішніх ФУ, однак дані для спостереження не вдалося отримати. Це свідчить про те, що значна кількість ПФР серед респондентів все ще стикається з проблемами отримання та реєстрації статистичної інформації.

Одним із вражаючих факторів при аналізі обсягу STR є те, що в більшості випадків STR від сектору VASP надходять від обмеженої кількості операторів. Наприклад, в одній країні один постачальник послуг (тобто біржа) склав 96% усіх STR від VASP у 2022 році, тоді як в іншій країні один VASP склав 95% загального обсягу STR від сектора в 2021 році. В обох випадках це великі VASP, які займають значну частку ринку за обсягами клієнтів.

6.1.2. Якість STR, наданих VASP

Огляд якості STR в юрисдикціях, де кількість STR, поданих VASP, є значно вищою (тобто 4 топ-юрисдикції), показує занепокоєння щодо загальної якості STR. Країни виділили кілька проблем, які впливають на якість STR від VASP, а саме:

(i) STR автоматично генеруються технологічними інструментами, що використовуються для керування загальною діяльністю VASP, і рідко мають високу якість. Ці інструменти ідентифікують «підозрілі» гаманці та адреси, оскільки вони можуть бути пов'язані з іншими адресами гаманців, які позначені з огляду на несприятливу інформацію, що пов'язує їх із злочинністю. Але іноді, цей зв'язок видимий за декілька кроків далі в ланцюжку транзакцій, що робить його дуже віддаленим. Ці інструменти є корисним джерелом для виявлення сумнівних адрес гаманців, однак вони не можуть замінити виявлення підозр за допомогою аналізу, та виявлення ознак і типологій (зокрема, коли немає поточного зв'язку зі злочинністю). Останній підхід дає більш корисну фінансову розвідувальну інформацію. Практики вважають, що втручання досвідченої людини-оператора у вибір відповідних STR було б корисним, навіть якщо це означало б зменшення кількості STR.

(ii) Також очевидно, що «захисне звітування» становить значну частину цих STR. Повідомляється про численні випадки подання STR через неможливість проведення CDD. Іноді такі STR не стосуються ніяких активів чи операцій.

(iii) VASP передають свої зобов'язання CDD, включно з моніторингом транзакцій, на аутсорсинг, що не сприяє накопиченню досвіду виявлення підозрілих операцій. Деякі країни забороняють передачу зобов'язань щодо ПВК/ФТ або особливих зобов'язань, таких як моніторинг транзакцій та аналіз підозр на аутсорсинг, з метою пом'якшення цієї проблеми.

(iv) Відзначено феномен «перетворення IT на комплаєнс» у приватному секторі (VASP). Це означає, що відповідна команда з комплаєнсу, в той час як володіє знаннями про технологію блокчейну та інструменти, пов'язані з ВА, не має базового розуміння питань з ПВК/ФТ.

(v) VASP, які працюють більш ніж в одній країні, часом важко визначити, куди повідомити про підозру, оскільки важко встановити юрисдикційний зв'язок конкретної транзакції, що призводить або до кількох звітів, або до неправильного звітування.

Країни наголосили на важливості інформаційно-роз'яснювальної роботи та інвестицій у розбудову потенціалу VASP, щоб допомогти їм виявляти та створювати більш якісні STR. Цього можна досягти шляхом: (i) формулювання та поширення інформації про тенденції та

типології ВК/ФТ, пов'язані з VASP та ВА; (ii) постійного збору даних та статистики щодо якості STR та обміну інформацією для подолання прогалин; (iii) проведення неформальних дискусій з операторами VASP, які могли б надати можливість ПФР та наглядовим органам отримати більше знань про операції VASP, водночас передаючи працівникам VASP досвід щодо виявлення підозрілих транзакцій.

6.1.3. Основні предикатні злочини

Дві країни-учасниці, які беруть участь у цьому проекті, надали дані про тенденції та типології, які вони визначили за допомогою STR, отриманих від VASP. Аналізуючи дані щодо заявлених основних предикатних правопорушень, було відзначено деякі спільні тенденції.

Шахрайство з інвестиціями в одній країні вважається найпоширенішим предикатним злочином, а в іншій — займає друге місце. Як правило, у таких випадках, клієнтів VASP обманом змушують передати ВА третім особам, які зазвичай обіцяють їм чудові інвестиційні можливості, що часто призводить до повної втрати активів. Соціальна інженерія також використовується для отримання адрес електронної пошти, через які шахраї намагаються отримати доступ до гаманців і криптоактивів.

Сексуальна експлуатація дітей була найпоширенішим предикатним злочином в одній із цих країн. Більшість випадків, пов'язаних із сексуальною експлуатацією дітей, включають передачу ВА (використовуючи гаманці VASP) на інші гаманці, які прямо чи опосередковано пов'язані з гаманцями, що фігурують в справах про жорстоке поводження з дітьми. Використовуючи інструменти аналізу блокчейнів, VASP можуть ідентифікувати такі зв'язки, що призводить до подання звітів на підставі підозрілих зв'язків із сексуальною експлуатацією дітей.

Зазначається, що одна країна-член повідомила про використання ВА для обходу цільових фінансових санкцій. Глобальний характер ВА незмінно означає, що цей сектор також приваблює клієнтів з юрисдикцій із підвищеним ризиком і, потенційно, може відбутися контакт із суб'єктами та/або юрисдикціями, щодо яких поширюються санкції. Ймовірно, що підсанкційні суб'єкти будуть досліджувати альтернативні методи оплати, зокрема використання ВА для того, щоб переміщати кошти та обійти санкції, а також пом'якшити обмежений доступ до платіжної системи SWIFT. Основними перешкодами для розширення використання ВА у цьому відношенні є ліквідність і розмір ринку, тоді як прозорий характер блокчейна може зменшити його привабливість для обходу санкцій.

6.2 Можливості для розслідування

Виходячи з інформації, отриманої з відповідей на опитувальник та інформації, доступної через MER, виявляється, що в більшості випадків юрисдикції не визначають слідчі зобов'язання з ВК/ФТ на основі *modus operandi* кейсів (наприклад, чи передбачають вони використання юридичних осіб, готівки або ВА, чи інших конкретних типологій). У країнах-членах MONEYVAL компетенція найчастіше визначається на основі предикатного злочину (наприклад, спеціалізовані підрозділи з розслідування справ ВК, яке випливає з корупції чи організованої злочинності, або спеціалізовані підрозділи з розгляду економічних злочинів чи складних справ). Як правило, менші юрисдикції мають один центральний ПО та/або підрозділ, що займається поверненням активів, який несе загальну відповідальність за

розслідування всіх кримінальних правопорушень, включаючи ВК/ФТ. Загалом виявляється, що розслідування справ ВК/ФТ за участю VASP або ВА, та застосування тимчасових запобіжних заходів, у зв'язку з цим, доручається ПО, на основі їхньої вже визначеної компетенції.

Проте є юрисдикції, які вирішили створити спеціалізовані підрозділи чи департаменти, в компетенції яких є розслідування справ (незалежно від їх характеру), пов'язаних із використанням ВА та VASP, або злочинів, скоєних із використанням технологій загалом.

Кейс 8: Спеціалізовані ПО для розслідування кейсів, пов'язаних із ВА або VASP – Боснія та Герцеговина і Болгарія

Боснія та Герцеговина – Міністерство внутрішніх справ Республіки Сербської (Republic of Srpska) створило спеціалізований відділ, відповідальний за виявлення та розслідування злочинів із залученням віртуальних активів. Відділ боротьби зі злочинністю у сфері високих технологій є частиною Відділу боротьби зі злочинністю Управління кримінальної поліції та бере на себе роль збору й обробки інформації про всі форми злочинності у сфері високих технологій, здійснюючи проактивний і реактивний збір, оцінку та аналіз даних розвідки.

Болгарія – в рамках Головного управління «Боротьби з організованою злочинністю» Міністерства внутрішніх справ, усі поліцейські мають повноваження розслідувати справи, пов'язані з віртуальними активами. Тим не менш, існує спеціалізований відділ, який в основному працює над такими справами, а саме Департамент боротьби з кіберзлочинністю Болгарії.

6.2.1. Збір розвідувальних даних і доказів від VASP

Що стосується збору розвідувальних даних, більшість країн-респондентів MONEYVAL зазначили, що їхні ПФР використовують свої законні права для збору інформації від фізичних та юридичних осіб, визначених як підзвітні суб'єкти, що також включає VASP. Однак, цей правовий механізм, значною мірою, залежить від підходу юрисдикції до призначення цілей ПВК/ФТ для VASP. Багато країн-членів MONEYVAL не визначили весь обсяг діяльності VASP, що зазначений у Рекомендаціях FATF. Як приклад, юрисдикції, які є країнами-членами ЄС і дотримуються положень 5-ї Директиви про боротьбу з відмиванням коштів, не охоплюють всю діяльність VASP за стандартами FATF[9]. Таким чином, поки існуватимуть прогалини в охопленні VASP серед країн-членів MONEYVAL і за їх межами, то залишатимуться юридичні перешкоди для збору фінансової інформації від VASP.

Меншість ПФР має ширші повноваження щодо запиту інформації від будь-якої фізичної чи юридичної особи, незалежно від того, чи є вони підзвітними суб'єктами, чи ні, як, наприклад, на острові Мен і в Мальті.

[9] Див. розділ 1.2 для отримання додаткової інформації про охоплення VASP у всьому регіоні MONEYVAL

Кейс 9: Отримання розвідувальної інформації від третіх сторін – Острів Мен і Мальта

Острів Мен – Стаття 18 Закону про Підрозділ фінансової розвідки, 2016 року, надає ПФР повноваження вимагати інформацію від будь-якої особи, яка не є спеціалізованим постачальником даних, але є особою, яка:
(i) згадується в отриманій інформації або її можна іншим чином ідентифікувати, вивчаючи таку інформацію;
(ii) за обґрунтованими відомостями чи переконаннями ПФР, володіє інформацією, що має відношення до аналізу отриманої ПФР інформації.

Мальта – статті 30 і 30A Закону про запобігання відмиванню коштів, надають ПФР Мальти повноваження збирати інформацію від будь-якої особи, органу чи організації, якщо ПФР Мальти вважає, що така інформація є актуальною та корисною для виконання будь-якої з його функцій, згідно з законом. Зокрема, функції аналітики розвідувальної інформації.

З огляду на те, що Рекомендація 15 вимагає ліцензування або реєстрації VASP, які знаходяться всередині юрисдикцій або мають свої приватні офіси, розташовані всередині країни, процес того, як будуть регулюватися децентралізовані бізнес-оператори, такі як децентралізовані криптобіржі, і, те, як саме можна отримати розвідувальну інформацію від них, враховуючи, що може не бути конкретної особи або осіб, які відповідають за операції, підлягає сумніву.

FATF намагалася вирішити це питання в оновленій версії керівних настанов, виданих у жовтні 2021 року[10]. У керівних настановах визнається, що Рекомендації FATF не застосовуються до базового програмного забезпечення, яке забезпечує транзакції ВА, а, отже, додатки децентралізованих фінансів (DeFi) не можна вважати VASP. Тим не менш, творці, власники та оператори, які можуть зберігати контроль або достатній вплив на функціонування цих протоколів DeFi, можуть підпадати під визначення VASP, оскільки вони будуть вважатися такими, що надають або сприяють послугам VASP. Однак, залишається сумнівним, чи всі DeFi протоколи матимуть певних контролерів або осіб, здатних впливати на операції, які розглядатимуться як VASP і використовуватимуться як джерело розвідувальної інформації та/або доказів.

Респонденти з країн-членів вказали, що з метою збору доказів та іншої інформації, вони покладаються на повноваження, які вони мають відповідно до кримінального законодавства, що застосовується до розслідування всіх інших видів злочинів. У деяких випадках, для отримання такої інформації потрібен дозвіл суду. Усі респонденти вказали, що ці повноваження щодо збору доказів також застосовуються до VASP та транзакцій з ВА. Респонденти також відзначили, що оскільки VASP можуть легко надавати послуги віддалено в різних юрисдикціях, для ПО виникають труднощі під час збору інформації від VASP, які не зареєстровані або не знаходяться в межах юрисдикції. Інші з респондентів, зауважили, що багато VASP не мають жодної зареєстрованої фізичної присутності, що ускладнює збір інформації.

6.2.2. Спеціальні інструменти розслідування

Як було зазначено у вступі до цієї глави, моніторинг і аналіз транзакцій ВА можуть бути певним чином полегшені тим фактом, що вся концепція технології блокчейн базується на

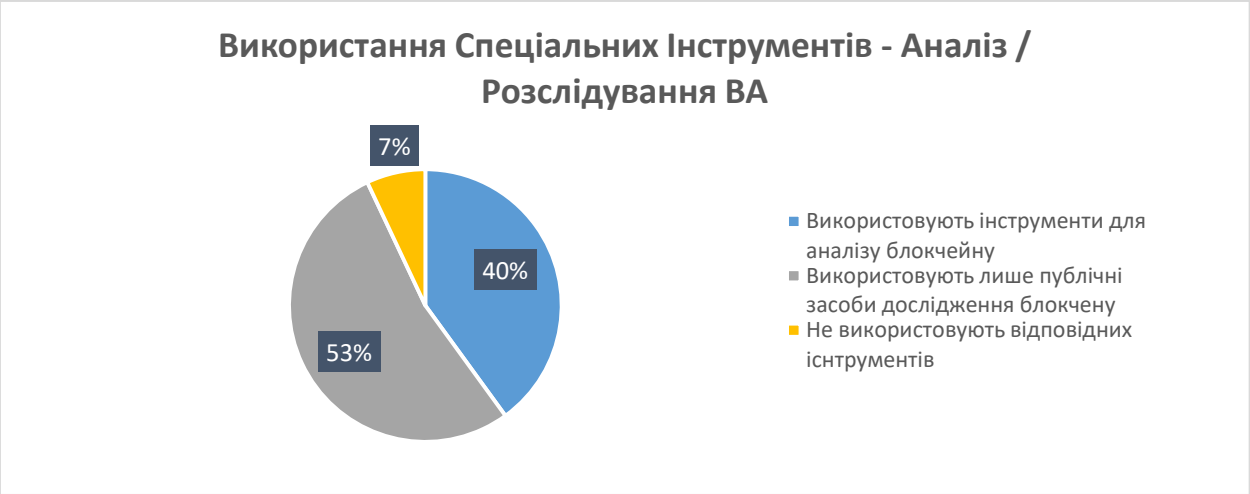
[10] https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html

понятті прозорості транзакцій і незмінності (тобто, не може бути змінено або видалено). Деякі блокчейн-мережі[11] є приватними, однак основні криптовалюти мають загальнодоступні дані про транзакції.

Це має позитивний характер, оскільки ПФР та ПО не повинні покладатися виключно на дані, надані ФУ та VASP, щоб мати можливість зрозуміти потік коштів, а можуть, до певної міри[12], отримати незалежний доступ до такої інформації. Щоб зробити це ефективним і надійним способом для досягнення цілей, а також мати можливість розшифровувати дані блокчейна зі значним успіхом, потрібні спеціальні інструменти. Можна послатися на звіт, опублікований Егмонтською Групою про співпрацю з Fintech та Асоціацією з типологій та ризиків кіберзлочинності[13], у якому зазначено, що в той час як деякі ПФР взагалі не можуть проаналізувати випадки, пов'язані з ВА, більше половини ПФР-респондентів заявили, що вони повинні покладатися на інформацію з відкритих джерел, оскільки їхнє внутрішнє аналітичне програмне забезпечення не мало можливості аналізувати такі транзакції. Це аж ніяк не вказує на позитивну перспективу можливостей ПФР виявляти та аналізувати випадки ВК/ФТ із застосуванням ВА.

З 15 країн-членів MONEYVAL, щодо яких була доступна інформація[14] про те, чи використовують вони будь-які спеціальні інструменти для аналізу чи дослідження транзакцій, пов'язаних із ВА, майже всі вказали, що вони використовують публічні засоби досліджень блокчейну або мають спеціальні інструменти для аналізу блокчейну, які надаються приватним сектором. Один з респондентів зазначив, що його ПФР/ПО не використовують ні те, ні інше, але знаходяться в процесі придбання інструменту для аналізу блокчейну. Тим не менш, шість країн-членів (загалом, із 15ти респондентів, які надали відповіді) вказали, що вони використовують інструменти для блокчейн-аналізу. Хоча, це неможливо порівняти (враховуючи, що проект Егмонтської Групи зосереджувався виключно на ПФР), схоже на те, що країни-члени MONEYVAL слідують загальносвітовим трендам, згідно з яких відповідні органи влади, переважно, не мають належних інструментів для аналізу та розслідування ВК/ФТ, пов'язаних з ВА.

Рисунок 14 – Використання Спеціальних Інструментів



[11] Наприклад Monero, Dash і Zcash

[12] Оскільки, доступна лише інформація про транзакції без персональних ідентифікаційних даних

[13] https://egmontgroup.org/wp-content/uploads/2022/11/2022-Report-on-FIE-FinTech-Cooperation-and-Assoc

[14] Інформація щодо цього аспекту була доступна або через відповіді на анкету, або через доступні MER

Країн-членів MONEYVAL також попросили поміркувати про основні функції, які вони шукали або шукали б, якщо потребували технологічних інструментів, щоб допомогти своїм органам у розслідуваннях або аналізі даних, пов'язаних з ВА. Країни-члени підкреслили наступні функції та аспекти:

- Інструмент повинен мати можливість групувати/кластеризувати транзакції та адреси гаманців, наприклад виділяти посередників та визначати потенційних зловмисників.
- Зручний і ефективний інструмент, який не потребує глибоких знань чи досвіду у сфері крипто-всесвіту.
- Здатність інструменту експортувати дані у формати, які можна читати та/або аналізувати.
- Наявність достовірних та актуальних даних.
- Економічна ефективність.

Деякі країни-члени повідомили, що передають частину цієї роботи спеціалізованим слідчим або експертам з приватного сектору, подібно до того, як патологоанатом, або група експертів з певних питань використовується в спеціалізованих кримінальних розслідуваннях.

6.3 Замороження та конфіскація ВА

Країн-членів MONEYVAL попросили надати інформацію про процес, прийнятий для застосування тимчасових запобіжних заходів для заморожування та арешту ВА. Сім країн-членів надали інформацію з цього приводу. Більшість зазначили, що вони звернуться за допомогою до VASP, які контролюють ВА, що можуть бути злочинними доходами, і накажуть їм заморозити активи. Деякі країни-члени заявили, що вони використовують офіційні/державні гаманці для передачі та зберігання конфіскованих ВА.

Здатність ефективно вилучати та передавати ВА, які не зберігаються у VASP (що зберігають ключі для гаманця), залежатиме від того, чи отримають ПО ключі для гаманця, що забезпечує контроль над ВА.

Кейс 10: Створення офіційного гаманця для конфіскації активів – Болгарія, Угорщина та Словенія

Болгарія – Національна слідча служба, яка входить до складу прокуратури, розробила процедуру, згідно з якою ВА конфіскуються шляхом переказу на адресу гаманця, який був створений з особливою метою для досудового провадження в апаратному гаманці прокуратури, або в гаманці, в якому для здійснення транзакції необхідно більше одного підпису.

Угорщина – відповідно до розділу 315 (Конфіскація та розпорядження про збереження електронних даних – Закон XC від 2017 року про Кримінально-процесуальний кодекс) конфіскація стає можливою шляхом переміщення ВА з гаманця підозрюваного в офіційний гаманець угорської поліції (BRFK).

Словенія. На практиці, конфіскація ВА здійснюється шляхом подання наказу про арешт відповідному VASP, в якому зазначається розпорядження перевести ВА в державний гаманець.

Виникають ситуації, коли ВА, які є доходами від злочину, скоєного в одній країні, можуть перебувати в іноземній юрисдикції. У таких ситуаціях, ПО зіткнуться з додатковими перешкодами в процесі заморожування або конфіскації таких ВА, оскільки вони не належать VASP, створеним у межах їхніх юрисдикції. Саме тут ефективне міжнародне співробітництво має фундаментальне значення для того, щоб мати можливість розслідувати подібні злочини та заморожувати або арештовувати злочинні активи.

Більшість юрисдикцій, які надали практичну інформацію про те, як саме вони розглядатимуть такі справи, справді посилалися на використання каналів міжнародного співробітництва (таких як ВПД). Респонденти зауважили, що сумніваються у тому, чи є такі механізми достатньо ефективними для забезпечення своєчасного вилучення або заморожування ВА. Країни-члени MONEYVAL також посилалися на використання повноважень ПФР щодо відстрочки для ефективного заморожування активів на досудовій стадії, поки не будуть застосовані більш офіційні засоби замороження та арешту активів.

Деякі країни-члени також зазначили, що вони намагаються попросити пряму допомогу іноземної VASP для арешту та заморожування активів, однак вони підкреслюють, що цей фактор неабияк залежить від готовності VASP добровільно співпрацювати.

Кейс 11: Замороження та конфіскація ВА, утримуваних в іноземних VASP – Латвія

Спосіб, у який здійснюється заморожування ВА, утримуваних в іноземних VASP, залежить від поточної ситуації. Бувають ситуації, коли ВА ідентифікуються разом із кодами доступу та паролями, що дозволяє негайно заарештувати та перенести ВА на гаманці, якими володіє компетентний орган. У таких ситуаціях цей актив можна перевести на гаманці ВА, які знаходяться на надійному зберіганні у Державному агентстві забезпечення Латвії. Бувають також ситуації, коли ВА належать іноземним VASP, які готові співпрацювати з ПО. У таких ситуаціях надсилається електронний лист із запитом до VASP призупинити операцію за участю відповідного ВА, яку VASP виконує на короткий період часу. Згодом (і залежно від ступеня співпраці з VASP та ступенем розвитку національної законодавчої бази, якою він обмежений), ПО можуть надіслати перекладений наказ про арешт в електронному вигляді до VASP з проханням арештувати та перевести ці активи в офіційний гаманець, що зберігається у VASP. Латвійське державне агентство забезпечення також може попросити VASP обміняти ВА на фіатні гроші і перерахувати еквівалентну вартість цих грошей на банківський рахунок ПО для зберігання.

Якщо законодавча база юрисдикції VASP не дозволяє йому виконувати такі прямі накази або, у випадку відсутності бажання VASP співпрацювати, запит про надання правової допомоги може бути надісланий органам влади юрисдикції, де знаходиться VASP. Наприклад, є ситуації, коли VASP не мають наміру спілкуватися з іноземними ПО, підтверджуючи, що вони будуть співпрацювати лише з місцевою владою. У таких випадках, успіх розслідування залежить від швидкості та якості співпраці між поліціями різних юрисдикцій та інших механізмів міжнародної співпраці.

Державна поліція Латвії створила ВА гаманці для найпопулярніших ВА – Bitcoin, Ethereum, Tether, Ripple XRP, Dogecoin, Shiba та інших. У 2022 році поліція успішно конфіскувала та продала ВА на суму приблизно 100 000 євро на публічному аукціоні.

Кейс 12: Заморожування та конфіскація ВА, які зберігаються в іноземних VASP – Німеччина

В одній справі, пов'язаній з розслідуванням щодо двох підозрюваних, аналіз транзакцій на банківських рахунках привів слідчих до виявлення придбання біткоїнів через VASP, який був створений в іноземній юрисдикції. Ордери на арешт були надіслані електронною поштою безпосередньо іноземному VASP. На підставі цих ордерів на арешт, VASP закриває облікові рахунки підозрюваних, щоб вони не мали змоги використовувати їх і розпорошувати ВА, які зберігаються там. Після цього, біткоїни були офіційно вилучені через судовий процес.

Можна також послатися на Посібник із арешту криптовалют[15], розроблений у рамках спільного проекту iPROCEEDS-2 Європейського Союзу та Ради Європи. Цей посібник може надати додаткову практичну інформацію та найкращі практики щодо конфіскації ВА.

6.4 Навчання та підвищення кваліфікації

Для ПФР та ПО надзвичайно важливо, щоб вони добре розуміли сектор ВА, а також особливості сектору VASP, що діють у межах їхніх юрисдикції. Це потребує постійного навчання для підвищення кваліфікації та розуміння органами влади цієї сфери, що постійно розвивається. Хороший рівень співпраці між регуляторними, наглядовими органами, ПФР та правоохоронними органами також бажаний для того, щоб усі відповідні органи були обізнані про ринкові операції в цій сфері, розуміли ризики та розробляли відповідні засоби контролю для їхнього пом'якшення, заради того, щоб протистояти зловживанню сектором для цілей ВК/ФТ.

Цей проект мав на меті проаналізувати частоту та тип навчання, пов'язаного з ВА/VASP, яке надають ПФР та ПО країн-членів MONEYVAL. 14 країн-членів вказали, що їхні ПФР пройшли навчання зі здобуття знань щодо ВА/VASP протягом періоду 2020–2022 років, тоді як 13 юрисдикцій вказали, що їхні ПО пройшли таке навчання за той самий період, що і проходили опитування. Регулярність тренінгів коливалася від 1 заходу протягом дворічного періоду до 7 заходів у випадку ПФР, і від 3 до 15 заходів для правоохоронних органів/прокуратури. У наведеному нижче списку наявна інформація про тип навчання, який пройшли ПФР щодо ВА/VASP.

- Відстеження, вилучення та конфіскація ВА
- Технічне навчання та вступні курси з віртуальних валют і технології блокчейн
- Навчання з ліцензування та нагляду за VASP
- Навчання з правових аспектів сфери ВА/VASP
- Вступні курси

[15] https://www.coe.int/en/web/cybercrime/-/iproceeds-2-guide-on-seizing-cryptocurrencies-available-on-the-octopus-cybercrime-community

- Використання Darknet
- Курси для слідчих, присвячені аналізу/розслідуванню випадків, пов'язаних із використанням ВА та ефективністю методів розслідування
- Спеціальне навчання, пов'язане з використанням спеціального програмного забезпечення для блокчейн-аналізу.
- Аналіз справ, пов'язаних із ВА/VASP
- Типології та методи ВК/ФТ за допомогою цифрових технологій, включаючи ВА
- Зосередженість на останніх технологічних розробках у цьому секторі.

Різні ПФР, ПО та прокурори посилалися на навчальні ініціативи, організовані міжнародними органами, такими як CEPOL, CoE, Еґмонтська Група, EUROJUST, EUROPOL та FATF. Деякі юрисдикції також використовували доступні онлайн-матеріали щодо ВА та VASP, надані міжнародними установами (наприклад, ECOFEL і CEPOL), тоді як інші юрисдикції заявили, що вони розробили внутрішні інструкції та навчальні матеріали, такі як онлайн-посібники та інструкції, що доступні для внутрішнього персоналу. Цей матеріал служить для надання базового та вступного огляду криптовалют, пов'язаних технологій та деяких вказівок щодо методів розслідування й червоних прапорців.

У деяких юрисдикціях були відмічені конкретні позитивні ініціативи щодо співпраці між ПФР, місцевими органами влади та VASP для отримання навчання щодо технологій та роботи VASP.

Кейс 13: Співпраця з приватним сектором і між державними органами для цілей навчання – Андорра та Словацька Республіка

Андорра – У травні 2021 року Unitat d'Intelligencia Financera (UIF) - ПФР Андорри - співпрацював з приватною юридичною фірмою та юридичною школою для організації навчання посадових осіб UIF з питань регулювання блокчейну та криптоактивів. Ще одна сесія відбулася в січні 2022 року у співпраці з Університетом Андорри, зосереджуючись на правових аспектах криптоактивів.

Словацька Республіка – Місцевий ПФР співпрацював зі словацькою криптокомпанією, щоб організувати одноденний навчальний захід для всього персоналу ПФР. Під час заходу було проведено тренінги з основ ВА, торгівлі криптовалютами та ризиків ВК, пов'язаних з ВА. Співробітники ПФР також взяли участь у двох семінарах, організованих Міністерством фінансів і Національним банком країни для навчання фінансовим технологіям та інноваціям.

6.5 Статистичні Дані – Розслідування, Вилучення, Заморожування та Конфіскація ВА

Декілька країн-членів MONEYVAL надали інформацію про загальну кількість розслідувань з ВК, проведених протягом 2020 та 2021 років. Ці країни-члени також надали інформацію про те, скільки розслідувань включало виявлення ймовірних злочинних доходів, які були віртуальними активами.

П'ять із восьми респондентів повідомили, що під час своїх розслідувань вони виявляли ВА, які ймовірно були отриманими злочинним шляхом. Однак, це сталося в дуже невеликій

кількості випадків ВК із загальної кількості розслідуваних (1%). Інші троє учасників повідомили, що вони ніколи не виявляли підозрювані злочинні доходи, які були ВА. Інші учасники повідомили, що вони не володіють статистичними даними, які б дозволили їм визначити, які розслідування виявили злочинні доходи, що були ВА.

Рисунок 15 – Розслідування ВК, пов'язані з ВА

Чотирьом із п'яти країн-членів, які розслідували відмивання коштів за участю ВА, вдалося вилучити та/або заморозити ВА на суму приблизно у 56,9 мільйона євро та 57 096 доларів США. Була одна країна-член на частку якої припадало 99% усієї приблизної вартості заморожених/арештованих ВА. Зазначається, що лише у двох країн-членів і у двох випадках після проведення розслідувань і заморожування активів, ВА вдалося конфіскувати.

6.6 Тематичні Дослідження

У цьому розділі представлено кілька кейсів з регіону MONEYVAL, які проливають світло на використання ВА в цілях ВК, серед яких, наприклад, типи основних злочинів, які зазвичай асоціюються з такими справами щодо ВК, а також *modus operandi* та типології того, як здійснюються такі випадки ВК. Зрозуміло, що ВА використовуються і, дивлячись на типології, ймовірно, можуть використовуватися як взаємозамінні з фіатними валютами.

Кейс 14: Крадіжка ВА через «тайпсквоттинг» – Острів Мен (у співпраці з Великобританією та Нідерландами)[16]

У 2019 році шість осіб були заарештовані у Великій Британії та Нідерландах у зв'язку з крадіжкою токенів Bitcoin. Вважається, що крадіжка торкнулася щонайменше 4000 жертв у 12 різних країнах, і викликала 14-місячне розслідування цієї крадіжки на 24 мільйони євро. Однією з жертв афери стала компанія з острова Мен.

Крадіжка була здійснена за допомогою техніки, яка називається «тайпсквоттинг», за допомогою якої веб-сайт відомої криптовалютної біржі було скопійовано, щоб відтворити оригінальний сайт і таким чином, привабити користувачів доступом до репліки сайту та отримання інформації про біткоїн-гаманці, для крадіжки коштів і даних для входу.

Поліція острова Мен (IOMC) співпрацювала в цій справі, обмінюючись розвідувальною інформацією та доказами, використовуючи механізми взаємодії між поліцейськими органами та ВПД. IOMC також працювала разом із Південно-Західним регіональним відділом боротьби з організованою злочинністю Великобританії (SWROCU) та голландським ПО, беручи участь у координаційних зустрічах Євроюсту. SWROCU допоміг IOMC у відстеженні та розшуку вкрадених біткоїнів. Більш масштабна справа була частиною спільної операції за участю Європейського центру боротьби з кіберзлочинністю (EC3) і Об'єднаної групи боротьби з кіберзлочинністю (J-CAT), на базі Європолу, після того, як британська влада виявила можливих підозрюваних, що проживають у Нідерландах.

Кейс 15: Продаж підроблених ВА – Азербайджан

Особи (громадяни іноземної держави), які раніше зареєстрували компанію в іноземній країні, що працює у сфері «емісії віртуальної валюти», зареєстрували рекламну компанію в Азербайджані («ADV»). Азербайджанська компанія рекламувала неіснуючу криптовалюту, заявляючи, що незабаром ця криптовалюта («XYZ Coin») буде продаватися на різних міжнародних платформах обміну криптовалютами. Зловмисники змогли зібрати великі суми грошей у громадян, яким обіцяли перебільшено високі доходи за інвестування в XYZ Coin.

Для тих, хто придбав XYZ Coin, були запропоновані три форми можливостей заробітку: (i) виплата дивідендів, що відповідає коштам, інвестованим у покупку XYZ Coin (через певний період часу), (ii) реферальні платежі за заохочення інших людей до інвестування у XYZ Coin та (iii) виплата високих прибутків після майбутнього розміщення XYZ Coin на іноземній біржі.

Злочинці штучно підвищували ціну на XYZ Coin кожні кілька місяців, щоб збільшити свій незаконний прибуток, заявляючи, що підвищення ціни відбулося через лістинг XYZ Coin на іноземній біржі. Ймовірні злочинці, щоб штучно знизити вартість інвестицій людей у XYZ Coin для власної вигоди, надали знижку людям, які купили монету на веб-сайті XYZCoin.com, пропонуючи обміняти 2 монети XYZ на XYZCoin.com на один XYZ Coin розміщений на біржі.

Кошти, перераховані на картки компанії ADV для купівлі XYZ Coin, склали кілька мільйонів одиниць валюти, 2/3 з яких становили платежі через платіжні термінали. Розслідування показало, що компанія не була зареєстрована на жодній біржовій платформі криптовалюти. Крім того, заявлена криптовалюта була лише псевдотокеном,

[16] https://www.europol.europa.eu/media-press/newsroom/news/6-arrested-in-uk-and-netherlands-in-%e2%82%ac24-million-cryptocurrency-theft

де передача відповідного токена іншій особі на біржі описувалася як процес продажу віртуальної валюти учасникам мережі. Попередня інформація про справу була отримана через соцмережі, веб-сайти та YouTube.

Кейс 16: Використання грошових мулів – Латвія

Відповідно до Оцінки ризиків відмивання коштів, фінансування тероризму та фінансування розповсюдження у секторі ВА, опублікованої Латвією в 2022 р.[17], кейси із залученням грошових мулів все ще вважаються актуальними. У відділі кримінальної поліції відкрито кримінальне провадження щодо організованої групи осіб, які тривалий час займалися ВК. За цей період було відкрито близько 100 рахунків у кредитних установах Латвії. У цьому конкретному випадку та за допомогою грошових мулів, доходи від шахрайства були переведені у вигляді фіатних грошей, які потім було отримано посередником та конвертовано у віртуальну валюту. Розслідування призвели до виявлення незареєстрованих VASP (які надавали послуги з обміну), які не контролювалися та не проводили належну перевірку клієнтів.

Крім того, ґрунтуючись на типології STR, латвійська оцінка ризику щодо віртуальних валют встановила, що в більшості STR, пов'язаних із використанням ВА (55%), основний злочин стосуватиметься майнових злочинів (включаючи шахрайство); у 34% не було визначено предикатний злочин і існують автономні ознаки ВК, тоді як в 7% висунули підозри щодо податкових правопорушень.

Кейс 17: Торгівля наркотиками та зброєю – Словацька Республіка[18]

Розслідування стосувалося громадянина Словаччини, який торгував вогнепальною зброєю, боєприпасами та наркотиками в даркнеті. Після затримання чоловіка, провели обшук його майна. Під час одного з обшуків було виявлено п'ять одиниць вогнепальної зброї, боєприпаси різного калібру, велику криту плантацію канабісу та біткоїн-гаманець, який містив біткоїни на суму 203 000 євро, які, як підозрюється, були отримані через незаконні послуги, що пропонувалися через даркнет.

Завдяки цьому розслідуванню влада Словаччини за сприяння Європолу ліквідувала онлайн-операцію з наркотиками в даркнеті, що діяла з 2015 року, через яку, за підозрами, було продано щонайменше 10 кг коноплі. Поліція також вилучила сервер, який використовувався для розміщення торгового майданчика у даркнеті, що дозволило владі розширити розслідування на користувачів і продавців, які використовували його. Крім того, завдяки міжнародній співпраці та допомозі Європолу, було виявлено ще одного даркнет-постачальника, який живе в іншій країні ЄС.

Ця справа стала проривом у Словацькій Республіці у сфері ВА, оскільки вона допомогла органам влади, які займалися цією справою, отримати досвід та можливі процедурні рішення, а також допомогла в розробці Посібника Генеральної прокуратури щодо віртуальних валют. Цей випадок також призвів до низки покращень після винесених уроків, таких як створення гаманця ПО, щоб дозволити конфіскацію активів, а також юридичні зміни до Кримінального кодексу, щоб полегшити конфіскацію ВА.

[17] https://fid.gov.lv/en/roles-and-responsibilities/guidelines

[18] https://www.europol.europa.eu/media-press/newsroom/news/darknet-dealer-of-drugs-and-arms-arrestedslovak-authorities

Кейс 18: Відмивання доходів, отриманих від торгівлі наркотиками – Мальта.

Громадянин ЄС, який проживає в іншій європейській країні, відкрив гаманець в біткоїнах у мальтійському VASP, у січні 2021 року. Протягом 20-місячного періоду, суб'єкт поклав на депозит загалом 29,255.02 фунтів стерлінгів за допомогою карток, виданих Європейським Банком. Ці кошти використовувалися для інвестування в ВА з використанням ліцензованого на Мальті VASP, причому більшість інвестиційної діяльності відбувалася протягом дев'яти днів. Протягом цього ж 20-місячного періоду суб'єкт був під розслідуванням в іншій європейській країні у зв'язку зі злочинами, пов'язаними з наркотиками. У той момент, коли кримінальне переслідування та обвинувальний вирок щодо суб'єкта за незаконний обіг наркотиків стало загальновідомим і було виявлено VASP за допомогою поточних процедур моніторингу, до FIAU було подано STR.

FIAU встановила, що суб'єкт був ув'язнений на сім років після того, як поліцейські в європейській країні вилучили певну кількість медичних і хімічних речовин, які використовувалися для виготовлення наркотиків. Хоча жодних подальших фінансових зв'язків на Мальті виявлено не було, і було встановлено, що суб'єкт не має жодних компаній чи банківських рахунків на Мальті, FIAU видала обґрунтовану підозру, що кошти, які зберігаються в мальтійському VASP, були доходами від злочинів, пов'язаних з наркотиками. Ця підозра була ще більше посилена тим фактом, що внесення ВА та інвестиційна діяльність суб'єкта відбувалися під час проведення розслідування над ним та його арешту, що додатково вказувало на спроби суб'єкта розпорошити потенційно злочинні доходи.

Після аналізу FIAU було надіслано звіт до поліції Мальти, яка подала клопотання про видачу наказу щодо накладення арешту на кошти, які зберігалися на адресі гаманця суб'єкта у мальтійському VASP. Станом на січень 2023 року суб'єкт мав на своєму рахунку 32,323.63 євро в біткоїнах, які наразі було конфісковано.