ЄВРОПЕЙСЬКА КОМІСІЯ

Брюссель, 24.07.2019
SWD(2019) 650 final

РОБОЧИЙ ДОКУМЕНТ ПЕРСОНАЛУ КОМІСІЇ,
який додається до

ЗВІТУ КОМІСІЇ ДО ЄВРОПЕЙСЬКОГО ПАРЛАМЕНТУ І РАДИ

про оцінку ризиків відмивання коштів та фінансування тероризму, що впливають на внутрішній ринок та пов'язані з транскордонною діяльністю

{COM(2019) 370 final}

ЗМІСТ

1. ВСТУП

Група з розробки фінансових заходів боротьби з відмиванням грошей (FATF) рекомендує країнам здійснювати оцінку ризиків з урахуванням їхнього потенціалу і досвіду у кожному секторі відповідно до вимог щодо протидії відмиванню коштів та фінансуванню тероризму (ПВК/ФТ). Країни повинні ідентифікувати, оцінювати та розуміти ризики відмивання коштів (ВК) та фінансування тероризму (ФТ) і вживати відповідних запобіжних заходів.

Визнаючи важливість наднаціонального підходу до ідентифікації ризиків, Директива (ЄС) 2015/849 (Четверта директива про боротьбу з відмиванням грошей) доручає Комісії здійснювати оцінку конкретних ризиків ВК/ФТ, які впливають на внутрішній ринок та пов'язані з транскордонною діяльністю.

Комісія опублікувала свою першу наднаціональну оцінку ризиків у 2017 році.[1] Відповідно до частини 1 статті 6 Четвертої директиви про боротьбу з відмиванням грошей Комісія повинна оновлювати свій звіт кожні два роки (або частіше, якщо доцільно). У цьому документі оновлюється інформація, що міститься у звіті 2017 року, аналізуються наявні ризики ВК/ФТ і пропонуються комплексні заходи для їх усунення. У ньому оцінюється ступінь виконання рекомендацій Комісії щодо пом'якшувальних заходів та оцінюється решта ризиків з урахуванням нових продуктів та секторів.

Докладна інформація про результати аналізу ризиків для кожного сектора та продукту представлена у **Додатку 1**.

2. МЕТОДОЛОГІЯ, ЯКА ВИКОРИСТОВУЄТЬСЯ ДЛЯ НАДНАЦІОНАЛЬНОЇ ОЦІНКИ РИЗИКІВ

У цій наднаціональній оцінці ризиків використовується методологія[2], яка використовувалася для наднаціональної оцінки ризиків 2017 року, що передбачає систематичний аналіз ризиків відмивання коштів та фінансування тероризму, пов'язаних з методами, використовуваними злочинцями. Метою є встановлення обставин, за яких послуги та продукти у певному секторі можуть бути використані для цілей ВК/ФТ, без винесення рішення щодо сектора в цілому.

У цій наднаціональній оцінці ризиків увага зосереджується на вразливостях на рівні ЄС, як в частині законодавчої бази, так і в частині її ефективного застосування. Тут представлені основні ризики для внутрішнього ринку в широкому діапазоні секторів та горизонтальні вразливості, які можуть впливати на такі сектори.

У цьому звіті визначені пом'якшувальні заходи, які мають вживатися на рівні ЄС та на національному рівні для усунення ризиків, та подано низку рекомендацій для різних зацікавлених сторін. Це не применшує значення пом'якшувальних заходів, які деякі держави-члени вживають або можуть вживати у відповідь на національні ризики ВК/ФТ. Тому пом'якшувальні заходи, про які йдеться у цьому звіті, слід вважати основою, яка може бути адаптована під ті національні заходи, які вже вживаються.

Відповідно до частини 4 статті 6 Четвертої директиви про боротьбу з відмиванням грошей, якщо держави-члени вирішать не застосовувати жодну з рекомендацій попередньої наднаціональної оцінки ризиків, вони повинні повідомити Комісії про своє рішення і надати обґрунтування (принцип «виконання або пояснення»). На сьогоднішній день Комісія не отримала жодного такого повідомлення.

---

[1] Звіт Комісії до Європейського Парламенту та Ради про оцінку ризиків відмивання коштів та фінансування тероризму, що впливають на внутрішній ринок та пов'язані з транскордонною діяльністю, COM(2017) 340 final.

[2] Більш докладна інформація міститься у SWD(2017) 241.

Процес

Під час підготовки цього звіту Комісія провела консультації з усіма зацікавленими сторонами, у ході яких було розглянуто різні сектори за допомогою цільових анкет та спеціальних семінарів.

У липні 2018 року Комісія провела консультації з державами-членами за допомогою анкети з додатками стосовно:

- національних пом'якшувальних заходів;
- шаблонів для фінансових і процесуальних даних про ВК/ФТ; та
- нових ризиків.

До кінця 2018 року Комісія отримала 23 відповіді.[3] Після цього з країнами-членами були проведені додаткові консультації на спеціальних засіданнях Експертної групи з питань відмивання коштів та фінансування тероризму[4], які відбулися 10 грудня 2018 року та 11 лютого 2019 року.

У листопаді-грудні 2018 року Комісія провела чотири семінари із зацікавленими сторонами приватного сектора: один з представниками фінансових установ, два з «встановленими нефінансовими підприємствами і професіями»[5] та один з громадянським суспільством (некомерційні організації) і науковцями. Другий етап цього раунду засідань відбувся у січні 2019 року. Усний внесок приватного сектора був доповнений 15 письмовими відповідями.

Комісія також провела консультації з іншими регулятивними установами та органами влади, такими як Європол та Європейські органи нагляду.[6]

Мета таких консультацій була подвійною: проконтролювати виконання рекомендацій, наданих у 2017 році, та оновити наднаціональну оцінку ризиків.

Нарешті, з огляду на еволюційний характер загроз та вразливостей, пов'язаних з ВК/ФТ, у наднаціональній оцінці ризиків має використовуватися інтегрований підхід до оцінки ефективності національних домовленостей щодо ПВК/ФТ.

Для моніторингу дотримання вимог ЄС, їх реалізації та їх запобіжної спроможності, Комісія належним чином враховує національні оцінки ризиків, здійснені державами-членами, для забезпечення належної ідентифікації та пом'якшення конкретних національних ризиків.[7]

---

[3] Болгарія, Кіпр, Франція, Угорщина та Ірландія не надали відповідей на анкету щодо виконання рекомендацій.

[4] Ця група складається з вищих державних службовців, відповідальних за ПВК у країнах ЄС/ЄЕП; http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=2914

[5] З представниками грального бізнесу консультації були проведені на окремому засіданні.

[6] Європейський служба банківського нагляду (EBA), Європейський орган страхування та пенсійного забезпечення (EIOPA) та Європейське управління з цінних паперів та ринків (ESMA).

[7] Це не применшує оцінки відповідних міжнародних організацій та розробників стандартів, таких як FATF та Комітет експертів з оцінки заходів протидії відмиванню коштів (Комітет експертів Ради Європи з оцінки заходів протидії відмиванню коштів та фінансуванню тероризму – Moneyval). Moneyval є постійним органом моніторингу Ради Європи. Він оцінює дотримання основних міжнародних стандартів ПВК/ФТ та ефективність їх реалізації, а також надає рекомендації національним органам влади щодо вдосконалення їх систем; https://www.coe.int/en/web/moneyval

Окремі сектори несуть відповідальність за третій рівень оцінки ризиків, де враховуються фактори ризику, включаючи ті, що стосуються конкретних клієнтів, країн, продуктів, послуг, операцій та каналів доставки.

Такі три рівні оцінки ризиків (наднаціональний, національний та галузевий), разом з пом'якшенням ризиків, якщо доцільно, сприяють всебічній обізнаності та аналізу ризиків ВК/ФТ в ЄС, в якому різні рівні доповнюють один одного і є однаково важливими.

Комісія застосовує та доповнює національні та галузеві оцінки шляхом оцінки ризиків, які впливають на внутрішній ринок Союзу та пов'язані з транскордонною діяльністю.

Законодавча база

Оцінка ризиків має забезпечувати короткий огляд ризиків відмивання коштів та фінансування тероризму та вимагає дотримання чітких термінів. Оцінка ризиків, що впливають на ЄС, була здійснена в той час, коли відповідну законодавчу базу становила Четверта директива про боротьбу з відмиванням грошей. Незважаючи на те, що П'ята директива про боротьбу з відмиванням грошей була ухвалена, її транспозиція ще не завершилася.

Тому наднаціональна оцінка ризиків ґрунтується на законодавстві ЄС, імплементованому на момент здійснення оцінки. На цьому слід наголосити кремо, оскільки деякі сектори не були охоплені або були охоплені лише обмежено зобов'язаннями, передбаченими у Четвертій директиві про боротьбу з відмиванням грошей. Тому рівень ризику може бути оцінений інакше для тих держав-членів, які вже застосовують більш суворий режим. Незважаючи на це, при визначенні нових пом'якшувальних заходів були враховані зміни, внесені П'ятою директивою про боротьбу з відмиванням грошей, яка має бути транспонована до січня 2020 року.

Хоча основним інструментом ЄС є Директива про боротьбу з відмиванням грошей, законодавча база Союзу про протидію відмиванню коштів та фінансуванню тероризму доповнюється іншими законодавчими актами ЄС. Орієнтовний перелік таких законодавчих актів наведений у **Додатку 2.**

Крім того, у **Додатку 3** містяться абревіатури, які використовуються в аналізі ризиків, а у **Додатку 5** – перелік використаної літератури.

3. РЕЗУЛЬТАТИ НАДНАЦІОНАЛЬНОЇ ОЦІНКИ РИЗИКІВ

У цій наднаціональній оцінці ризиків зосереджено увагу на ризиках, пов'язаних з кожним відповідним сектором, та оцінюються рекомендації, надані для усунення відповідних ризиків. Комісія визначила **47 продуктів та послуг**, які на її думку є потенційно вразливими до ризиків ВК/ФТ на рівні внутрішнього ринку, порівняно з 40 продуктами та послугами в оцінці 2017 року. Ці 47 продуктів та послуг стосуються **11 секторів**, зокрема:

- 10 секторів або продуктів, ідентифікованих Четвертою директивою про боротьбу з відмиванням грошей, тобто кредитні та фінансові установи, системи грошових переказів, пункти обміну валюти, торговці товарами та активами високої вартості, агенти з нерухомості, особи, які надають послуги з управління довірчими фондами та компаніями, аудитори, бухгалтери-ревізори та податкові консультанти, нотаріуси та інші незалежні юристи та провайдери послуг грального бізнесу.
- 1 категорія різноманітних продуктів, які не охоплені Четвертою директивою про боротьбу з відмиванням грошей, але вважаються важливими для оцінки ризиків, що включає підприємства з високим оборотом готівки, віртуальні валюти, «краудфандинг» та некомерційні організації. Ця категорія також охоплює певні неформальні засоби, наприклад, ті, що використовуються системою «хавала»[8] та іншими неформальними провайдерами послуг переказу грошових коштів; та
- чотири нові продукти/сектори, які не були оцінені у звіті 2017 року, а саме: приватні банкомати (АТМ-термінали); професійний футбол; порти вільної торгівлі та схеми надання інвесторам громадянства та виду на проживання («золоті паспорти/візи»).

Крім того, цей звіт містить розширений аналіз деяких послуг, які були оцінені у звіті 2017 року, а саме: FinTech; платформи обміну віртуальних валют та провайдери електронних гаманців; а також банківські рахунки нерезидентів.

Описи та оцінки багатьох продуктів/секторів, проаналізованих у звіті 2017 року, не були докорінно змінені впродовж останніх двох років, тоді як переглянута законодавча база Союзу щодо ПВК/ФТ була значною мірою оновлена з 2017 року.

У цій оцінці оновлено інформацію, що містилася у звіті 2017 року, шляхом її уточнення у декількох сферах (наприклад, некомерційні організації/НКО) та шляхом оновлення показників і джерел інформації. Крім того, ця оцінка включає посилання на чинну законодавчу базу Союзу щодо ПВК/ФТ з урахуванням того, що більшість рекомендацій щодо пом'якшувальних заходів у наднаціональній оцінці ризиків 2017 року[9] тепер включені до П'ятої директиви про боротьбу з відмиванням грошей. Більше того, особливу увагу було приділено імплементаційним положенням держав-членів Четвертої директиви про боротьбу з відмиванням грошей, які мали бути транспоновані до липня 2017 року. Інші пом'якшувальні заходи, рекомендовані у наднаціональній оцінці ризиків 2017 року, наразі враховуються останніми законодавчими актами ЄС, такими як Директива щодо закону про компанії[10] або новий Регламент про контроль готівкових коштів.[11]

---

[8] «Хавала» є популярною та неформальною системою переказу грошових коштів, яка базується на ефективності та гарній репутації величезної мережі грошових брокерів («хаваладарів»), а не на руху готівки.
Неформальні перекази грошових коштів здійснюються у системах або мережах, які отримують гроші для сплати коштів або еквівалентної вартості третій стороні у будь-якому місці, незалежно від того, чи сплачуються вони у тій самій формі або ні. Зазвичай вони здійснюються за межами звичайної банківської системи.

[9] Деякі з них були розроблені у світлі Регламенту 2005/60/ЄС Європейського Парламенту та Ради від 26 жовтня 2005 року про запобігання використанню фінансової системи для цілей відмивання коштів та фінансування тероризму, OB L 309, 25.11.2005, с. 15-36.

[10] Директива (ЄС) 2017/1132 Європейського Парламенту та Ради від 14 червня 2017 року щодо певних аспектів закону про компанії; OB L 169, 30.06.2017, с. 46. Ця Директива охоплює такі питання:
- Розголошення інформації про документи компанії, чинність зобов'язань, взятих на себе компанією, та втрата чинності. Вона застосовується до всіх публічних та приватних компаній з обмеженою відповідальністю. Створення публічних компаній з обмеженою відповідальністю та формування правил щодо збереження та зміни їх капіталу. Вона встановлює мінімальну вимогу до капіталу для публічних компаній з обмеженою відповідальністю ЄС у розмірі 25 000 євро. Вимоги до розкриття інформації для іноземних філій компаній. Вона охоплює компанії ЄС, які заснували філії в іншій країні ЄС, або компанії з країн, які не є членами ЄС, що засновують філії в ЄС.

[11] Регламент (ЄС) 2018/1672 Європейського Парламенту та Ради від 23 жовтня 2018 року про контроль

ДОДАТОК 1 – АНАЛІЗ РИЗИКІВ ЗА ПРОДУКТАМИ/СЕКТОРАМИ

У цій наднаціональній оцінці ризиків використовується спеціальна методологія, що передбачає систематичний аналіз ризиків ВК/ФТ, пов'язаних з методами, що використовують злочинці. Метою є встановлення обставин, за яких послуги та продукти у певному секторі можуть бути використані для цілей ВК/ФТ (без винесення рішення щодо сектора в цілому).

Оцінка ґрунтується на Директиві (ЄС) 2015/849 (Четверта директива про боротьбу з відмиванням грошей), яка становила законодавчу базу, що застосовувалася на момент здійснення аналізу. П'ята директива про боротьбу з відмиванням грошей (Директива (ЄС) 2018/843), якою внесено зміни до Четвертої директиви про боротьбу з відмиванням грошей, вважається частиною пом'якшувальних заходів.

Кожен ризик оцінюється з точки зору його загрози та вразливості. Оцінка здійснюється за шкалою від 1 до 4 таким чином:

1) **незначний (1 бал)**
2) **помірно значний (2 бали)**
3) **значний (3 бали)**
4) **дуже значний (4 бали)**

Оцінка використовувалася для підведення підсумку результатів аналізу. Вона не повинна розглядатися окремо від фактичного опису ризику.

ввезення в ЄС та вивезення з ЄС готівкових коштів і про скасування Регламенту № 1889/2005/ЄС, OB L 284, 12.11.2018, с. 6-2. Цей Регламент доповнює законодавчу базу ЄС щодо запобігання фінансуванню тероризму, передбачену у Директиві 2015/849. У ньому розглядаються сфери, в яких оцінкою Регламенту (ЄС) № 1889/2005 (Регламент про контроль готівкових коштів) було визначено можливість для вдосконалення, та реалізується низка заходів, передбачених у Плані дій Комісії для посилення боротьби з фінансуванням тероризму, COM(2016) 50 final, 02.02.2016.

ГОТІВКОВІ КОШТИ

1. Кур'єри готівкових коштів

Продукт
Кур'єри готівкових коштів/транскордонні переміщення готівкових коштів

Загальний опис сектора та відповідного продукту/діяльності
Ця оцінка охоплює наднаціональні ризики – тобто ввезення в ЄС та вивезення з ЄС готівкових коштів через зовнішні кордони ЄС.

Еволюція міжнародних стандартів щодо контролю транскордонних потоків готівкових коштів, оцінка того, наскільки цей Регламент досягає своїх цілей, а також отримана від держав-членів інформація змусили Комісію дійти висновку, що, хоча загальна ефективність цього Регламенту і була задовільною, для покращення його функціонування слід посилити низку напрямків.

Для визначення таких напрямків, а також у рамках Європейського порядку денного щодо безпеки та Плану дій щодо посилення боротьби з фінансуванням тероризму, у грудні 2016 року Комісія ухвалила пропозицію щодо нового Регламенту про контроль готівкових коштів. Після законодавчої роботи з Європейським Парламентом та Радою, у жовтні 2018 року був ухвалений новий Регламент (ЄС) № 2018/1672[12], який набуде чинності у червні 2021 року.

Чинний наразі Регламент про контроль готівкових коштів (Регламент (ЄС) 1889/2005)[13] встановлює єдиний підхід ЄС до контролю готівкових коштів на основі обов'язкової системи декларування. Якщо фізична особа, яка в'їжджає на територію ЄС або виїжджає з території ЄС (у тому числі транзитом), перевозить готівку на суму понад 10 000 євро, вона повинна задекларувати такі кошти. Граничне значення у 10 000 євро вважається досить високим, щоб не обтяжувати більшість подорожуючих і торговців зайвими адміністративними формальностями. Проте за наявності ознак протиправної діяльності, пов'язаної з переміщенням готівкових коштів у сумі менше 10 000 євро, збирання та реєстрування пов'язаної з такими переміщеннями інформації також є санкціонованим. Це положення було введено з метою обмеження практики «дроблення» чи «структурування», практики навмисного перевезення сум, менших за граничне значення, з наміром уникнення виконання зобов'язання щодо декларування (наприклад, шляхом розбивання суми між різними пов'язаними особами з однієї групи/родини).

[12] Регламент (ЄС) 2018/1672 Європейського Парламенту та Ради від 23 жовтня 2018 року про контроль ввезення в ЄС та вивезення з ЄС готівкових коштів і про скасування Регламенту № 1889/2005/ЄС, OB L 284, 12.11.2018, с. 6-2.
[13] Регламент № 1889/2005/ЄС, OB L 284, 12.11.2018, с. 6-2.

Чинні норми щодо переміщення готівкових коштів в ЄС та за межами ЄС застосовуються з 15 червня 2007 року і є невід'ємною частиною законодавчої бази ЄС щодо протидії відмиванню коштів та фінансуванню тероризму. Новий Регламент оновлює ці правила і доповнює законодавчу базу ЄС щодо запобігання відмиванню коштів та фінансуванню тероризму, передбачену Директивою 2015/849, із змінами та доповненнями, внесеними Директивою 2018/843.

Новий Регламент про контроль готівкових коштів, який набуде чинності у 2021 році, вдосконалює існуючу систему контролю за ввезенням в ЄС та вивезенням з ЄС готівкових коштів – останні зміни у міжнародних стандартах щодо протидії відмиванню коштів та фінансуванню тероризму, розроблені FATF, будуть відображені у законодавстві ЄС.

Згідно з новим Регламентом, визначення готівкових коштів було розширено та охоплює не тільки валюту та обігові інструменти на пред'явника, але й високоліквідні товари, такі як золото. Регламент також поширюється на готівкові кошти, які пересилаються поштою, вантажем або кур'єрською доставкою. Крім того, він дозволяє митним органам вживати заходів щодо сум, нижчих за граничне значення для декларування у розмірі 10 000 євро, за наявності підозр у злочинній діяльності та одночасно покращити обмін інформацією між органами влади (митні органи та підрозділи фінансової розвідки) і державами-членами.

Нове законодавство розширює зобов'язання будь-якого подорожуючого, який в'їжджає або виїжджає з території ЄС та перевозить готівкові кошти на суму понад 10 000 євро, щодо декларування таких коштів у митних органах. Декларування є необхідним, незалежно від того, чи перевозять подорожуючі готівкові кошти особисто, у своєму багажі або транспортними засобами. На запит органів влади вони повинні надати до них доступ для цілей перевірки.

Якщо готівкові кошти пересилаються іншими засобами («несупроводжувані готівкові кошти»), відповідні органи влади матимуть право вимагати від відправника або одержувача заповнення декларації. Органи влади зможуть здійснювати контроль за будь-якими поставками, відправленнями або транспортними засобами, які можуть містити несупроводжувані готівкові кошти.

Держави-члени повинні обмінюватися інформацією за наявності ознак того, що готівкові кошти пов'язані із злочинною діяльністю, яка може негативно вплинути на фінансові інтереси ЄС. Ця інформація також має бути передана Європейській Комісії.

Крім того, у частині 4 статті 5 нового Регламенту про контроль готівкових коштів передбачено, що при встановленні загальної системи критеріїв ризику для здійснення контролю митні органи повинні враховувати оцінки ризиків, здійснені Комісією та підрозділами фінансової розвідки.

Новий Регламент не перешкоджатиме державам-членам здійснювати додатковий національний контроль над переміщенням готівкових коштів у межах Союзу відповідно до їх національного законодавства, за умови, що такий контроль не порушуватиме основних свобод Союзу.

Щороку подається в середньому 90 000 декларацій про готівкові кошти на загальну суму близько 52 млн євро. Митний контроль виявляє 12 000 випадків недекларування готівкових коштів на суму близько 345 млн євро на рік.

Загальні зауваження

Цей сценарій ризиків по суті пов'язаний з використанням готівкових коштів/готівковими платежами, а також із сценарієм ризику банкнот високого номіналу.[14]

Злочинці або особи, що фінансують терористичну діяльність, які генерують/накопичують готівкові надходження, прагнуть об'єднати та перемістити такі прибутки зі свого джерела, будь то для репатріації коштів або для їх переміщення у місце, де буде легше інтегрувати їх у правову економіку.

Для таких місць характерне домінуюче використання готівкових коштів, більш слабкий нагляд за фінансовою системою або суворіші правила збереження банківської таємниці. Цей сценарій також може використовуватися терористами для швидкого та безпечного переказу грошових коштів з одного місця в інше, в тому числі шляхом приховування готівкових коштів під час повітряного транзиту.

Кур'єри готівкових коштів можуть використовувати повітряний, морський, автомобільний або залізничний транспорт для перетину зовнішнього кордону ЄС. Крім того, готівкові кошти можуть переміщуватися через зовнішні кордони без супроводу, наприклад, у контейнерних та інших формах вантажу, або приховуватися у поштових відправленнях та бандеролях. Якщо злочинці хочуть перемістити дуже велику суму готівкових коштів, вони можуть сховати її у вантажу, який може бути розміщений у контейнері або іншим чином перевозитися через кордон.

Злочинці можуть також використовувати складні методи приховування готівкових коштів у товарах, що перевозяться через зовнішній кордон кур'єром або надсилаються звичайним поштовим відправленням чи бандероллю. Хоча несупроводжувані перевезення, як правило, є меншими за ті, що приховуються у транспортних засобах або перевозяться кур'єрами готівкових коштів, використання банкнот високого номіналу все ще може призвести до конфіскації значимих сум.

Загроза

Фінансування тероризму

Оцінка загрози ФТ, пов'язаної з кур'єрами готівкових коштів/переміщеннями несупроводжуваних готівкових коштів, вказує на те, що терористичні групи використовують різноманітні способи переміщення фізичних готівкових коштів через зовнішні кордони, особливо у разі крупних організацій.

Така загроза є особливо актуальною для кур'єрів готівкових коштів з ЄС до третіх країн. Правоохоронні органи конфіскують крупні грошові суми у зонах конфлікту, призначені нібито для фінансування терористичних організацій. Більше того, були виявлені випадки, коли кількість (потенційних) іноземних бойовиків-терористів збільшилася вдвічі в якості кур'єрів готівкових коштів для фінансування своїх подорожей і перебування у зонах конфлікту. Зазвичай ці особи перевозять менші суми, які складніше виявити, і можуть не підлягати зобов'язанню щодо декларування, яке накладається на фізичних осіб, що перевозять суми у розмірі понад 10 000 євро готівкою. Оскільки це передбачає анонімність, такий спосіб дій вважається привабливим і досить безпечним, незважаючи на те, що він все ще зумовлює певні ризики. Саме тому такий спосіб дій також має розглядатися при аналізі банкнот високого номіналу. Чим вищого номіналу використовуються банкноти, тим простішим буде перевезення готівки – хоча ризики, пов'язані з придбанням банкнот високого номіналу (які є недоступними), не можуть переважати над

[14] Див., загалом, звіт (2015) ЄВРОПОЛ *«Чому готівка досі править?» (Why is cash still king?):* https://www.europol.europa.eu/sites/default/files/documents/europolcik%20%281%29.pdf

додатковою компактністю. Перевезення готівкових коштів є часто використовуваним способом дій для терористичних груп у Сирії – хоча середні суми, що їх перевозить іноземний бойовик, який виїжджає з ЄС, можуть бути незначними порівняно з наявними коштами.

Також може мати місце загроза перевезення готівкових коштів до ЄС з третьої країни, зокрема, з країн, які є схильними до ризиків ФТ, або із зон конфлікту (наприклад, були одержані повідомлення про кур'єрів готівкових коштів з Сирії, регіону Перської затоки, Росії до ЄС). Існують обмежені ознаки переміщення крупних сум готівкових коштів до Союзу (тобто таких, які значною мірою перевищують граничне значення для декларування) для цілей фінансування тероризму. Виявлено і випадки перевезення менших сум з інтеграцією грошових сум, що перевозяться з третіх країн, у фінансову систему/правову економіку ЄС (це питання окремо аналізується нижче).

З точки зору управління ризиками злочинців, пересилання готівкових коштів за допомогою поштових або вантажних відправлень з використанням декількох відправлень, кожне з яких містить менші суми, є теоретично привабливим рішенням, оскільки в цьому випадку немає кур'єра, який фізично перетинає зовнішній кордон, перевозячи готівку, якого можна було б перехопити. Хоча митний контроль може здійснюватися, він не передбачає збирання всіх відповідних даних.

Нарешті, злочинці можуть також конвертувати готівку в інші види анонімних активів, які не підлягають декларуванню (золото, передплачені картки, що також окремо аналізується нижче).[15]

Висновки: Правоохоронні органи зібрали докази того, що кур'єри готівкових коштів, які періодично використовуються терористичними групами для фінансування своєї діяльності або подорожей іноземних терористів-бойовиків. Аналогічно аналізу, здійсненому щодо готівкових коштів, використання злочинними елементами або особами, які фінансують терористичну діяльність, кур'єрів готівкових коштів має певні переваги, оскільки такий алгоритм дій є легкодоступним і не вимагає спеціального планування або знань. У цьому контексті, рівень загрози ФТ, пов'язаної з використанням кур'єрів готівкових коштів, вважається дуже значним (рівень 4).

Відмивання коштів

Звіт FATF: Відмивання коштів шляхом фізичного перевезення готівки (жовтень 2015 року)[16]

Спираючись на робочий документ Європейського центрального банку – використання споживчих готівкових коштів – порівняння між країнами з даними опитування щоденника платежів,[17] у звіті зазначається, що в опитаних країнах від 46 % до 82 % усіх фінансових операцій здійснюються готівкою, а саме Австралія (65 %), Австрія (82 %), Канада (53 %), Франція (56 %), Німеччина (82 %), Нідерланди (52 %) та Сполучені Штати Америки (46 %).[18]

Що стосується економіки, пов'язаної з транснаціональною організованою злочинністю, у звіті говорилося про фізичне перевезення готівкових коштів через міжнародний кордон, що є «однією з найстаріших та основних форм відмивання коштів», яка використовується також для

[15] Новий Регламент про контроль готівкових коштів, який набуде чинності у червні 2021 року, також охоплюватиме золото. Що стосується передплачених карток, за наявності вагомих доказів того, що злочинці використовують передплачені картки для переказу грошових коштів через кордони ЄС з обходом законодавства, тоді може бути використаний делегований акт для включення передплачених карток у Регламент.

[16] http://www.fatf-gafi.org/media/fatf/documents/reports/money-laundering-through-transportation-cash.pdf

[17] https://www.ecb.europa.eu/pub/pdf/scpwps/ecbwp1685.pdf

[18] Робочий документ Європейського центрального банку, № 1685/червень 2014, Таблиця 1, с. 38.

фінансування тероризму.[19] Хоча немає достовірних даних щодо грошових сум, які були «відмиті» у такий спосіб, у звіті визначено, що їх обсяг становить від «сотень мільярдів до трильйона доларів США на рік». У звіті пояснюється, що найбільш часто використовуються і «відмиваються» стабільні та популярні валюти, зокрема, долар США, євро, швейцарський франк та британський фунт стерлінгів, як правило, з використанням банкнот високого номіналу. У звіті також підкреслюється, що злочинці використовують існуючі механізми декларування готівкових коштів, наприклад, шляхом «повторного використання декларацій щодо готівкових коштів для тієї самої мети».[20]

У звіті Європолу за 2015 рік *«Чому готівка досі править?» (Why is cash still king?)* правоохоронні органи підтверджують, що готівкові кошти та, зокрема, банкноти високого номіналу зазвичай використовуються злочинними групуваннями як допоміжний засіб відмивання коштів. Самі по собі операції виявляють величезні суми готівкових коштів, переміщувані та приховувані злочинцями, які постійно інвестуються та інтегруються у правову економіку у різноманітні способи, що позбавляє злочинців від громіздких запасів готівкових коштів, які можуть бути конфісковані. Ці методи вимагають від співучасників та спільників або підставних осіб гарантування того, що їх інтеграція у правову економіку не викликає підозр.

В ЄС використання готівкових коштів досі залишається основною причиною, що ініціює звіти про підозрілі операції у межах фінансової системи, і становить 34% усіх звітів.

Злочинці, які генерують готівкові надходження, прагнуть об'єднати та перемістити такі прибутки зі свого джерела, будь то для репатріації коштів або для їх переміщення у місце, де буде легше інтегрувати їх у правову економіку, можливо, з огляду на переважне використання готівки в економіці деяких юрисдикцій, більш слабкий нагляд за фінансовою системою або суворіші правила збереження банківської таємниці, чи тому що вони можуть мати більший вплив в економічному та політичному істеблішменту.

Контрабанда готівкових коштів може мати місце на інших етапах, а також використовується у правопорушеннях, які не відносяться до правопорушень, що генерують готівкові кошти. Наприклад, кіберзлочини, такі як фішинг та хакерство, використовують грошових «мулів» для отримання та зняття сум, які були обманним шляхом отримані з банківських рахунків жертв, у готівковій формі. Після цього кошти надсилаються банківським переказом до інших юрисдикцій, де їх збирає готівкою певна кількість осіб, ймовірно, для подальшого перевезення.

З 2017 року готівка залишається актуальною загрозою, пов'язаною з відмиванням коштів. Європейські розслідування вказують на те, що переміщення готівкових коштів у межах ЄС та за межами ЄС пов'язане з кримінальними правопорушеннями. Найбільш актуальним напрямком злочину є незаконна торгівля наркотиками. Пов'язані з наркотиками готівкові надходження, що генеруються в результаті продажу та розповсюдження переважно кокаїну та гашишу, накопичуються та отримуються призначеними особами. Після цього організації з торгівлі наркотиками (DTO) встановлюють зв'язок з грошовими брокерами (як правило, за межами ЄС); ці брокери стягують комісію за свої послуги з організацій з торгівлі наркотиками, залежно від суми їх виручки. Брокери управляють власними мережами відмивання коштів у різних країнах. Після досягнення домовленості готівкові надходження передаються призначеним посередникам. Звідси готівкові кошти починають переміщуватися, перетинаючи ЄС у напрямку до призначеного вихідного пункту або безпосередньо залишаючи територію ЄС. Чинна законодавча база ЄС значною мірою перешкоджає інтеграції у фінансову систему великої кількості незаконних надходжень від торгівлі наркотиками. Через це гроші використовуються у схемах відмивання коштів на основі торговельної діяльності (TBML)[21] або вивозяться з території ЄС до

[19] Звіт FATF. с. 3.
[20] Там же, с. 16.
[21] Відмивання коштів на основі торговельної діяльності (TBML) є процесом, за допомогою якого злочинці використовують законну торгівлю для приховування злочинних надходжень зі своїх незаконних джерел.

юрисдикцій, які мають менш суворі вимоги до готівкових коштів. В останні роки Дубай та Бейрут показали себе як переважні пункти призначення готівки та зростаючі фінансові центри в ЄС.

Кур'єри готівкових коштів пов'язані із загрозою банкнот високого номіналу: 500 та 200 євро.

Висновки: рівень загрози ВК, пов'язаної з використанням кур'єрів готівкових коштів, вважається дуже значним (рівень 4)

Вразливість

Фінансування тероризму

a) схильність до ризику

Оцінка вразливості до ФТ, пов'язаної з використанням кур'єрів готівкових коштів, вказує на те, що з огляду на характер готівкових коштів, використання кур'єрів готівкових коштів уможливлює швидке та анонімне здійснення значних обсягів операцій/перевезень.

Транскордонний аспект цього способу дій збільшує ризик залучення географічних районів, визначених як зони високого ризику.

b) обізнаність про ризики

Чинне законодавство (обов'язкове декларування готівкових коштів фізичними особами на зовнішніх кордонах ЄС) підвищило рівень обізнаності про ризики, принаймні, що стосується фізичних осіб. Обізнаність про ризики існує для перевезення несупроводжуваних готівкових коштів, що наразі підпадає під дію нового регламенту, але є більш обмеженим.

c) законодавча база і засоби контролю

Існують засоби контролю шляхом обов'язкового декларування перевезення готівкових коштів на зовнішніх кордонах ЄС (Регламент про контроль готівкових коштів), і новий регламент розширює ці засоби митного контролю до готівкових коштів, що надсилаються у поштових або вантажних відправленнях, передплачених карток та дорогоцінних товарів, таких як золото, які раніше не підлягали митному контролю. Цей законодавчий акт підвищив рівень обізнаності про ризики, принаймні, що стосується фізичних осіб. Таке декларування готівкових коштів дозволяє полегшити виявлення підозрілих операцій та звітування підрозділам фінансової розвідки.

Що стосується несупроводжуваних готівкових коштів (готівкові кошти, що надсилаються вантажними або поштовими відправленнями), новий регламент дає змогу компетентним органам вимагати від відправника або одержувача, залежно від випадку, здійснення декларування. Декларування має бути здійснено у письмовому чи електронному вигляді за допомогою стандартної форми. Органи влади також матимуть право здійснювати контроль за будь-якими поставками, відправленнями або транспортними засобами, які можуть містити несупроводжувані готівкові кошти.

Злочин передбачає використання низки схем для ускладнення документації законних торгових операцій; такі дії можуть включати переміщення незаконних товарів, фальсифікацію документів, неправдиве представлення фінансових операцій та недооцінку чи переоцінку вартості товарів.

Висновки: Схильність до ризику фізичних осіб, пов'язана з використанням кур'єрів готівкових коштів, по суті пов'язана з діяльністю на основі готівкових коштів (великий обсяг, анонімність, швидкість), що посилюється тим фактом, що (особливо у контексті терористичної діяльності) окремі кур'єри часто перевозять суми нижче декларативного граничного значення. Незважаючи на те, що обсяг кур'єрів готівкових коштів може бути важливішим, ніж для несупроводжуваних перевезень, обізнаність про ризики та контроль все-таки мають місце.

Використання кур'єрів готівкових коштів або способів ввезення в ЄС/вивезення з ЄС несупроводжуваних готівкових коштів, у поєднанні з анонімністю готівкових коштів та (принаймні, стосовно несупроводжуваної готівки) недосконалим механізмом контролю становить неабияку проблему. Хоча обсяг несупроводжуваних готівкових коштів, що ввозиться в ЄС/вивозиться з ЄС, вірогідно, є меншим, ніж у разі використання кур'єрів готівкових коштів, обізнаність про ризики та контроль останніх становлять ще більшу проблему.

У цьому контексті рівень вразливості фізичних осіб до ФТ, пов'язаної з кур'єрами готівкових коштів, вважається значним (рівень 3). Рівень вразливості до ФТ, пов'язаний з поштовими/вантажними перевезеннями, вважається дуже значним, враховуючи існуючі засоби контролю/законодавчу базу, більше за притаманну схильність до ризику (рівень 4).

Відмивання коштів

a) схильність до ризику

Оцінка вразливості до ВК, пов'язаної з кур'єрами готівкових коштів, вказує на те, що схильність до ризику по суті пов'язана з діяльністю на основі готівкових коштів (анонімність, швидкість). Отже, схильність до ризику є особливо важливою для цього алгоритму дій.

b) обізнаність про ризики

Чинне законодавство (обов'язкове декларування готівкових коштів на зовнішніх кордонах ЄС для готівки, що перевозиться фізичними особами) підвищило рівень обізнаності про ризики, принаймні, що стосується фізичних осіб.

Обізнаність про ризики існує для перевезення несупроводжуваної фізичної готівки, але є більш обмеженою по відношенню до поштових перевезень/вантажних перевезень/перевезень кур'єрами.

c) законодавча база і засоби контролю

Подібно до ФТ, здійснюється контроль шляхом обов'язкового декларування перевезень готівкових коштів через зовнішні кордони ЄС (Регламент про контроль готівкових коштів) фізичними особами.

Таке декларування готівкових коштів дозволяє полегшити виявлення підозрілих операцій та повідомляється підрозділам фінансової розвідки (хоча в обміні інформацією мають місце недоліки, і приведення у виконання може бути різним у різних державах-членах).

Що стосується несупроводжуваних готівкових коштів (готівкові кошти, що надсилаються за допомогою вантажних або поштових відправлень), новий регламент дозволяє компетентним органам здійснювати аналіз ризиків та концентрувати свої зусилля на тих відправленнях, які, на їх думку, представляють найвищий ризик, не накладаючи при цьому систематичних додаткових формальностей. Зобов'язання щодо розкриття інформації підпорядковується граничному значенню, ідентичному граничному значенню для готівкових коштів, що перевозяться фізичними особами.

Висновки: Схильність до ризику фізичних осіб, пов'язана з використанням кур'єрів готівкових коштів, по суті пов'язана з діяльністю на основі готівкових коштів (великий обсяг, анонімність, швидкість). Незважаючи на те, що обсяг кур'єрів готівкових коштів може бути більш важливим, обізнаність про ризики та контроль все-таки мають місце. Використання кур'єрів готівкових коштів або способів ввезення в ЄС/вивезення з ЄС несупроводжуваних готівкових коштів, у поєднанні з анонімністю готівкових коштів та (принаймні, стосовно несупроводжуваних готівкових коштів) недосконалим механізмом контролю є неабиякою проблемою. Хоча обсяг несупроводжуваних готівкових коштів, що ввозиться в ЄС/вивозиться з ЄС, вірогідно, є меншим, ніж у разі використання кур'єрів готівкових коштів, обізнаність про ризики та контроль становлять ще більшу проблему. У цьому контексті, рівень вразливості фізичних осіб до ВК, пов'язаної з використанням кур'єрів готівкових коштів, вважається значним (рівень 3), а для поштових/вантажних відправлень – дуже значним (рівень 4).

Пом'якшувальні заходи:

Новий Регламент про контроль готівкових коштів, який застосовуватиметься з 3 червня 2021 року, посилює існуючі правила щодо переміщення грошових коштів:

- дозволяє органам влади вживати заходів щодо сум, які є нижчими за граничне значення декларування у розмірі 10 000 євро, за наявності підозр у злочинній діяльності;
- покращує обмін інформацією між органами влади та державами-членами;
- дає змогу компетентним органам вимагати розкриття інформації щодо готівкових коштів, які надсилаються у супроводжуваних відправленнях, таких як готівка, що надсилається у поштових або вантажних відправленнях;
- розширює визначення поняття «готівка» до дорогоцінних товарів, що виступають як високоліквідні запаси вартості, такі як золото, а також до передплачених платіжних карток, які наразі не підпадають під дію стандартного декларування готівкових коштів.

2. Підприємства з високим оборотом готівки

Продукт
Підприємства з високим оборотом готівки

Сектор
Бари, ресторани, будівельні компанії, роздрібні торговці автотранспортом, мийки автомобілів, продавці предметів мистецтва та антикваріату, аукціонні будинки, ломбарди, магазини ювелірних виробів, магазини текстилю, магазини алкогольних і тютюнових виробів, роздрібні/нічні магазини, установи, які надають послуги азартних ігор, стрип-клуби, масажні салони.

Загальний опис сектора та відповідного продукту/діяльності

Цікавий опис використання готівкових грошей був представлений Європейським центральним банком у його звіті *«Тенденції та зміни у використанні готівкових коштів в євро протягом останніх десяти років»*[22] (опублікований в Економічному віснику ЄЦБ, випуск 6/2018).[23]

2 лютого 2016 року Комісія опублікувала Повідомлення Європейському Парламенту та Раді щодо Плану дій для подальшої активізації боротьби з фінансуванням тероризму.[24] План дій побудований на чинних положеннях ЄС для адаптації до нових загроз та спрямований на оновлення політики ЄС відповідно до міжнародних стандартів. У ньому обговорюються численні питання та рішення у різних сферах, пов'язаних з фінансуванням тероризму.

У контексті заходів Комісії щодо розширення сфери застосування Регламенту про контроль ввезення в ЄС та вивезення з ЄС готівкових коштів, містилося посилання на доцільність дослідження відповідності можливих верхніх граничних значень готівкових платежів.[25] У Плані дій також додатково зазначено, що «Декілька держав-членів мають заборони на готівкові платежі вище встановленого граничного значення». Однак такі заборони не розглядаються на рівні ЄС.

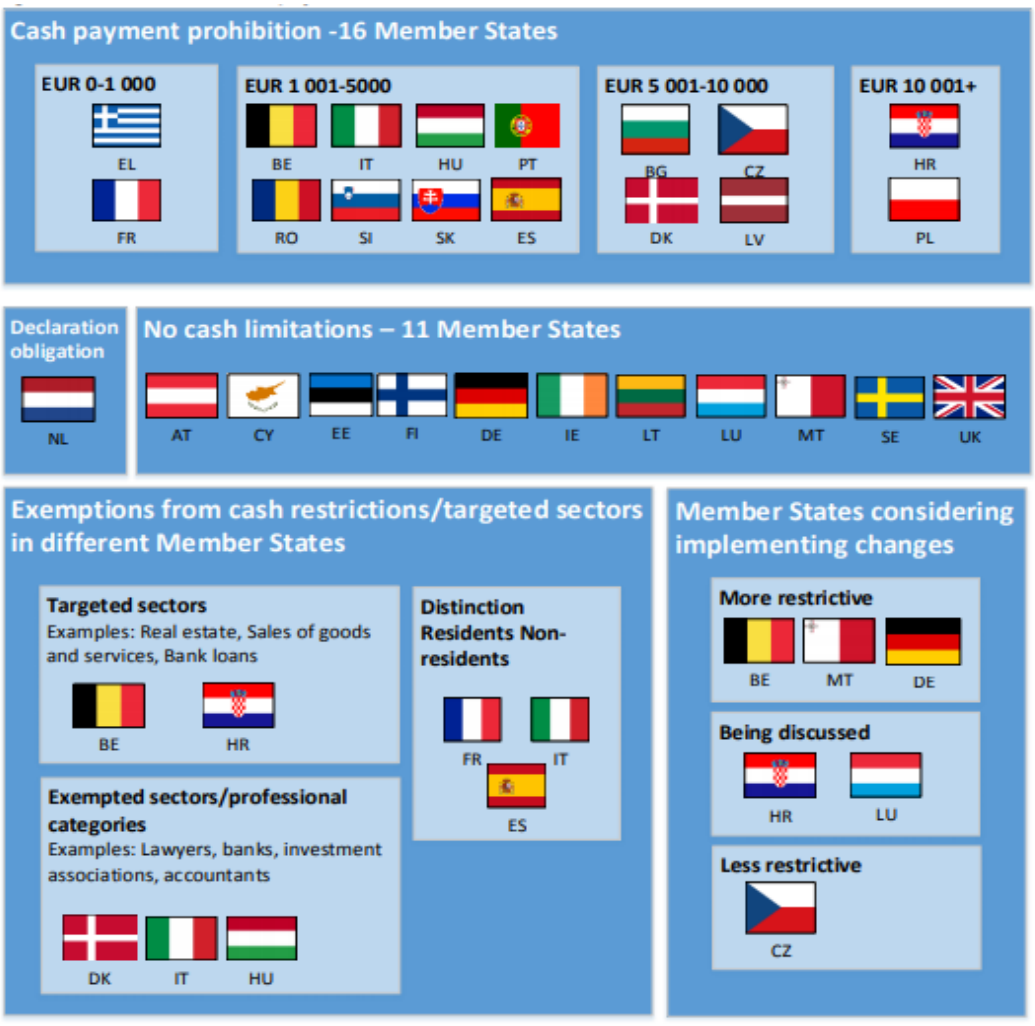
На рисунку нижче представлено обмеження щодо готівкових платежів, які наразі діють у державах-членах ЄС, а також вказується, чи є плани щодо їх адаптування або зміни. На першій інфографіці показано, що заборона на готівкові платежі наразі застосовується у 16 державах-членах. Граничні значення коливаються від 500 євро у Греції та 1 000 євро у Франції до приблизно 13 800 євро у Хорватії та 15 000 євро у Польщі. Нідерланди є єдиною країною, яка прийняла зобов'язання щодо декларування, а в інших 11 державах-членах ЄС не встановлено жодних готівкових обмежень.

У деяких державах-членах ЄС окремі бізнес-сектори або споживачі звільняються від заборон на готівкові кошти або підлягають ним. У Франції, Італії та Іспанії розрізняють резидентів у відповідних країнах та нерезидентів. У цьому сенсі у Франції та Іспанії нерезиденти можуть здійснювати платежі на суму до вищого граничного значення (15 000 євро), тоді як в Італії загальне граничне значення не застосовується до нерезидентів. Інші країни виключають з готівкових обмежень окремі сектори, що дозволяє спеціалістам у цих секторах здійснювати операції готівкою вище загальноприйнятного граничного значення. Наприклад, у Данії одинадцять професійних категорій, включаючи банки та адвокатів, звільнені від застосування

[22] https://www.ecb.europa.eu/pub/economic-bulletin/articles/2018/html/ecb.ebart201806_03.en.html#toc2
[23] https://www.ecb.europa.eu/pub/economic-bulletin/html/eb201806.en.html
[24] COM (2016)50.
[25] У Плані дій зазначено, що «Платежі готівкою широко використовуються для фінансування терористичної діяльності... У цьому контексті також може бути досліджена відповідність потенційних верхніх граничних значень для готівкових платежів. Декілька держав-членів мають заборони на готівкові платежі вище визначеного граничного значення».

граничних значень. Що стосується Бельгії та Хорватії, у деяких секторах застосовуються нижчі граничні значення. Наприклад, у Бельгії готівкові операції повністю заборонені у секторі нерухомості.

У ряді країн обговорюється можливість накладення нових заборон на готівкові платежі, в той час як інші країни розглядають можливість зміни свого діючого граничного значення. Бельгія розглядає можливість розширення сфери застосування обмежень та включення всіх операцій, крім фізичних осіб. Німеччина та Мальта розглядають можливість накладення заборони на готівкові платежі. Це питання також обговорюється у Люксембургу та Хорватії, без конкретної пропозиції щодо підготовки більш чи менш обмежувальних заходів. Чеська Республіка є єдиною країною, яка рухається у напрямку застосування менш обмежувальних заходів.



Source: Ecorys and CEPS own elaboration.

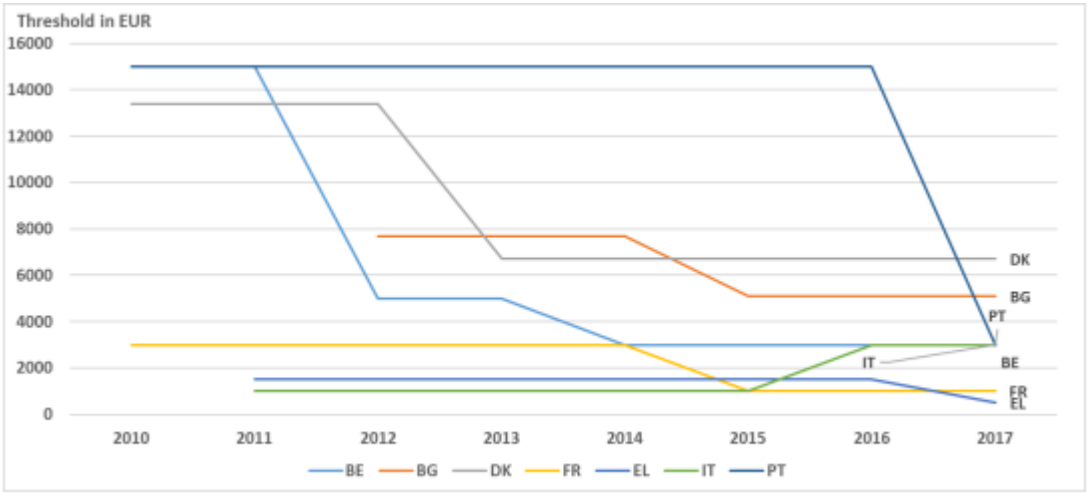
Заборона на готівкові платежі – 16 держав-членів			
0 -1 000 євро	1 001 – 5 000 євро	5 001 – 10 000 євро	10 001+ євро
Зобов'язання щодо декларування	**Відсутність обмежень на готівкові платежі – 1 держав-членів**		

Винятки з обмежень на готівкові платежі/цільові сектори у різних державах-членах		**Держави-члени, які розглядають можливість внесення змін**
Цільові сектори Приклади: нерухомість, продаж товарів та послуг, банківські позики	**Різниця між резидентами та нерезидентами**	**Більш обмежувальні** **Питання обговорюється** **Менш обмежувальні**
Звільнені сектори/професійні категорії Приклади: юристи, банки, інвестиційні асоціації, бухгалтери		

Джерело: Власні розробки Ecorys та CEPS.

На рисунку нижче показано, що шість держав-членів ЄС, в яких діє заборона на готівкові платежі, протягом останніх семи років знизили своє граничне значення. Італія є єдиною

державою-членом ЄС, яка наклала заборону на готівкові платежі на нижчому граничному значенні (1 000 євро), а потім підвищила його до 3 000 євро у 2016 році.



Source: Ecorys and CEPS own elaboration.

Граничне значення в євро
Джерело: Власні розробки Ecorys та CEPS.

Опис сценарію ризиків

Злочинці використовують підприємства з високим оборотом готівки:

- для відмивання крупних сум готівкових коштів, одержаних злочинним шляхом, заявляючи, що ці кошти були одержані в результаті здійснення економічної діяльності;
- для відмивання готівкових коштів, які є доходами від злочинної діяльності, обґрунтовуючи їх походження на основі фіктивної економічної діяльності (як для товарів, так і для послуг);
- для фінансування терористичної діяльності за допомогою часто невеликих сум готівкових коштів без будь-якої можливості їх відстеження.

Загальні зауваження

Цей сценарій ризиків по суті пов'язаний з використанням готівкових коштів/готівковими платежами, а також із сценарієм ризику банкнот високого номіналу.

Загроза

Фінансування тероризму

Оцінка загрози ФТ, пов'язаної з використанням підприємств з високим оборотом готівки, вказує на те, що підприємствами з високим оборотом готівки, як правило, керують фізичні особи через бари, ресторани, салони мобільного зв'язку тощо, але фактично управляє мережа осіб, що утворюють терористичну організацію. Загалом, вони використовуються для швидкого отримання чистої готівки (наприклад, продаж автомобілів або ювелірних виробів). Однак цей сценарій ризиків використовується по-різному всіма терористичними організаціями (наприклад, ніколи не використовується для «Даеш») і не є популярним, оскільки для нього потрібна здатність керувати бізнесом.

Висновки: елементи, зібрані правоохоронними органами та підрозділами фінансової розвідки, вказують не те, що зареєстровано лише декілька випадків, що означає, що терористичні групи не надають переваги використанню такого сценарію ризиків, оскільки він вимагає певних технічних знань та інвестицій для самостійного керування

бізнесом, що зменшує привабливість такого способу дій. Однак, оскільки цей ризик є не лише гіпотетичним і враховуючи той факт, що у підприємствах з високим оборотом готівки присутні «кроти», рівень загрози ФТ, пов'язаної з використанням підприємств з високим оборотом готівки, вважається помірно значним (рівень 2).

Відмивання коштів

Оцінка загрози ВК, пов'язаної з використанням підприємств з високим оборотом готівки, вказує на те, що цей спосіб дій використовується злочинцями, оскільки він є життєздатним, досить привабливим та безпечним рішенням. Це найпростіший спосіб приховати незаконний дохід від злочинної діяльності. Однак, що стосується ФТ, використання цього способу потребує помірного рівня знань, аби мати змогу керувати бізнесом і не бути виявленими.

Правоохоронні органи підтверджують, що підприємства з високим оборотом готівки продовжують використовуватися для відмивання доходів від злочинної діяльності.

Висновки: для відмивання доходів від злочинної діяльності злочинні організації надають перевагу підприємствам з високим оборотом готівки. Оскільки для керування бізнесом потрібен певний рівень знань, рівень загрози ВК, пов'язаної з використанням підприємств з високим оборотом готівки, вважається значним (рівень 3).

Вразливість

Фінансування тероризму

Оцінка вразливості до ФТ, пов'язаної з використанням підприємств з високим оборотом готівки, вказує на те, що основні фактори пов'язані з ризиками, що створюються готівковими коштами.

a) схильність до ризику

Хоча підприємства з високим оборотом готівки є менш привабливими для терористичних організацій, ніж для злочинців (див. оцінку загроз нижче), коли вони використовуються терористами, вони представляють певні вразливості, тому що основний ризик пов'язаний з готівковими коштами. Оцінка вразливості до ФТ, пов'язаної з використанням підприємств з високим оборотом готівки, по суті пов'язана з оцінкою вразливості, пов'язаної з використанням готівкових коштів/готівковими платежами загалом, і може мати те саме обґрунтування. Підприємства з високим оборотом готівки дають змогу обробляти величезну кількість анонімних операцій, які не вимагають вміння управляти новими технологіями та інструментами відстеження. Отже, вони мають високу схильність до ризику.

b) обізнаність про ризики

Обізнаність про ризики здається досить низькою, оскільки, навіть якщо крупні суми готівкових коштів можуть бути отримані від підприємств з високим оборотом готівки, деякі підрозділи фінансової розвідки помічають, що терористичні організації надають перевагу використанню банкнот нижчого номіналу, які зобов'язаним суб'єктам та правоохоронним органам не так легко визначити як підозрілі.

c) законодавча база і засоби контролю

Чинна законодавча база пов'язана з обмеженнями щодо готівкових платежів, запровадженими деякими державами-членами. Ця база є досить різною в різних державах-членах в частині

контролю готівкових коштів та обмежень щодо готівкових платежів, і тому контроль може бути відсутнім.

Висновки: вразливість, пов'язана з використанням підприємств з високим оборотом готівки, по суті пов'язана з вразливостями, пов'язаними з використанням готівкових коштів загалом. Враховуючи розмаїття чинних законодавчих баз, широке використання готівки в економіках ЄС і той факт, що сектор, здається, не усвідомлює цього ризику, рівень вразливості до ФТ, пов'язаної з використанням підприємств з високим оборотом готівки, вважається дуже значним (рівень 4).

Відмивання коштів

Оцінка вразливості до ВК, пов'язаної з використанням підприємств з високим оборотом готівки, вказує на те, що основні фактори пов'язані з ризиками, що створюються готівковими коштами.

a) схильність до ризику

Оцінка вразливості до ВК, пов'язаної з використанням підприємств з високим оборотом готівки, по суті пов'язана з оцінкою вразливості, пов'язаної з використанням готівкових коштів/готівковими платежами загалом, і може мати те саме обґрунтування. Підприємства з високим оборотом готівки діють змогу обробляти величезну кількість анонімних операцій, які не потребують вміння управляти новими технологіями та інструментами відстеження. Ця схильність до ризику стосується готівкових платежів, як за товари, так і за послуги. Отже, вони мають високу схильність до ризику.

b) обізнаність про ризики

Зобов'язані суб'єкти, як правило, обізнані про ризик, що створюється готівковими коштами, хоча контроль не так просто реалізувати. Однак, що стосується інших професійних категорій, які не підпадають під зобов'язання щодо ПВК/ФТ, обізнаність про ризики залишається проблемою.

c) законодавча база і засоби контролю

Наразі на рівні ЄС не встановлено жодних верхніх граничних значень для готівкових платежів. У своєму Плані дій щодо посилення боротьби з фінансуванням тероризму Комісія вже повідомила про можливість подальшого дослідження верхніх граничних значень для обмежень щодо готівкових коштів як про додаткову ініціативу для доповнення чинної європейської законодавчої бази щодо ПВК/ФТ.[26]

На вразливість сектора впливає існування або відсутність норм щодо обмежень для готівкових платежів:

- у разі існування норм щодо обмежень для готівкових коштів, вразливості до ВК, пов'язані з використанням підприємств з високим оборотом готівки, легше усуваються завдяки правовим вимогам, які дозволяють відхилити готівкові платежі, що перевищують певне граничне значення. У цих випадках здійснюється контроль, який полегшує виявлення тривожних сигналів та підозрілих операцій. Крім того, ці граничні значення для готівкових платежів сприймаються сектором та правоохоронними органами як більш ефективні та менш обтяжливі, ніж накладення зобов'язання щодо здійснення належної перевірки клієнтів. Однак, такі законні підприємства також можуть приховувати тіньову та незаконну

[26] Див. COM2015(50).

діяльність, яка здатна обходити обмеження щодо готівкових платежів;

- у разі існування норм щодо обмежень для готівкових коштів, і хоча рівень обізнаності про ризики є досить високим, сектор не знає, як управляти ризиками. У нього немає інструментів для контролю та виявлення підозрілих операцій. У результаті, кількість звітів про підозрілі операції є досить низькою або навіть нульовою.

Деякі держави-члени запровадили звіти про готівкові операції, які підлягають декларуванню для готівкових операцій, що перевищують певне граничне значення. Однак на рівні ЄС немає загального підходу.

З точки зору внутрішнього ринку, відмінності між законодавствами держав-членів щодо обмежень для готівкових коштів збільшують вразливість для внутрішнього ринку; злочинцям легше обходити контроль у своїй країні походження шляхом інвестування у підприємства з високим оборотом готівки в інших державах-членах, які мають слабкіший контроль/в яких відсутній контроль за обмеженнями для готівкових коштів. Наявність обмежень щодо готівкових платежів у деяких державах-членах та їх відсутність в інших державах-членах створює можливість для обходу обмежень шляхом переміщення до держав-членів, в яких обмеження відсутні, з одночасним здійсненням своєї терористичної або іншої незаконної діяльності в іншій «суворішій» державі-члені.

Для збільшення пильності та пом'якшення ризиків, що створюють такі готівкові платежі, особи, які торгують товарами, підпадають під дію Директиви, якщо вони здійснюють або отримують грошові платежі у розмірі понад 10 000 євро. На таке саме граничне значення також є посилання у Директиві 2018/843 (П'ята директива про боротьбу з відмиванням грошей). Держави-члени можуть встановити нижчі граничні значення, додаткові загальні обмеження щодо використання готівкових коштів та ухвалити додаткові суворіші положення.

Однак ефективність таких заходів все ще обмежена з огляду на кількість звітів про підозрілі операції. Обсяг звітів про підозрілі операції є зазвичай низьким, оскільки готівкові операції важко виявити, наявна інформація є недостатньою, і торговці можуть втрачати своїх клієнтів на користь конкурентів, які застосовують слабкіший контроль. Крім того, торговцю товарами високої вартості може бути важко розробити політику ПВК/ФТ в обмежених випадках, коли готівкова операція відбувається за межами граничного значення (тобто режим ПВК/ФТ поширюється не на сам сектор, а лише на торговців товарами високої вартості, які стикаються з готівковими операціями за межами граничного значення). З цієї причини деякі держави-члени розширили сферу дії до певних секторів, незалежно від використання готівкових коштів. Деякі держави-члени також вирішили застосувати загальний режим обмеження для готівкових коштів на цьому рівні граничного значення, аби зменшити ризик неефективного або обтяжливого застосування правил щодо належної перевірки клієнтів (CDD) з боку торговців товарами високої вартості. Однак це не пом'якшує ситуацій підприємств з високим оборотом готівки, які базуються на готівкових операціях нижчої суми або на повторній кількості готівкових операцій низької суми.

Крім того, підприємства з високим оборотом готівки є по суті ризикованими з огляду на відсутність норм щодо перевірки керівників таких підприємств на професійну придатність і доброчесність. Деякі підприємства з високим оборотом готівки є більш вразливими, ніж інші, оскільки вони є більш схильними до обміну готівки (роздрібна торгівля автотранспортом або ломбарди).

Висновки: на схильність до ризику ВК, пов'язаного з використанням підприємств з високим оборотом готівки, впливає наявність законних обмежень для готівкових коштів, які є ефективними для пом'якшення ризиків, але не завжди є достатніми. У транскордонному контексті, розмаїття нормативних положень про готівкові платежі є також фактором уразливості. За відсутності норм, рівень обізнаності сектора про ризики

є досить низьким, що призводить до подання підрозділам фінансової розвідки незначної кількості звітів про підозрілі операції. Можливості правоохоронних органів для розслідування є досить обмеженими. У цьому контексті, рівень вразливості до ВК, пов'язаної з використанням підприємств з високим оборотом готівки, вважається дуже значним (рівень 4).

Пом'якшувальні заходи:

- Комісія проаналізувала, чи слід швидкими темпами зміцнювати законодавчу базу ЄС щодо запобігання фінансуванню тероризму шляхом підвищення прозорості готівкових платежів за допомогою введення обмеження для готівкових платежів або будь-яким іншим відповідним способом.[27] Організована злочинність та фінансування тероризму покладаються на готівкові кошти для здійснення своєї незаконної діяльності та отримання вигоди від неї. Обмежуючи можливості використання готівкових коштів, ця пропозиція сприятиме припиненню фінансування тероризму та, зокрема, пов'язаної з відмиванням коштів діяльності,[28] оскільки потреба у використанні неанонімних платіжних засобів стримуватиме діяльність або полегшуватиме її виявлення та розслідування. У звіті зроблено висновок, що наразі не будуть пропонуватися жодні додаткові законодавчі акти стосовно цього питання.

- Комісія продовжуватиме здійснювати моніторинг застосування зобов'язань щодо ПВК/ФТ з боку торговців товарами, на які поширюється дія Директиви про боротьбу з відмиванням грошей, і надалі оцінюватиме ризики, які створюють провайдери послуг, що приймають готівкові платежі. Вона також оцінюватиме додану вартість та вигоду підпорядкування додаткових секторів положенням щодо ПВК/ФТ.

- У своїх національних оцінках ризиків держави-члени повинні враховувати ризики, що створюються готівковими платежами, аби визначити відповідні пом'якшувальні заходи для усунення ризиків. Держави-члени повинні розглянути можливість піпорядкування секторів, які є особливо схильними до ризиків відмивання коштів та фінансування тероризму, під дію режиму ПВК/ФТ на основі результатів своїх національних оцінок ризиків.

[27] Звіт Комісії до Європейського Парламенту і Ради щодо обмежень на готівкові платежі (COM(2018) 483 final) був представлений 12 червня 2018 року.

[28] Варто зазначити, що у вищезгаданому звіті Комісії стверджується, що *«...обмеження на готівкові платежі суттєво не запобігатимуть фінансуванню тероризму, але такі обмеження можуть бути корисними у боротьбі з відмиванням коштів»*.

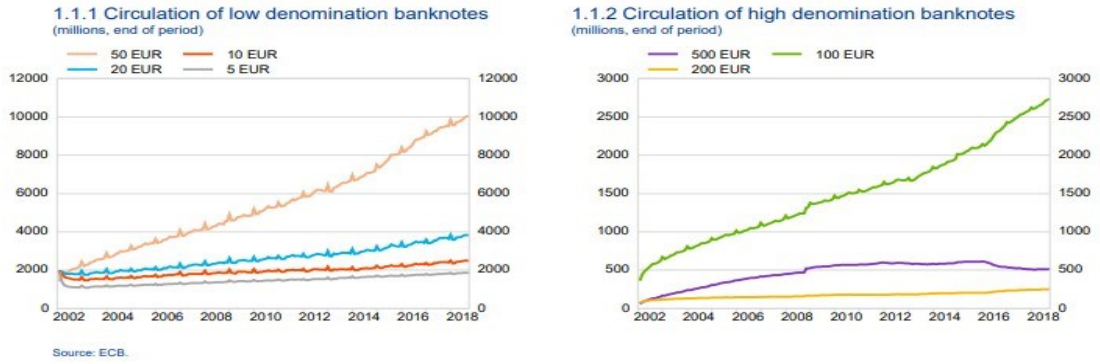
3. Банкноти високого номіналу

Продукт
Банкноти високого номіналу

Сектор
/

Загальний опис сектора та відповідного продукту/діяльності

Незважаючи на постійне зростання кількості методів на основі безготівкових платежів та поступове зменшення обсягів використання готівкових коштів для платежів, загальна вартість євро-банкнот в обігу продовжує зростати з кожним роком, перевищуючи темпи інфляції. Готівкові кошти широко використовуються для платежів низької вартості, і за оцінками, на їх використання для цілей операцій припадає приблизно одна третина банкнот, що знаходяться в обігу. Однак попит на банкноти високого номіналу, наприклад, банкноти номіналом 500 євро, які зазвичай не пов'язані з платежами, зберігається. Це аномалія, яка може бути пов'язана із злочинною діяльністю.



1.1.1 Обіг банкнот низького номіналу (млн., станом на кінець періоду)
1.1.2 Обіг банкнот високого номіналу (млн., станом на кінець періоду)

Джерело: ЄЦБ.

Мабуть, найважливішим висновком щодо готівкових коштів є те, що наявна інформація стосовно їх використання як для законних, так і для незаконних цілей, є недостатньою. Характер готівкових коштів та характер злочинних фінансів свідчить про недостатність або відсутність надійних даних про масштаби та використання готівкових коштів звичайними громадянами, не кажучи вже про злочинців.

Один з небагатьох наявних достовірних показників – обсяг та вартість банкнот, які були випущені та перебувають в обігу на території ЄС, залишає відкритими питання щодо використання великої частки готівкових коштів, особливо коли йдеться про банкноти номіналом 500 євро. Із загальної кількості банкнот на суму приблизно 1 трлн євро, які перебували в обігу станом на кінець 2014 року, використання значної частки таких банкнот залишається невідомим. Більше того, на одні тільки банкноти номіналом 500 євро припадає понад 30 % вартості всіх банкнот, що знаходяться в обігу, незважаючи на те, що вони не є звичайним засобом платежу. Хоча були припущення, що такі банкноти використовуються для накопичення, ці припущення не доведені. Навіть якщо це так, характер готівкових коштів, що накопичуються (злочинні або законні), є невідомим.

4 травня 2016 року Керівна рада Європейського центрального банку (ЄЦБ) прийняла рішення припинити виробництво та випуск банкнот номіналом 500 євро. Вона зробила це з огляду на

занепокоєння Європолу[29] та багатьох держав-членів тим, що ці банкноти сприяють незаконній діяльності. На підставі рішення ЄЦБ, з 27 квітня 2019 року ці банкноти більше не випускаються центральними банками в Єврозоні, але залишаються законним платіжним засобом і можуть використовуватися як засіб оплати.

Опис сценарію ризиків

Злочинці використовують банкноти високого номіналу, такі як банкноти номіналом 500 євро, для полегшення перевезення готівкових коштів (чим більшим є номінал, тим більше коштів можна перевезти за один раз).

Загальні зауваження

Цей сценарій ризиків по суті пов'язаний з використанням готівкових коштів/готівковими платежами, а також із сценарієм ризиків, пов'язаним з використанням підприємств з високим оборотом готівки.

Загроза

Фінансування тероризму

Оцінка загрози ФТ, пов'язаної з використанням банкнот високого номіналу, вказує на те, що терористичні групи неохоче використовують банкноти високого номіналу. До них не так легко отримати доступ, і враховуючи те, що їх можна досить легко виявити, вони не є привабливими для терористичних груп, головною метою яких є якомога швидше отримати готівкові кошти. Терористичні групи, як правило, надають перевагу банкнотам низького номіналу. Правоохоронні органи виявили декілька випадків, які демонструють, що намір та здатність не є насправді значними.

<u>Висновки:</u> У цьому контексті, рівень загрози ФТ, пов'язаної з використанням банкнот високого номіналу, вважається <u>помірно значним</u> (рівень 2).

Відмивання коштів

Оцінка загрози ВК, пов'язаної з використанням банкнот високого номіналу, вказує на те, що вони постійно використовуються злочинними організаціями для відмивання доходів, одержаних злочинним шляхом. Ризик, пов'язаний з використанням банкнот високого номіналу, не обмежується банкнотами номіналом 500 євро, і поки буде можливість збирати крупні суми готівкою, злочинні організації вважатимуть їх привабливими. Це не вимагає будь-якого планування чи складних операцій, тобто злочинці мають технічні навички, аби легко використовувати цей продукт. Це залишається «низькозатратною» операцією і дозволяє зберігати крупні суми у дуже малих обсягах, що є дуже привабливим для організованої злочинності. Правоохоронні органи повідомили, що деякі злочинні угруповання шукають банкноти номіналом 500 євро, сплачуючи додаткову ціну, аби отримати доступ до таких крупних банкнот; це ще раз підтверджує їх привабливість.

Самі по собі операції виявляють величезні суми готівкових коштів, переміщувані та приховувані злочинцями, які постійно інвестуються та інтегруються у правову економіку різноманітними способами, що позбавляє злочинців від громіздких запасів готівкових коштів, які можуть бути конфісковані. Ці методи вимагають від співучасників та задіяних посередників гарантувати, що їхнє включення у правову економіку не викликатиме підозр.

[29] https://www.europol.europa.eu/newsroom/news/europol-welcomes-decision-of-ecb-to-stop-printing-eur-500-notes

В ЄС використання готівкових коштів досі залишається основною причиною подання звітів про підозрілі операції у межах фінансової системи і складає 34 % усіх звітів.

Злочинці, які генерують готівкові надходження, прагнуть об'єднати та перемістити такі прибутки зі свого джерела, будь то для репатріації коштів або для їх переміщення у місце, де буде легше інтегрувати їх у правову економіку, можливо, завдяки переважному використанню готівки в економіці деяких юрисдикцій, більш слабкому нагляду за фінансовою системою або суворішим правилам банківської таємниці чи тому що вони можуть мати більший вплив в економічному та політичному істеблішменту.

Контрабанда готівкових коштів може відбуватися на інших етапах, а також використовується у правопорушеннях, які не відносяться до правопорушень, що генерують грошові кошти. Наприклад, у кіберзлочинах, таких як фішинг та хакерство, використовуються грошові «мули» для отримання та зняття сум, які були одержані обманним шляхом з банківських рахунків жертв, у готівковій формі. Після цього такі кошти надсилаються банківським переказом до інших юрисдикцій, де їх забирає готівкою певна кількість осіб, ймовірно, для подальшого транспортування.

Кур'єри готівкових коштів пов'язані із загрозою, яку представляють банкноти високого номіналу: 500 та 200 євро. Ці банкноти не використовуються в якості законного засобу платежу, і фактично у багатьох країнах Європи вони не приймаються в якості оплати. Банкноти високого номіналу використовуються злочинцями для зберігання вартості або для транспортування (менший обсяг високої загальної суми). Наприклад, у сейфі бельгійського підпільного оператора, виявленому під час розслідування відмивання доходів від продажу гашишу марокканських організованих злочинних груп, містилися банкноти номіналом переважно 500 та 200 євро на загальну суму 1 600 000 євро.

Підроблені євро-банкноти все ще незаконно продаються навалом за допомогою вантажних автомобілів та кур'єрами. Послуги поштових відправлень та бандеролей дедалі частіше використовуються для розповсюдження підроблених євро-банкнот, які продаються на онлайн-платформах. Особи, які займаються підробкою валют, продовжують вводити в обіг підроблені банкноти, купуючи товари низької вартості з використанням банкнот високого номіналу для отримання законної валюти.

<u>Висновки</u>: банкноти (номіналом 500 євро, але не виключно) постійно використовуються злочинними організаціями. Цей спосіб дій є широко використовуваним і низькозатратним. Для цілей ВК, вдаватися до зловживання досить легко, і це не вимагає спеціального планування чи знань. У цьому контексті, рівень загрози ВК, пов'язаної з використанням банкнот високого номіналу, вважається <u>дуже значним</u> (рівень 4).

Вразливість

Фінансування тероризму

Оцінка вразливості до ФТ, пов'язаної з використанням банкнот високого номіналу, вказує на те, що цей продукт є настільки ж вразливим до ФТ, як і до ВК з наступних причин:

а) схильність до ризику

Великий обсяг банкнот високого номіналу знаходиться в обігу, незважаючи на низьке використання у комерційних операціях. Готівкові кошти все ще дозволяють здійснювати операції у прискорений, анонімний та невідстежуваний спосіб.

b) обізнаність про ризики

Правоохоронні органи та підрозділи фінансової розвідки мають високий рівень обізнаності про ризики, як і зобов'язані суб'єкти, що підпадають під зобов'язання щодо ПВК/ФТ. Обізнаність секторів, які не підпорядковуються зобов'язанням щодо ПВК/ФТ або обмеженням щодо готівкових коштів, про ризики все ще залишається проблемою. Наявна література, особливо звіти Європолу, вказують на «сліпу пляму» в обізнаності про ризики (тобто в частині точного використання банкнот високого номіналу, відмінностей у випусках між державами-членами, виключень з ВВП). Існує дуже мало або взагалі відсутні достовірні дані про масштаби та використання готівкових коштів звичайними громадянами, не кажучи вже про злочинців.

c) законодавча база і засоби контролю

Навіть якщо для терористичних груп банкноти високого номіналу є менш привабливими, виявити їх досить складно, оскільки законодавча база ЄС щодо використання банкнот високого номіналу не гармонізована. Контроль є неоднаковим; дуже мало звітів подається підрозділам фінансової розвідки, і зазвичай вони не в змозі провести різницю між ВК та ФТ. На використання банкнот високого номіналу для цілей ВК може вплинути рішення ЄЦБ щодо поступового припинення використання банкнот номіналом 500 євро з огляду на визнані зв'язки із злочинною діяльністю. Однак коефіцієнт окупності, як правило, є досить низьким, і ці банкноти можуть ще довго використовуватися. Тому це не можна вважати негайним пом'якшувальним заходом.

<u>Висновки</u>: з точки зору вразливості, схильність до ризику є високою, рівень обізнаності є низьким, а існуючі засоби контролю не гармонізовані, що створює потенційні лазівки, коли під загрозою знаходяться транскордонні операції. У цьому контексті, рівень вразливості до ФТ, пов'язаної з використанням банкнот високого номіналу, вважається <u>дуже значним</u> (рівень 4).

Відмивання коштів

Оцінка вразливості до ВК, пов'язаної з використанням банкнот високого номіналу, вказує на такі особливості:

a) схильність до ризику

Банкноти високого номіналу дозволяють зберігати/вводити в обіг великі обсяги готівки у швидкий та анонімний спосіб. Великий обсяг банкнот високого номіналу знаходиться в обігу, незважаючи на низький рівень їх використання у комерційних операціях. Навіть якщо використання банкнот високого номіналу викликає занепокоєння, такі купюри необов'язково використовуються для платежів, а швидше для переміщення коштів. Великі суми можуть зберігатися у дуже малих обсягах. Їх не так легко виявити підрозділами фінансової розвідки та зобов'язаним суб'єктам.

b) обізнаність про ризики

Правоохоронні органи та підрозділи фінансової розвідки мають високий рівень обізнаності про ризики, як і зобов'язані суб'єкти, що підпадають під зобов'язання щодо ПВК/ФТ. Обізнаність секторів, які не підпорядковуються зобов'язанням щодо ПВК/ФТ або обмеженням щодо

готівкових коштів, про ризики все ще залишається проблемою. Наявна література, особливо звіти Європолу, вказують на «сліпу пляму» в обізнаності про ризики (тобто в частині точного використання банкнот високого номіналу, відмінностей у випусках між державами-членами, виключень з ВВП). Існує дуже мало або взагалі відсутні достовірні дані про масштаби та використання готівкових коштів звичайними громадянами, не кажучи вже про злочинців.

c) законодавча база і засоби контролю

На використання банкнот високого номіналу для цілей ВК може вплинути рішення ЄЦБ щодо поступового припинення використання банкнот номіналом 500 євро з огляду на визнані зв'язки із злочинною діяльністю. Однак коефіцієнт окупності, як правило, є досить низьким, і ці банкноти можуть ще довго використовуватися. Банкноти номіналом 500 євро залишаться законним платіжним засобом і тому можуть надалі використовуватися як засіб оплати і зберігати вартість. Тому це не можна вважати негайним пом'якшувальним заходом.

<u>Висновки:</u> аналогічно результатам оцінки вразливості до ФТ, пов'язаної з використанням банкнот високого номіналу, рівень вразливості до ВК, пов'язаної з такими продуктами, вважається <u>дуже значним</u> (рівень 4).

Пом'якшувальні заходи:

- Моніторинг коефіцієнта окупності банкнот номіналом 500 євро буде продовжено, як і оцінку змін у використанні банкнот номіналом 200 євро.

4. Готівкові платежі

Продукт
Готівкові платежі

Сектор
/

Загальний опис сектора та відповідного продукту/діяльності

Європейський центральний банк (ЄЦБ) провів всебічне дослідження[30] з метою аналізу використання готівки, карток та інших платіжних інструментів, які використовувалися у точках продажу (POS) споживачами Єврозони у 2016 році. Результати опитування показують, що у 2016 році готівка була домінуючим платіжним інструментом у пунктах продажу. У кількісному вираженні, 79 % усіх операцій здійснювалися з використанням готівкових коштів, що становить 54 % від загальної вартості всіх платежів. Картки були другим найбільш часто використовуваним платіжним інструментом у точках продажу; 19 % усіх операцій здійснювались за допомогою платіжних карток. У вартісному вираженні, це становить 39 % від загальної вартості, сплаченої у пунктах продажу.

Таким чином, готівка без сумніву залишається способом оплати, який обирають споживачі для операцій на незначні суми (тобто менше 20 євро).

Опис сценарію ризиків

Злочинцям часто приходиться використовувати значну частку готівкових коштів, які вони набули, для сплати за незаконний товар, який вони продали, для придбання наступних партій товару або для оплати різних витрат, понесених у зв'язку з транспортуванням товару до місця призначення.

Незважаючи на переваги та недоліки використання готівки (як докладно описано вище у цьому звіті) злочинними групами, вибір, як правило, невеликий. У злочинній економіці все ще переважною мірою використовується готівка. Це означає, що, незалежно від того, чи подобається їм це або ні, злочинці, які продають будь-який незаконний продукт, швидше за все, одержать плату готівкою. Чим успішнішими є злочинці і чим більше товару вони продають, тим більше готівки вони одержують. Це може заподіяти злочинцям неабиякі проблеми у використанні, зберіганні та розпорядженні своїми доходами. Однак, незважаючи на ці проблеми, готівка надає їм значні переваги.

Крім того, метою злочинців є відмити крупні суми готівкових коштів, одержаних злочинним шляхом, заявляючи, що ці кошти були одержані в результаті економічної діяльності. Вони можуть відмивати суми готівкових коштів шляхом обґрунтування їх походження на основі фіктивної економічної діяльності (як для товарів, так і для послуг). Терористи можуть фінансувати терористичну діяльність за допомогою часто невеликих сум готівкових коштів без будь-якої можливості їх відстеження (див. загальний опис у розділі про підприємства з високим оборотом готівки).

[30] *Використання готівки домогосподарствами в Єврозоні,* Документ неперіодичної серії ЄЦБ, випуск № 201/листопад 2017 року: https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op201.en.pdf

Загальні зауваження

Цей сценарій ризику по суті пов'язаний із сценаріями ризику підприємств з високим оборотом готівки та банкнот високого номіналу.

Загроза

Фінансування тероризму

Оцінка загрози ФТ, пов'язаної з готівковими платежами, вказує на те, що терористичні групи регулярно використовують готівкові кошти, оскільки такий спосіб дій є легкодоступним і низькозатратним. Готівка лежить в основі будь-якого незаконного продажу та незаконного придбання продуктів. Загалом, готівка є дійсно привабливою, її важко (навіть неможливо) виявити і вона не вимагає наявності спеціальних знань.

<u>Висновки</u>: на основі зворотного інформації, наданої правоохоронними органами та підрозділами фінансової розвідки, рівень загрози ФТ вважається <u>дуже значним</u> (рівень 4).

Відмивання коштів

Оцінка загрози ВК, пов'язаної з готівковими платежами, вважається подібною до оцінки загрози ФТ. Що стосується ВК, готівкові кошти також є переважним вибором серед злочинців, який дозволяє легко приховувати незаконні доходи, одержані злочинним шляхом, та швидко переміщувати кошти, в тому числі через кордон. Що стосується ФТ, для цього не потрібні спеціальні знання чи планування.

Незаконні готівкові кошти передаються посередникам для купівлі товарів у країнах, в яких немає або дуже мало обмежень для готівкових платежів. Продукти, що купуються, можуть мати високу вартість, наприклад, предмети розкоші, або на них може бути специфічний, але значний попит, наприклад, транспортні засоби (незалежно від того, чи є вони вживаними або преміум-класу, будівельні машини).

Зростає інтеграція готівки шляхом купівлі у законних торгових компаній товару, який експортується за ринковою ціною.

<u>Висновки</u>: на основі зворотної інформації, наданої правоохоронними органами та підрозділами фінансової розвідки, рівень загрози ВК вважається <u>дуже значним</u> (рівень 4).

Вразливість

Фінансування тероризму

Оцінка вразливості до ФТ, пов'язаної з готівковими платежами, вказує на такі особливості:

a) схильність до ризику

Готівкові платежі дозволяють здійснювати швидкі та анонімні операції. Рівень схильності до ризику є дуже високим, враховуючи те, що крупні суми можуть також переміщуватися через кордони за участі клієнтів та/або географічних зон високого ризику.

b) обізнаність про ризики

Правоохоронні органи та підрозділи фінансової розвідки мають високий рівень обізнаності про ризики, як і зобов'язані суб'єкти, що підпадають під зобов'язання щодо ПВК/ФТ. Обізнаність секторів, які не підпорядковуються зобов'язанням щодо ПВК/ФТ або обмеженням щодо готівкових коштів, про ризики все ще залишається проблемою. Наявна література, особливо звіти Європолу, вказують на «сліпу пляму» в обізнаності про ризики (тобто в частині точного використання банкнот високого номіналу, відмінностей у випусках між державами-членами, виключень з ВВП). Існує дуже мало або взагалі відсутні достовірні дані про масштаби та використання готівкових коштів звичайними громадянами, не кажучи вже про злочинців.

c) законодавча база і засоби контролю

Хоча обмеження щодо готівкових платежів можуть дозволити пом'якшити рівень вразливості, чинна законодавча база, пов'язана з обмеженнями щодо готівкових платежів, сильно відрізняється, залежно від держави-члена, тому контроль може бути відсутнім. З точки зору внутрішнього ринку, відмінності між законодавствами держав-членів щодо обмежень для готівкових коштів збільшують вразливість для внутрішнього ринку; злочинцям легше обходити контроль у своїй країні походження шляхом інвестування у підприємства з високим оборотом готівки в інших державах-членах, які мають слабкіший контроль/в яких відсутній контроль за обмеженнями для готівкових коштів.

Четверта директива про боротьбу з відмиванням грошей передбачає, що торговці товарами високої вартості, які приймають готівковий платіж у сумі понад 10 000 євро, підпадають під дію положень щодо ПВК/ФТ та повинні застосовувати вимоги щодо належної перевірки клієнтів (CDD). Це зобов'язання застосовується до будь-яких осіб, які торгують товарами, коли платіж здійснюється готівкою у сумі понад 10 000 євро, але воно не застосовується до послуг, крім послуг грального бізнесу, коли операції здійснюються на суму 2 000 євро. Такі граничні значення передбачені у Директиві 2018/843 (П'ята директива про боротьбу з відмиванням грошей).

Однак ефективність таких заходів все ще обмежена з огляду на кількість звітів про підозрілі операції. Обсяг звітів про підозрілі операції є зазвичай низьким, оскільки готівкові операції важко виявити, наявна інформація є недостатньою, і торговці можуть втратити своїх клієнтів на користь конкурентів, які застосовують слабкіший контроль. Для тих держав-членів, які подають звіти про валютні операції, у більшості випадках вони не пов'язані з жодним звітом про підозрілі операції, і аналіз не може бути здійснений (наприклад, крупні суми, зняті з банкомату, ініціюють подання звіту про валютні операції, але з цим не пов'язані жодні конкретні підозри, і підрозділ фінансової розвідки не може розпочати жодне розслідування).

Крім того, торговцю товарами високої вартості може бути важко розробити політику ПВК/ФТ в обмежених випадках, коли готівкова операція відбувається за межами граничного значення (тобто режим ПВК/ФТ поширюється не на сам сектор, а лише на торговців товарами високої вартості, які стикаються з готівковими операціями за межами граничного значення). З цієї причини деякі держави-члени розширили сферу дії до певних секторів, незалежно від використання готівкових коштів. Деякі держави-члени також вирішили застосувати загальний режим обмеження для готівкових коштів на цьому рівні граничного значення, аби зменшити ризик неефективного або обтяжливого застосування норм щодо належної перевірки клієнтів (CDD) з боку торговців товарами високої вартості. Однак це не пом'якшує ситуацій підприємств з високим оборотом готівки, які базуються на готівкових операціях нижчої суми або на повторній кількості готівкових операцій низької суми.

У будь-якому разі, деякі компетентні органи вважають, що навіть за наявності обмежень для готівкових платежів, приведення у виконання цих обмежень є дуже складним завданням і може обмежувати їх вплив на діяльність з ФТ.

Висновки: враховуючи той факт, що готівкові платежі можуть сприяти швидкому та анонімному здійсненню крупних операцій, в тому числі транскордонних, що з готівковими платежами можуть стикатися всі сектори і, навіть якщо вони усвідомлюють, що такі платежі створюють певні ризики, вони не мають засобів для їх пом'якшення (тому що немає жодної законодавчої бази/засобів контролю, або через те, що приведення у виконання засобів контролю є неефективним), рівень вразливості до ФТ, пов'язаної з готівковими платежами, вважається дуже значним (рівень 4).

Відмивання коштів

Оцінка вразливості до ВК, пов'язаної з готівковими платежами, свідчить про таке:

a) схильність до ризику

Сектор демонструє таку саму вразливість для ФТ, як і для ВК. Що стосується фінансування тероризму, готівкові платежі дозволяють здійснювати швидкі та анонімні операції для відмивання доходів від злочинної діяльності. Рівень схильності до ризику є дуже високим, враховуючи те, що крупні суми можуть також переміщуватися через кордони за участі клієнтів та/або географічних зон високого ризику.

b) обізнаність про ризики

Правоохоронні органи та підрозділи фінансової розвідки мають високий рівень обізнаності про ризики, як і зобов'язані суб'єкти, що підпадають під зобов'язання щодо ПВК/ФТ. Обізнаність секторів, які не підпорядковуються зобов'язанням щодо ПВК/ФТ або обмеженням щодо готівкових коштів, про ризики все ще залишається проблемою. Наявна література, особливо звіти Європолу, вказують на «сліпу пляму» в обізнаності про ризики (тобто в частині точного використання банкнот високого номіналу, відмінностей у випусках між державами-членами, виключень з ВВП). Існує дуже мало або взагалі відсутні достовірні дані про масштаби та використання готівкових коштів звичайними громадянами, не кажучи вже про злочинців.

c) законодавча база і засоби контролю

Хоча обмеження щодо готівкових платежів можуть дозволити пом'якшити рівень вразливості, чинна законодавча база, пов'язана з обмеженнями щодо готівкових платежів, сильно відрізняється, залежно від держави-члена, тому контроль може бути відсутнім. З точки зору внутрішнього ринку, відмінності між законодавствами держав-членів щодо обмежень для готівкових коштів збільшують вразливість для внутрішнього ринку; злочинцям легше обходити контроль у своїй країні походження шляхом інвестування у підприємства з високим оборотом готівки в інших державах-членах, які мають слабкіший контроль/в яких відсутній контроль за обмеженнями для готівкових коштів.

Обсяг звітування є дуже низьким, оскільки готівкові операції важко виявити. Для тих держав-членів, які подають звіти про валютні операції, у більшості випадках вони не пов'язані з жодним звітом про підозрілі операції, і аналіз не може бути здійснений (наприклад, крупні суми, зняті з банкомату, ініціюють подання звіту про валютні операції, але з цим не пов'язані жодні конкретні підозри, і підрозділ фінансової розвідки не може розпочати жодне розслідування).

У будь-якому разі, деякі компетентні органи вважають, що навіть за наявності обмежень для готівкових платежів, приведення у виконання цих обмежень є дуже складним завданням і може обмежувати їх вплив на діяльність з ВК.

<u>Висновки:</u> враховуючи той факт, що готівкові платежі можуть сприяти швидкому та анонімному здійсненню крупних операцій, в тому числі транскордонних, що з готівковими платежами можуть стикатися всі сектори і, навіть якщо вони усвідомлюють, що такі платежі створюють певні ризики, вони не мають засобів для їх пом'якшення (тому що немає жодної законодавчої бази/засобів контролю, або через те, що приведення у виконання засобів контролю є неефективним), рівень вразливості до ВК, пов'язаної з готівковими платежами, вважається <u>дуже значним (рівень 4)</u>.

Пом'якшувальні заходи:

- Комісія повинна продовжувати моніторинг застосування зобов'язань щодо ПВК/ФТ з боку торговців товарами, на яких поширюється дія Директиви про боротьбу з відмиванням грошей, і надалі оцінювати ризики, які створюють провайдери послуг, що приймають готівкові платежі. Вона також має оцінювати додану вартість та вигоду підпорядкування додаткових секторів нормам щодо ПВК/ФТ.

- У своїх національних оцінках ризиків держави-члени повинні враховувати ризики, що створюють готівкові платежі, аби визначити відповідні пом'якшувальні заходи для усунення ризиків. Держави-члени повинні розглянути можливість піпорядкування секторів, які є особливо схильними до ризиків відмивання коштів та фінансування тероризму, під дію режиму ПВК/ФТ на основі результатів їх національних оцінок ризиків.

5. Приватні банкомати

Продукт
Приватні банкомати

Сектор
/

Загальний опис сектора та відповідного продукту/діяльності

Правоохоронні органи звернули увагу на можливе зловживання касовими автоматами (банкоматами). Відповідно до отриманої інформації, юридична можливість приватних осіб купувати та орендувати банкомати в оптових постачальників створює лазівку, якою користуються злочинці.

Для багатьох продавців, власників клубів, барів та ресторанів встановлення одного такого банкомату стало бізнес-орієнтованим рішенням – клієнтам пропонується можливість зручно знімати готівку, а продавець максимально збільшує вірогідність того, що частина таких готівкових коштів буде витрачена на його бізнес.

Опис сценарію ризиків

а) Способи завантаження банкоматів

Одним із способів завантаження банкоматів є використання послуг компаній з управління готівкою/доставки готівки.

Продавці, які ведуть свій бізнес також можуть завантажувати готівку з власної каси. Це дозволяє торговцям ухилятися від сплати податків, збуваючи товар в обмін на готівку без видачі чеків. Вони просто поміщають свою чорну готівку у свій банкомат і чекають, коли її знімуть звичайні клієнти. Інформація про такі продажі ніколи не повідомляється податковому органу наприкінці року.

Третім і найбільш проблемним способом є завантаження банкомату готівкою, одержаною від злочинної діяльності. Зібрана у ході розслідування інформація свідчить про те, що у випадках, коли використовується готівка, одержана від злочинної діяльності, порядок дій є наступним: кур'єр доставляє власнику банкомату/торговцю готівку, одержану від злочинної діяльності. Така готівка може бути отримана в результаті різноманітної діяльності з генерування готівки, такої як незаконна торгівля наркотиками, нелегальна імміграція, торгівля людьми, трудова та сексуальна експлуатація, продаж підроблених контрабандних товарів, крадіжки, пограбування тощо. Готівка, одержана злочинним шляхом, завантажується у банкомат. Коли непідозрюючі клієнти або перехожі, яким потрібна готівка, використовують свої картки для зняття готівки, та сама сума списується з їхніх банківських рахунків і зараховується на рахунок власника банкомату/продавця. Після цього він може просто переказати гроші на будь-який рахунок, який контролюється злочинцем, сплативши встановлену комісію.

b) Відключення банківських рахунків та ризики інтернаціоналізації

Інтернаціоналізований, можливо, ще більш небезпечний сценарій ризиків має місце, коли відповідно до національних положень приватний суб'єкт, який купує банкомат, після його придбання має надати номер національного банківського рахунка, пов'язаного з банкоматом та його діяльністю, але торговець необов'язково повинен замовляти готівку для банкомату з того самого банківського рахунка, який пов'язаний з його банкоматом, або навіть з того самого банку.

За результатами огляду компаній, які пропонують послуги приватних банкоматів, є декілька основних постачальників, британських та американських,[31] яким вдалося вивести свій бізнес на міжнародний рівень.[32]

Важливі питання виникають стосовно рахунків, з якими пов'язані ці банкомати (що продаються європейськими та американськими компаніями та присутні у країнах ЄС). Якщо вони пов'язані з національним банківським рахунком в ЄС, але фізично перебувають в іншій країні, буде практично неможливо встановити походження готівки, що завантажується у такі банкомати.

c) Уникнення від сплати податків та шахрайство

Приватні банкомати також використовуються для ухилення від сплати податків та шахрайства, особливо, коли деякі оператори підприємств з високим оборотом готівки заохочують своїх клієнтів знімати готівку за послуги, за які не виставляються рахунки і які не обліковуються. Сума грошей, не включена у податкові надходження внаслідок ухилення від сплати податків та шахрайства з використанням приватних банкоматів, є значно вищою, ніж сума, яка була відмита.

d) Мікроструктурування за допомогою організованої злочинності

Що стосується відмивання грошей, приватні банкомати часто використовуються для «мікроструктурування» – внесення та зняття невеликих грошових сум, що відповідають звичайним сумам, що знімаються з банкоматів, які не виявляються банківським контролем. Учасники організованої злочинності здійснюватимуть велику кількість невеликих щоденних грошових депозитів на 100 чи більше банківських рахунків, використовуючи приватні банкомати, щоб уникнути виконання вимог щодо звітування щодо боротьби з відмиванням коштів.

Загальні зауваження

Приватні банкомати зазвичай розташовуються у підприємствах з високим оборотом готівки. Крім того, приватні банкомати можуть розташовуватися і в компаніях, які надають розрахунково-касові послуги, здійснюють обмін валюти, грошові перекази без відкриття банківських рахунків. Беручи до уваги той факт, що наявність банкомату в компанії, яка надає розрахунково-касові послуги, здійснює обмін валюти, грошові перекази без відкриття банківських рахунків є нелогічним з огляду на характер послуг такої компанії, а також той факт,

---

[31] Наприклад: YourCash Europe – компанія, яка контролює 32 % ринку безкоштовних у використанні банкоматів на території Сполученого Королівства – має філії у Нідерландах, Бельгії та Ірландії, а також банкомати у додаткових юрисдикціях. Крім того, Cardtronics (деякі філії працюють під торговою маркою DC Payments) працює в 11 країнах. Окрім зазначених філій за межами Європи (Південна та Північна Америка, Нова Зеландія та Австралія, Південна Африка) та філії у Сполученому Королівстві, вони працюють в Ірландії, Німеччині, Польщі та Іспанії.

[32] Як додатковий приклад, розділ про місцезнаходження банкоматів на веб-сайті LINK: (https://www.link.co.uk/consumers/locator/) свідчить про те, що в Бельгії, Чехії, Франції, Німеччині, Гібралтарі, Італії, Нідерландах, Ірландії та Швейцарії, а також на острові Гернсі, острові Мен та Джерсі фізично присутні приватні банкомати Сполученого Королівства.

що багато законних компаній з боку «хаваладарів»[33] управляють компаніями, які надають розрахунково-касові послуги, здійснюють обмін валюти, грошові перекази без відкриття банківських рахунків, ризик зловживання може бути легко ідентифікований.

Загроза

Фінансування тероризму

Наразі існує лише декілька спеціальних оцінок загрози ФТ, пов'язаної з приватними банкоматами. Тим не менш, комбінована оцінка щодо готівкових платежів, а також аналіз щодо кур'єрів готівкових коштів свідчать про те, що такий порядок дій є широко доступним і низькозатратним.

Також може мати місце загроза ввезення готівкових коштів на територію ЄС з третіх країн, зокрема, з країн, які є схильними до ризиків ФТ, або із зон конфлікту. Виявлено випадки ввезення менших сум з інтеграцією готівки, що ввозиться з третіх країн, у фінансову систему/правову економіку ЄС (аналізуються в окремому розділі нижче).

<u>Висновки</u>: на основі зворотної інформації, наданої правоохоронними органами та підрозділами фінансової розвідки, рівень загрози ФТ вважається <u>дуже значним</u> (рівень 4).

Відмивання коштів

Оцінка загрози ВК, пов'язаної з використанням приватних банкоматів, вказує на те, що такий спосіб дій використовується злочинцями, оскільки він є життєздатним, досить привабливим та безпечним рішенням. Це найпростіший спосіб уникнути сплати податків та приховати незаконний дохід, одержаний від злочинної діяльності. Однак, що стосується ФТ, використання цього способу потребує помірного рівня знань, аби мати змогу керувати бізнесом і не бути виявленими.

<u>Висновки</u>: на основі зворотної інформації, наданої правоохоронними органами та підрозділами фінансової розвідки, рівень загрози ВК вважається <u>дуже значним</u> (рівень 4).

Вразливість

Фінансування тероризму

Оцінка вразливості до ФТ, пов'язаної з приватними банкоматами, вказує на те, що основні фактори пов'язані з ризиками, які створюються готівковими коштами.

a) схильність до ризику

Оцінка вразливості до ФТ, пов'язаної з приватними банкоматами, по суті пов'язана з оцінкою вразливості, пов'язаної з використанням готівкових коштів/готівковими платежами загалом, і може мати те саме обґрунтування. Приватні банкомати дозволяють обробляти величезну кількість анонімних операцій, які вимагають лише початкових інвестицій. Тому вони мають високу схильність до ризику.

b) обізнаність про ризики

[33] Див., розділ про систему «хавала».

Рівень обізнаності про ризики є досить низьким.

c) законодавча база і засоби контролю

Діючі законодавчі бази є різними в різних державах-членах, тому контроль може бути відсутнім.

<u>Висновки:</u> вразливість, пов'язана з використанням приватних банкоматів, по суті пов'язана з вразливостями, пов'язаними з використанням готівкових коштів загалом.
З огляду на широке використання готівки в економіках ЄС і той факт, що сектор, здається, не усвідомлює цього ризику, рівень вразливості до ФТ вважається <u>дуже значним</u> (рівень 4).

Пом'якшувальні заходи:

Компанії, які мають приватні банкомати, становлять підвищений ризик для банків і повинні вважатися компаніями високого ризику при оцінці ризику ВК. Ризики для банків є не тільки фінансовими, а і репутаційними.

- По-перше, клієнти, які мають приватні банкомати або експлуатують їх, мають бути належним чином ідентифіковані.

- Після того, як банк ідентифікує власника або оператора банкомата, він повинен отримати додаткову інформацію для належного розуміння власника/оператора банкомата, а також для розуміння процедур, здійснюваних власником банкомата.

- Після отримання достатньої інформації банк-спонсор повинен здійснити процедуру для моніторингу рахунків власників банкоматів. Інформація, отримана під час здійснення процедури належної перевірки, має дозволити банку визначити необхідний обсяг моніторингу, а також періодичність його здійснення.

- Держави-члени повинні гарантувати зобов'язання щодо реєстрації, обмеження права власності, моніторингу або перевірки приватних банкоматів – до (включно) зобов'язання щодо підключення банкоматів до банківського рахунка держави-члена, в якій вони фізично розташовані.

ФІНАНСОВИЙ СЕКТОР

1. Депозити на рахунках

Продукт
Депозити на рахунках

Сектор
Кредитні та фінансові установи

Загальний опис сектора та відповідного продукту/діяльності

Що стосується тенденцій, за даними Європейської банківської федерації з 1998 року, внутрішні зобов'язання або зобов'язання на рівні Єврозони щодо депозитів зросли в ЄС на 3,1 % та досягли 23,6 трлн євро у грудні 2017 року (17,5 трлн євро в Єврозоні та 5,3 трлн євро у решті держав-членів ЄС). Це був найвищий зафіксований рівень, з попереднім піком у 2012 році на рівні 23,1 трлн євро. Депозити від інших грошово-кредитних фінансових установ вперше з 2011 року зросли до 7,1 трлн євро.

Загальна сума депозитів від установ, які не є грошово-кредитними фінансовими установами, за винятком центральних органів влади, зросли на 2,5 % у 2017 році і досягли 16,3 трлн євро в ЄС наприкінці 2017 року, при цьому 12,1 трлн євро депозитів надійшли з Єврозони.

Зростання було обумовлене збільшенням депозитів від домогосподарств, які зросли на 2,9 % у річному обчисленні і досягли 9,1 трлн євро, а також депозитів від нефінансових корпорацій, які зросли на 6,7 % і досягли 3,2 трлн євро.

Опис сценарію ризиків

Злочинці розміщують доходи від злочинної діяльності у фінансовій системі через регульований кредитний та фінансовий сектор, аби приховати їх незаконне походження. Терористи, прихильники або фасилітатори вносять кошти із законних чи злочинних джерел у фінансову систему з метою їх використання для терористичних цілей.

Механізми грошових «мулів» можуть використовуватися для переказу надходжень з банківського сектора за допомогою особистих рахунків, через кіберзлочинність (шахрайство, фіктивні банківські веб-сайти тощо) або через послуги переказу грошових коштів.

«З'єднуючі рахунки» також використовуються для відмивання грошей. Це рахунки юридичних або фізичних осіб в ЄС, призначені для переказу коштів у країни, які не є членами ЄС.

Загроза

Фінансування тероризму

Оцінка загрози фінансування тероризму, пов'язаної з депозитами на рахунках, вказує на те, що такий сценарій ризику стосується як розміщення, так і зняття коштів (тобто депозити на рахунках та використання такого рахунка шляхом зняття цих коштів або їх переказу на інші банківські рахунки).

Депозити на рахунках часто використовуються терористами, а також родичами/друзями; це розширює сферу аналізу наміру та здатності.[34] Крім того, правоохоронні органи повідомляють про використання терористами підроблених або викрадених документів для відкриття банківських рахунків. Згідно з інформацією компетентних органів, іноземні терористи-бойовики зазвичай знімають депозити з банківських рахунків через банкомати, розташовані у країнах високого ризику, які не є членами ЄС, або у зонах конфлікту загалом чи у прикордонних країнах. Терористи за межами зон конфлікту також знімають кошти через банкомати, щоб сплатити готівкою частину витрат, пов'язаних з їхніми операціями. У будь-якому разі використання депозитних рахунків для цілей ФТ у зонах конфлікту може бути ускладнено відсутністю доступу до коштів, особливо у разі обмеження доступу до банкоматів чи діючої банківської мережі. Джерело коштів, що зберігаються на банківських рахунках, може мати як законне, так і незаконне походження.

Загалом, використання депозитних рахунків є легкодоступним, особливо у разі використання законних коштів, тому вони не викликають жодних підозр при відкритті банківського рахунка. Складається враження, що терористичні групи не стикаються з жодними проблемами у приховуванні реального бенефіціара коштів або справжньої мети операції (призначення коштів), з огляду на те, що вони можуть включати членів родини або родичів у ланцюг права власності. Для цього потрібно принаймні базове планування та базові знання того, як працюють банківські системи. Одночасно з цим, зняття готівки (одразу після його здійснення) дозволяє транскордонні переміщення, що робить такий сценарій ризику досить привабливим.

Висновки: терористичні групи досить часто використовують депозити на рахунках, щоб легко вносити готівку на банківські рахунки та знімати гроші для цілей терористичної діяльності, хоча це вимагає певних базових знань та здатності планувати, аби забезпечити видимість законного внесення коштів. Як результат, цей метод є досить привабливим для терористичних груп. У цьому контексті, рівень загрози фінансування тероризму, пов'язаної з депозитами на рахунках, вважається значним/дуже значним (рівень 3/4).

Відмивання коштів

Оцінка загрози відмивання коштів, пов'язаної з депозитами на рахунках, вказує на те, що такий сценарій ризику стосується як розміщення, так і зняття коштів (тобто депозити на рахунку та подальше використання такого рахунка, зняття коштів з такого депозитного рахунка або переказ коштів для маскування їх походження).

[34] Аналіз наміру та здатності описаний у методології:

- Компонент загрози *«намір»* має покладатися на відомий намір (конкретне виникнення загрози), успішний або зірваний, та очевидну привабливість ФТ завдяки використанню спеціального методу/механізму. Хоча загальний намір щодо ФТ оцінюється як постійно високий, намір використання конкретного алгоритму дій/методу відрізняється, залежно від привабливості алгоритму дій та відомого існування гарантій протидії щодо ПФТ.
- Компонент загрози *«здатність»* означає здатність груп загроз (терористів) успішно переказувати незаконні або законні кошти для фінансової підтримки терористичної мережі.

  Оцінка компонента «здатність» має враховувати простоту використання конкретного алгоритму дій для ФТ (необхідні технічні знання та підтримка), доступність та відповідні витрати (фінансова спроможність) на використання конкретного алгоритму дій.

Депозити на рахунку часто використовуються організованими злочинними організаціями, а також родичами/близькими особами, що розширює сферу аналізу наміру та здатності.[35] Правоохоронні органи повідомляють про часте використання цього методу, оскільки це один з найпростіших способів інтегрувати незаконні кошти у фінансову систему. Хоча у разі незначних грошових сум глибоке планування та знання того, як працюють банківські системи, можуть не знадобитися, у разі складного випадку відмивання коштів, що передбачає передачу внесених на рахунок коштів через ланцюг складних операцій, необхідні більш глибокі знання, тому злочинці можуть використовувати наявні знання посередників.

Висновки: У світлі вищезазначених загроз, зокрема, використання злочинними організаціями, рівень загрози відмивання коштів, пов'язаної з депозитами на рахунках, вважається дуже значним (рівень 4).

Вразливість

Фінансування тероризму

Оцінка вразливості до фінансування тероризму, пов'язаної з депозитами на рахунках, пов'язана з розміщенням та зняттям коштів.

a) схильність до ризику

Банки і досі наражаються на ризики фінансування тероризму: депозити на рахунках є найпростішим способом введення грошей у фінансову систему. Що стосується ризику фінансування тероризму, схильність до ризику є навіть вищою, коли походження коштів є законним. Використання коштів на депозитних рахунках для терористичних цілей важко виявити, оскільки терористичні групи зазвичай використовують незначні грошові суми. Що стосується пересилання грошей у зони конфлікту, ризик фінансування тероризму є нижчим для депозитів на рахунках, оскільки злочинці надають перевагу використанню інших продуктів, таких як послуги переказу грошових коштів або електронні продукти електронних грошей.

b) обізнаність про ризики

Обізнаність кредитних та фінансових установ про ризики, як правило, є належною, і банківський сектор видав настанови щодо виявлення відповідних тривожних сигналів, що свідчать про випадки фінансування тероризму. Однак системи та перевірки, які вводяться компаніями для пом'якшення ризику фінансування тероризму, є схожими і часто аналогічними перевіркам, що здійснюються для цілей відмивання коштів. Органи нагляду та правоохоронні органи обізнані про вразливості до фінансування тероризму і активно взаємодіють із сектором.

[35] Див. попередню виноску.

c) законодавча база і перевірки

Депозити на рахунках охоплені законодавчою базою щодо протидії відмиванню коштів (ПВК) та фінансуванню тероризму (ФТ), починаючи з першого законодавчого акту щодо ПВК/ФТ на рівні ЄС у 1991 році. Здійснювані перевірки зазвичай вважаються ефективними, хоча санкційна перевірка не замінює ефективних перевірок щодо ПФТ. Фінансові санкції спрямовані на фізичних осіб або групи, які, як відомо, становлять загрозу, тоді як ризик фінансування тероризму часто походить від фізичних осіб, що не підпадають під санкційний режим. Ось чому перевірки щодо ПВК/ФТ на основі ризиків та, зокрема, моніторинг операцій є ключовими для ефективної боротьби з фінансуванням тероризму.

Зазвичай банки не мають доступу до відповідної інформації, яка може допомогти їм ідентифікувати ризики фінансування тероризму ще до того, як вони матеріалізуються, оскільки такою інформацією часто володіють правоохоронні органи. Аналогічно, зусиллям правоохоронних органів щодо припинення терористичної діяльності і мереж може перешкоджати їх нездатність отримати інформацію про фінансові потоки, які можуть бути забезпечені лише компаніями. Наразі мають місце ініціативи на національному та наднаціональному рівнях для перевірки того, як правоохоронні органи можуть надавати компаніям більш конкретну та змістовну інформацію про конкретних осіб, які становлять інтерес, дозволяючи компаніям зосередити моніторинг операцій на таких особах.

Висновки: схильність до ризику може вважатися досить високою, тому сектор, незважаючи на належний рівень обізнаності, потребує підвищення ефективності перевірок для пом'якшення ризику фінансування тероризму. Співпраця з правоохоронними органами є надзвичайно важливою у цій галузі. Як результат, рівень вразливості до фінансування тероризму, пов'язаної з депозитами на рахунках, вважається значним (рівень 3).

Відмивання коштів

Вразливість до відмивання коштів в основному залежить від ефективності систем моніторингу для виявлення підозрілих операцій, коли готівка вноситься на банківські рахунки, або операцій, пов'язаних з готівковими коштами. Рівень вразливості є таким же високим, коли йдеться про перекази коштів від клієнтів з високим ризиком.

a) схильність до ризику

Депозити на рахунках є найбільш простим способом введення грошових коштів від незаконної діяльності у фінансову систему. Мають місце великі обсяги продуктів, де у разі використання готівки не завжди можна простежити походження коштів. Хоча депозити є досить поширеною практикою для кредитних та фінансових установ, вони представляють велику кількість операцій, в яких можуть брати участь клієнти різного типу. Деякі клієнти можуть представляти високий ризик, оскільки вони є впливовими політичними особами або тому що вони ідентифікуються як клієнти з високим ризиком (тобто деякі банківські рахунки нерезидентів у банках ЄС).

Більшість органів нагляду вважають широке використання готівки у деяких підсекторах та у деяких державах-членах одним із факторів, що сприяють схильності сектора до ризику відмивання коштів, особливо, якщо сектор представлений великою кількістю роздрібних банків. Органи нагляду також вважають, що транскордонна діяльність схильна до значного та дуже значного ризику відмивання коштів, особливо в тих державах-членах, які вважаються міжнародними фінансовими центрами. Клієнти-нерезиденти з юрисдикцій високого ризику та офшорні компанії також сприяють підвищенню ризику в цьому секторі. У деяких державах-членах, де внутрішня депозитна база є невеликою по відношенню до розміру фінансового сектора, депозити нерезидентів, особливо з країн, що межують з країнами, які не є членами ЄС,

є привабливим джерелом фінансування. Однак досвід останніх років показав, що такі депозити, залежно від юрисдикції джерела та інших обставин, часто вимагали посиленого контролю в області ПВК, який був відсутній або не відповідав рівню ризику, який вони створювали. Надмірний ризик, з якими стикаються кредитні установи, призвів до значного впливу на юрисдикції ЄС потоків коштів потенційно підозрілого походження з третіх країн. Останнім часом спостерігається тенденція до постійного зменшення частки депозитів нерезидентів у юрисдикціях ЄС завдяки добровільному зниженню ризиків банківським сектором, а також державній політиці відповідних юрисдикцій ЄС.

b) обізнаність про ризики

Обізнаність про ризики є загалом належною, оскільки сектор випустив настанови щодо виявлення відповідних тривожних сигналів стосовно відмивання коштів. Хоча в банківському секторі існує високий ризик відмивання коштів, він також має належні інструменти для його виявлення. Це підтверджується високим рівнем звітування. Підрозділи фінансової розвідки та правоохоронні органи також добре обізнані про вразливості сектора та активно взаємодіють із сектором.

Що стосується органів нагляду, хоча банківський сектор вважається по суті ризикованим, оскільки кредитні установи часто є першою вхідною точкою у загальний сектор фінансових послуг, концентрація компаній, що вважаються компаніями дуже високого ризику, є порівняно невеликою. Однак останнім часом скандали в європейських банках показали, що слабкі місця, пов'язані з клієнтами з колишніх радянських республік, посилюють вразливість до відмивання коштів.

c) законодавча база і перевірки

Депозити на рахунках охоплені законодавчою базою щодо ПВК/ФТ, починаючи з першого законодавчого акту щодо ПВК/ФТ на рівні ЄС у 1991 році. Здійснювані перевірки вважаються ефективними, але може виникнути потреба у тематичному нагляді для перевірки ефективності систем моніторингу, що використовуються для виявлення підозрілих готівкових операцій, особливо у разі залучення юридичних суб'єктів та юридичних утворень. Органи нагляду також занепокоєні перевірками, здійснюваними кредитними установами для управління ризиками, пов'язаними з клієнтами, які включають складні офшорні структури; зокрема, перевірки з метою ідентифікації та верифікації особи бенефіціарних власників вважаються недостатньо надійними.

Висновки: притаманний ризик відмивання коштів, пов'язаний з депозитами, пом'якшується кредитними установами належним чином. Однак мають місце певні занепокоєння щодо ефективності перевірок, зокрема, перевірок клієнтів зі складними офшорними структурами та іноземних замовників з юрисдикцій високого ризику. У цьому контексті, рівень вразливості до відмивання коштів, пов'язаної з депозитами на рахунках/роздрібним банкінгом, вважається значним (рівень 3).

Пом’якшувальні заходи:

Для Комісії:

- глибокий огляд транспозиції П’ятої директиви про боротьбу з відмиванням грошей з акцентуванням уваги на положеннях стосовно інформації про бенефіціарне право власності, включаючи взаємозв’язок реєстрів бенефіціарних власників на рівні ЄС;

- єдині практики електронної ідентифікації для фінансового сектора та запровадження стандартів для виконання зобов’язань щодо належної перевірки клієнтів з компаніями Reg-Tech;

- сприяння співпраці між правоохоронними органами та фінансовими установами для підвищення ефективності систем оповіщення про випадки фінансування тероризму на наднаціональному рівні.

Для держав-членів/компетентних органів:

· співпраця публічно-приватного сектора для обміну інформацією, пов’язаною з фінансуванням тероризму;

· тематичні перевірки з фокусуванням уваги на:

  - оцінці ефективності систем моніторингу для готівкових операцій та розміщення коштів на банківських рахунках, пов’язаних з одночасним переказом коштів у країни з високим рівнем ризику, які не є членами ЄС;

  - ефективність належної перевірки клієнтів та розширеної належної перевірки клієнтів для юридичних суб’єктів та юридичних утворень.

2. Сектор інституційних інвестицій – Банкінг

Продукт
Депозити на рахунках

Сектор
Кредитні установи – Інституційні інвестиції

Загальний опис сектора та відповідного продукту/діяльності

Сектор управління активами ЄС складається з двох взаємнодоповнюючих елементів. Перший елемент представлений пайовими інвестиційними фондами, фондами Організації колективного інвестування в обігові цінні папери (UCITS) (9,7 трлн євро активів під управлінням у 2017 році). Другий елемент включає альтернативні інвестиційні фонди (станом на кінець 2017 року чиста вартість активів альтернативних інвестиційних фондів становила 4,9 трлн євро), такі як хедж-фонди (11 %), фонди приватного капіталу (4 %), фонди фондів (16 %) та фонди нерухомості (11 %). Станом на кінець 2017 року активи під управлінням в ЄС перевищили граничне значення у розмірі 15 трлн євро. Сектор управління активами ЄС обслуговує як роздрібних клієнтів, які зазвичай представлені домогосподарствами та фізичними особами з високим чистим капіталом, так і інституційних клієнтів. Інституційними клієнтами є, наприклад, страхові компанії та пенсійні фонди, на які станом на кінець 2016 року припадало відповідно 25 % та 28 % загальних активів під управлінням в ЄС.

Опис сценарію ризиків

Існує декілька сценаріїв, коли злочинці можуть вчинити зловживання щодо інвесторів або фінансових ринків, наприклад, шляхом інтеграції доходів, таких як право власності на акції, з метою приховування бенефіціарного права власності за допомогою шахрайства або ринкових махінацій (що включають інсайдерську діяльність, ринкові маніпулювання та незаконне розголошення внутрішньої інформації, які підпадають під дію Регламенту про зловживання на ринку ЄС[36] та Директиви про кримінальні санкції ЄС щодо ринкових зловживань[37]), брокерських рахунків, інвестицій для обґрунтування злочинних доходів як прибутку, предикатного інвестиційного шахрайства або розміщення надходжень шляхом використання спеціальних фінансових послуг з високим коефіцієнтом окупності.

Загальні зауваження

Цей сценарій ризику може вважатися пов’язаним зі сценарієм для інвестицій, здійснюваних брокерами. Що стосується вразливості до відмивання коштів, вважається, що рівень ризику для брокерів є вищим.

[36] Регламент (ЄС) № 596/2014 Європейського Парламенту та Ради від 16 квітня 2014 року про зловживання на ринку (регламент про зловживання на ринку) і про визнання такими, що втратили чинність, Директиви 2003/6/ЄС Європейського Парламенту та Ради і Директив Комісії 2003/124/ЄС, 2003/125/ЄС та 2004/72/ЄС, Текст, що має значення для ЄЕП; OB L 173, 12.06.2014, с. 1-61.
[37] Директива 2014/57/ЄС Європейського Парламенту та Ради від 16 квітня 2014 року про кримінальні санкції щодо ринкових зловживань (директива про зловживання на ринку); OB L 173, 12.06.2014, с. 179-189.

Загроза

Фінансування тероризму

Рівень загрози фінансування тероризму, пов'язаної з інституційними інвестиціями, може бути значним у разі інвестування великих обсягів законних коштів для фінансування тероризму, але якщо йдеться про генерування невеликих сум для здійснення терористичних атак, загроза фінансування тероризму не є значною для такого продукту/сектора.

Висновок: рівень загрози фінансування тероризму, пов'язаної з інституційними інвестиціями через банки, вважається незначним (рівень 1).

Відмивання коштів

Зростаюча роль фасилітаторів у схемах відмивання коштів може збільшити схильність сектора до таких загроз, хоча для їх реалізації потрібні знання і технічні навички. Злочинні організації можуть покладатися на таких фасилітаторів для відмивання доходів від незаконної діяльності. Хоча за допомогою цього процесу можна зібрати великі суми коштів, не так легко отримати доступ до нього, він не є фінансово життєздатним (залежно від якості інвестицій) і у будь-якому разі вимагає знань і технічних навичок. Тому злочинні організації не надають перевагу подібному сценарію ризиків, хоча роль фасилітаторів є важливою при створенні непрозорих структур для приховування доходів від злочинної діяльності.

Тим не менш, протягом останніх декількох років було ідентифіковано кілька методів переміщення крупних незаконних потоків, розроблених висококваліфікованими фасилітаторами:

- клієнти ринку капіталу, що здійснюють майбутні позабіржові свопи через біржі та використовують незаконні кошти для розрахунків після настання дати платежу;
- одночасне придбання, передача та продаж цінних паперів через юрисдикції двома, здавалося б, непов'язаними, але взаємоконтрольованими суб'єктами;
- клієнти з фіксованим доходом на ринку капіталу, які здійснюють продаж облігацій від імені організованих злочинних груп, використовуючи незаконні кошти для придбання облігацій, а потім інтегрують кошти у фінансові установи після продажу таких облігацій.

Висновки: у цьому контексті, рівень загрози відмивання коштів, пов'язаної з інституційними інвестиціями через банки, вважається значним (рівень 3).

Вразливість

Фінансування тероризму

Вразливість до фінансування тероризму, пов'язана з інституційними інвестиціями, становить незначний ризик. Фактори ризику (продукти, клієнти, географічні зони та канали доставки) не сприяють використанню цього продукту/сектора для цілей фінансування тероризму. Злочинці зазвичай не мають досвіду для доступу до сектора, в той час як низькі обсяги грошових коштів, які використовуються у терористичних атаках, зробили інші сектори більш привабливими для їх цілей.

Висновок: у світлі вищезазначеного, рівень вразливості до фінансування тероризму, пов'язаної з інституційними інвестиціями через банки, вважається незначним (рівень 1).

Відмивання коштів

Оцінка вразливості до відмивання коштів, пов'язаної з інституційними інвестиціями через банки, вказує на таке:

a) схильність до ризику

Основним фактором, що пом'якшує ризик відмивання коштів, є низький рівень операцій на основі готівкових коштів, незважаючи на те, що цей сектор стикається з клієнтами високого ризику, включаючи впливових політичних осіб, в той час як обсяг і рівень транскордонних операцій є високим. Для одержання доступу до сектора, злочинці мають вводити гроші через банківську систему, а приховування незаконних коштів через непрозорі структури вимагає високого рівня знань. Тому банки є першим бар'єром, який пом'якшує ризик відмивання коштів.

b) обізнаність про ризики

Рівень обізнаності про ризики у секторі є невисоким, якщо операції здійснюються за межами банківського сектора. Це пояснюється тим, що компанії зазвичай покладаються на банки для здійснення належної перевірки клієнтів та моніторингу у разі внесення грошових коштів на банківські рахунки.

Органи нагляду вважають загальний ризик сектора помірно значним; однак профіль ризику на рівні компанії вказує на те, що значна частина компаній класифікується як такі, що мають незначний ризик. Незважаючи на це, більшість органів нагляду вважають, що цей сектор представляє дуже значний транскордонний ризик. Ще одним ключовим ризиком, з яким стикається цей сектор, є узгодження стандартів щодо протидії відмиванню коштів у країнах реєстрації та приймаючих державах-членах, якщо філії групи розташовані у різних країнах.

За даними підрозділів фінансової розвідки, кількість звітів про підозрілі операції є досить низькою порівняно з обсягом відповідних операцій, тому що цей сектор більш знайомий з виявленням випадків шахрайства, таких як інсайдерська торгівля або зловживання на ринку, ніж з підозрами щодо відмивання коштів. Одночасно з цим, відповідні фінансові операції є більш складними, а підозрілі операції, ймовірно, не так легко можуть бути виявлені зобов'язаними суб'єктами.

У цьому секторі також спостерігається значний конфлікт інтересів між занепокоєнням з приводу відмивання коштів та необхідністю залучення клієнтів, деякі з яких представляють високий ризик відмивання коштів, таких як впливові політичні особи, клієнти з країн високого ризику, які не є членами ЄС, а також клієнти з високим рівнем доходу. У цьому сенсі той факт, що послуга надається брокером, впливає на рівень вразливості до відмивання коштів, роблячи його вищим, ніж рівень вразливості стосовно кредитних установ.

c) законодавча база і перевірки

Інституційні інвестиції через банки підпадають під дію вимог щодо ПВК/ФТ на рівні ЄС. У сфері інвестицій менеджер клієнта зацікавлений у підтриманні ділових відносин (винагорода/заробітна плата), і це може призвести до того, що він втратить пильність під час здійснення належної перевірки клієнтів.

Органи нагляду вважають, що неналежні перевірки обмежують ефективність звітування про підозрілі операції та ефективність чинних політик та процедур моніторингу, включаючи моніторинг операцій. Навпаки, більшість порушень, виявлених під час перевірок, вважалися незначними. Найпоширенішим висновком були неналежні перевірки щодо впливових політичних осіб.

Висновки: схильність до ризику є високою завдяки характеру клієнтів та великим сумам, пов'язаним з операціями. Однак притаманний ризик пом'якшується завдяки низькому рівню операцій на основі готівкових коштів та завдяки банківським перевіркам боротьби з відмиванням коштів, якщо інвестиційні послуги надаються кредитними установами. Тим не менш, використання непрозорих структур або складних схем може збільшити вразливість, якщо зобов'язані суб'єкти не матимуть ресурсів для виявлення та звітування перед підрозділами фінансової розвідки. Зважаючи на це, рівень вразливості до відмивання коштів, пов'язаної з інституційними інвестиціями, що надаються через банківські установи, вважається помірно значним/значним (рівень 2/3).

Пом'якшувальні заходи:

Для Комісії:

- глибокий огляд транспозиції П'ятої директиви про боротьбу з відмиванням грошей з акцентуванням уваги на положеннях стосовно інформації про бенефіціарне право власності, включаючи взаємозв'язок реєстрів бенефіціарних власників на рівні ЄС;

- єдині практики електронної ідентифікації для фінансового сектора та запровадження стандартів для виконання зобов'язань щодо належної перевірки клієнтів з компаніями Reg-Tech.

Для держав-членів/компетентних органів:

- набрання чинності Директивою 2018/822/ЄС від 2020 року, згідно з якою посередники зобов'язані подавати інформацію про транскордонні податкові механізми своїм національним органам;

- поглиблення та поліпшення впровадження реєстрів бенефіціарних прав власності та взаємозв’язку, передбаченого у П'ятій директиві про боротьбу з відмиванням грошей;

- співпраця публічно-приватного сектора для обміну інформацією, пов’язаною з фінансуванням тероризму;

- тематичні перевірки для оцінки:

  - ефективності належної перевірки клієнтів та розширеної належної перевірки клієнтів, якщо вони застосовуються до юридичних суб’єктів та юридичних утворень, і виконання вимог щодо ідентифікації бенефіціарного власника.

3. Сектор інституційних інвестицій – Брокери

Продукт
Депозити на рахунках

Сектор
Інвестиційні фірми — Інституційні інвестиції

Загальний опис сектора та відповідного продукту/діяльності

Сектор управління активами ЄС складається з двох взаємнодоповнюючих елементів. Перший елемент представлений пайовими інвестиційними фондами, фондами Організації колективного інвестування в обігові цінні папери (UCITS) (9,7 трлн євро активів під управлінням у 2017 році). Другий елемент включає альтернативні інвестиційні фонди (станом на кінець 2017 року чиста вартість активів альтернативних інвестиційних фондів становила 4,9 трлн євро), такі як хедж-фонди (11 %), фонди приватного капіталу (4 %), фонди фондів (16 %) та фонди нерухомості (11 %). Станом на кінець 2017 року активи під управлінням в ЄС перевищили граничне значення у розмірі 15 трлн євро. Сектор управління активами ЄС обслуговує як роздрібних клієнтів, які зазвичай представлені домогосподарствами та фізичними особами з високим чистим капіталом, так і інституційних клієнтів. Інституційними клієнтами є, наприклад, страхові компанії та пенсійні фонди, на які станом на кінець 2016 року припадало відповідно 25 % та 28 % загальних активів під управлінням в ЄС.

Опис сценарію ризиків

Існує декілька сценаріїв, коли злочинці можуть вчинити зловживання щодо інвесторів або фінансових ринків, наприклад, шляхом інтеграції доходів, таких як право власності на акції, з метою приховування бенефіціарного права власності за допомогою шахрайства або ринкових махінацій (що включають інсайдерську діяльність, ринкові маніпулювання та незаконне розголошення внутрішньої інформації, які підпадають під дію Регламенту про зловживання на ринку ЄС та Директиви про кримінальні санкції ЄС щодо ринкових зловживань), брокерських рахунків, інвестицій для обґрунтування злочинних доходів як прибутку, предикатного інвестиційного шахрайства або розміщення надходжень шляхом використання спеціальних фінансових послуг з високим коефіцієнтом окупності.

Загальні зауваження

Цей сценарій ризику може вважатися пов’язаним зі сценарієм для інвестицій, здійснюваних брокерами. Що стосується вразливості до відмивання коштів, вважається, що рівень ризику для брокерів є вищим.

Загроза

Фінансування тероризму

Рівень загрози фінансування тероризму, пов'язаної з інституційними інвестиціями через брокерів (цінні папери, управління активами та інвестиції), може бути відповідним у разі інвестування великих обсягів законних коштів для фінансування тероризму, але якщо йдеться про невеликі суми грошових коштів для здійснення терористичних атак, загроза фінансування тероризму не є значною для такого продукту/сектора.

Висновок: рівень загрози фінансування тероризму, пов'язаної з інституційними інвестиціями через брокерів, вважається незначним (рівень 1).

Відмивання коштів

Зростаюча роль фасилітаторів у схемах відмивання коштів може збільшити схильність сектора до таких загроз, хоча для їх реалізації потрібні знання і технічні навички. Злочинні організації можуть покладатися на таких фасилітаторів для відмивання доходів від незаконної діяльності. Хоча за допомогою цього процесу можна зібрати великі суми коштів, не так легко отримати доступ до нього, він не є фінансово життєздатним (залежно від якості інвестицій) і у будь-якому разі вимагає знань і технічних навичок. Тому злочинні організації не надають перевагу подібному сценарію ризиків, хоча роль фасилітаторів є важливою при створенні непрозорих структур для приховування доходів від злочинної діяльності.

Тим не менш, протягом останніх декількох років було ідентифіковано кілька методів переміщення крупних незаконних потоків, розроблених висококваліфікованими фасилітаторами:

- клієнти ринку капіталу, що здійснюють майбутні позабіржові свопи через біржі та використовують незаконні кошти для розрахунків після настання дати платежу;
- одночасне придбання, передача та продаж цінних паперів через юрисдикції двома, здавалося б, непов'язаними, але взаємоконтрольованими суб'єктами;
- клієнти з фіксованим доходом на ринку капіталу, які здійснюють продаж облігацій від імені організованих злочинних груп, використовуючи незаконні кошти для придбання облігацій, а потім інтегрують кошти у фінансові установи після продажу таких облігацій.

Висновки: у цьому контексті, рівень загрози відмивання коштів, пов'язаної з інституційними інвестиціями через брокерів, вважається значним (рівень 3).

Вразливість

Фінансування тероризму

Вразливість до фінансування тероризму, пов'язана з інституційними інвестиціями через брокерів (цінні папери, управління активами та інвестиції), становить незначний ризик. Різні фактори ризику, продукти, клієнти, географічні зони та канали доставки у секторі означають, що його використання для цілей фінансування тероризму не є привабливим. У цьому сенсі, злочинці зазвичай не мають досвіду для доступу до сектора, в той час як низькі обсяги грошових коштів, які використовуються у терористичних атаках, зробили інші сектори більш привабливими для їх цілей.

Висновок: у світлі вищезазначеного, рівень вразливості до фінансування тероризму, пов'язаної з інституційними інвестиціями через брокерів, вважається незначним (рівень 1).

Відмивання коштів

Оцінка вразливості до відмивання коштів, пов'язаної з інституційними інвестиціями через брокерів (цінні папери, управління активами та інвестиції), вказує на таке:

a) схильність до ризику

Основним фактором, що пом'якшує ризик відмивання коштів, є низький рівень операцій на основі готівкових коштів, незважаючи на те, що цей сектор стикається з клієнтами високого ризику, включаючи впливових політичних осіб, в той час як обсяг і рівень транскордонних операцій є високим. Для одержання доступу до сектора, злочинці мають вводити гроші через банківську систему, а приховування незаконних коштів через непрозорі структури вимагає високого рівня знань. Тому банки є першим бар'єром, який пом'якшує ризик відмивання коштів.

b) обізнаність про ризики

Рівень обізнаності про ризики у секторі є невисоким, якщо операції здійснюються за межами банківського сектора. Це пояснюється тим, що компанії зазвичай покладаються на банки для здійснення належної перевірки клієнтів та моніторингу у разі походження грошових коштів з банківських рахунків.

Органи нагляду вважають загальний ризик сектора помірно значним; однак профіль ризику на рівні компанії вказує на те, що значна частина компаній класифікується як такі, що мають незначний ризик. Незважаючи на це, більшість органів нагляду вважають, що цей сектор представляє дуже значний транскордонний ризик. Ще одним ключовим ризиком, з яким стикається цей сектор, є узгодження стандартів щодо протидії відмиванню коштів у країнах реєстрації та приймаючих державах-членах, якщо філії групи розташовані у різних країнах.

За даними підрозділів фінансової розвідки, кількість звітів про підозрілі операції є досить низькою порівняно з обсягом відповідних операцій, тому що цей сектор більш знайомий з виявленням випадків шахрайства, таких як інсайдерська торгівля або зловживання на ринку, ніж з підозрами щодо відмивання коштів. Одночасно з цим, відповідні фінансові операції є більш складними, а підозрілі операції, ймовірно, не так легко можуть бути виявлені зобов'язаними суб'єктами.

У цьому секторі також спостерігається значний конфлікт інтересів між занепокоєнням з приводу відмивання коштів та необхідністю залучення клієнтів, деякі з яких представляють високий ризик відмивання коштів, таких як впливові політичні особи, клієнти з країн високого ризику, які не є членами ЄС, а також клієнти з високим рівнем доходу. У цьому сенсі той факт, що послуга надається брокером, впливає на рівень вразливості до відмивання коштів, роблячи його вищим, ніж рівень вразливості стосовно кредитних установ.

c) законодавча база і перевірки

Інституційні інвестиції через брокерів охоплюються вимогами щодо ПВК/ФТ на рівні ЄС. Однак якість виконання цієї законодавчої бази є сумнівною. У сфері інвестицій менеджер клієнта зацікавлений у підтриманні ділових відносин (винагорода/заробітна плата), і це може призвести до того, що він буде більш розслабленим під час здійснення належної перевірки клієнтів.

Органи нагляду вважають, що неналежні перевірки обмежують ефективність звітування про підозрілі операції та ефективність чинних політик та процедур моніторингу, включаючи моніторинг операцій. Навпаки, більшість порушень, виявлених під час перевірок, вважалися незначними. Найпоширенішим висновком були неналежні перевірки щодо впливових політичних осіб.

Висновки: схильність до ризику є по суті високою через характер клієнтів та великі суми, пов'язані з операціями. Однак притаманний ризик пом'якшується з огляду на низький рівень операцій на основі готівкових коштів. Якщо інвестиційні послуги надаються брокерами, вразливість до відмивання грошей є вищою, ніж тоді, коли такі послуги надаються банками. Відсутність ресурсів для застосування надійних процедур належної перевірки клієнтів та певний конфлікт інтересів щодо залучення клієнтів із профілем відмивання коштів з високим ризиком можуть збільшити вразливість. У цьому контексті, рівень вразливості до відмивання коштів, пов'язаної з інституційними інвестиціями через брокерів, вважається значним (рівень 3).

Пом'якшувальні заходи:

Для Комісії:

- глибокий огляд транспозиції П'ятої директиви про боротьбу з відмиванням грошей з акцентуванням уваги на положеннях стосовно інформації про бенефіціарне право власності, включаючи взаємозв'язок реєстрів бенефіціарних власників на рівні ЄС;
- набрання чинності Директивою 2018/822/ЄС від 2020 року, згідно з якою посередники зобов'язані подавати інформацію про транскордонні податкові механізми своїм національним органам влади;
- єдині практики електронної ідентифікації для фінансового сектора та запровадження стандартів для виконання зобов'язань щодо належної перевірки клієнтів з компаніями Reg-Tech.

Для європейських органів нагляду:

- Настанови щодо найкращих наглядових практик для інвестиційного сектора. Визначення основних сценаріїв ризику відмивання коштів, а також найефективніші способи здійснення виїзних та документарних перевірок.

Для держав-членів/компетентних органів:

- набрання чинності Директивою 2018/822/ЄС від 2020 року, згідно з якою посередники зобов'язані подавати інформацію про транскордонні податкові механізми своїм національним органам влади;

- поглиблення та поліпшення впровадження реєстрів бенефіціарних прав власності та взаємозв'язку, передбаченого у П'ятій директиві про боротьбу з відмиванням грошей;

- співпраця публічно-приватного сектора для обміну інформацією, пов'язаною з фінансуванням тероризму;

- тематичні перевірки для оцінки:

  · ефективності належної перевірки клієнтів та розширеної належної перевірки клієнтів, якщо вони застосовуються до юридичних суб'єктів та юридичних утворень, і виконання вимог щодо ідентифікації бенефіціарного власника.

4. Сектор корпоративного банкінгу

Продукт
Депозити на рахунках

Сектор
Кредитні установи – Корпоративний банкінг

Опис сценарію ризиків

Злочинці використовують підставні компанії для внесення доходів у правову економіку, використовуючи рахунки компанії з кількома підписантами.

Загроза

Фінансування тероризму

Корпоративний банкінг може забезпечити великі обсяги законних коштів для фінансування терористичної діяльності або спрямування грошових коштів у зони конфлікту. Однак такий сценарій ризику є малоймовірним, оскільки у терористичних актах використовуються невеликі грошові суми, а також існують інші менш простежувані продукти/сектори, які використовуються для спрямовування грошей у зони ризику. Злочинці не надають перевагу подібним продуктам для фінансування терористичної діяльності, тому загроза фінансування тероризму не є значною для такого продукту/сектора.

Висновок: рівень загрози фінансування тероризму, пов'язаної з корпоративним банкінгом, вважається незначним (рівень 1).

Відмивання коштів

Оцінка загрози відмивання коштів, пов'язаної з корпоративним банкінгом, вказує на те, що цей сценарій ризику регулярно застосовувався для таких схем. Використання корпоративного банкінгу для відмивання коштів вимагає вирішення більш складних завдань, ніж роздрібний фінансовий сектор, але залежно від відповідної фінансової послуги, рівень необхідної складності може бути нижчим: наприклад, персональна документація потрібна лише за наявності попиту на позику. Тим не менш, з огляду на рівень складності, який вимагається корпоративними банківськими операціями, їх використання для відмивання коштів може вимагати співучасті фінансових/юридичних посередників, які мають одержувати винагороду за свої «послуги». Цей параметр може впливати на компонент «намір».

Правоохоронні органи мають докази спеціалістів з відмивання коштів, які діють як посередники для інших організованих злочинних груп, які відкривають банківські рахунки для підставних компаній або компаній-оболонок. Ці корпоративні банківські рахунки використовуються для шахрайських торгових операцій, компенсаційних кредитів в інших корпоративних суб'єктів та інвестицій у нерухомість.

Висновки: цей метод використовується організованими злочинними групами із збільшенням ролі посередників. На думку правоохоронних органів, цей метод вимагає лише помірного рівня знань та досвіду. У цьому контексті, рівень вразливості до відмивання коштів, пов'язаної з корпоративним банкінгом, вважається значним (рівень 3).

Вразливість

Фінансування тероризму

Рівень уразливості до фінансування тероризму в корпоративному банківському секторі є незначним. Різні фактори ризику, продукти, клієнти, географічні зони та канали доставки у секторі означають, що його використання для цілей фінансування тероризму не є привабливим. Злочинці зазвичай не мають досвіду доступу до сектора, в той час як низькі обсяги коштів, які використовуються у терористичних атаках, зробили інші сектори більш привабливими для їх цілей.

Висновок: у світлі вищезазначеного, рівень вразливості до фінансування тероризму, пов'язаної з інституційними інвестиціями через банки, вважається незначним (рівень 1).

Відмивання коштів

Оцінка вразливості до відмивання коштів, пов'язаної з корпоративним банкінгом, вказує на таке:

а) схильність до ризику

Притаманний ризик є потенційно високим з огляду на характер клієнтів та більш складні операції, ніж у роздрібному банкінгу. Ідентифікація бенефіціарного власника деяких компаній є однією з основних вразливостей цього продукту. Деякі операції на основі торговельної діяльності, пов'язані з корпоративними банківськими рахунками, можуть збільшити ризик відмивання коштів, особливо у разі залучення юрисдикції високого ризику. Ризик, пов'язаний з підробленою документацією, також впливає на рівень схильності до ризику, в той час як зростаюча роль посередників та фасилітаторів, що працюють на організовані злочинні групи, також може впливати на ризик таких продуктів. Деякі готівкові операції можуть бути врегульовані за допомогою цих продуктів, якщо компаніями, залученими у корпоративні банківські продукти, є підприємства з високим оборотом готівки.

Більше того, притаманний таким банківським продуктам ризик також може бути збільшений за рахунок використання нових технологій та непрямих ділових відносин.

Що стосується органів нагляду в області боротьби з відмиванням коштів, відмінності у складі та характері секторів кредитних установ держав-членів відображаються у рейтингах притаманних ризиків, що варіюються від «значного» та «дуже значного» до «помірно значного» і навіть «незначного». З іншого боку, більшість органів нагляду вважають широке використання готівки у деяких підсекторах та у деяких державах-членах одним із факторів, що сприяють схильності сектора до ризику відмивання коштів, особливо якщо сектор представлений великою кількістю роздрібних банків. Органи нагляду також вважають, що транскордонна діяльність схильна до значного та дуже значного ризику відмивання коштів, особливо в тих державах-членах, які вважаються міжнародними фінансовими центрами. Клієнти-нерезиденти з юрисдикцій високого ризику та офшорні компанії також сприяють підвищенню ризику в цьому секторі.

b) обізнаність про ризики

Обізнаність сектора про ризики є високою, і сектор розробив інструменти для ініціювання відповідних тривожних сигналів. Зазвичай тривожні сигнали ініціюються у відповідь на клієнтів високого ризику, юрисдикції високого ризику та наявність транскордонних операцій. Підрозділи фінансової розвідки підтвердили цей елемент, зазначивши, що стосовно цього питання надійшла велика кількість звітів про підозрілі операції. Однак сектор скаржиться на відсутність зворотного зв'язку з боку підрозділів фінансової розвідки. Цей факт обмежує здатність сектора вдосконалювати свої системи моніторингу.

У більшості держав-членів органи нагляду в області боротьби з відмиванням коштів надають настанови щодо підтримки кредитних установ у виявленні потенційно підозрілих корпоративних банківських операцій.

c) законодавча база і перевірки

Корпоративний банкінг охоплюються вимогами щодо ПВК/ФТ на рівні ЄС. Ця база вважається задовільною як така, що охоплює іншу фінансову діяльність, яка здійснюється кредитними установами.

Більшість органів нагляду оцінили перевірки, здійснювані кредитними установами для пом'якшення ризиків відмивання коштів як «належні» або «прекрасні» загалом. Незважаючи на це, вони оцінюють ефективність цих політик та процедур, особливо тих, що стосуються постійного моніторингу операцій та звітів про підозрілі операції, як неналежні або погані.

Висновки: корпоративний банкінг представляє певну вразливість з огляду на фактори ризику, пов'язані з клієнтами. Однак існуюча законодавча база вважається адаптованою до таких вразливостей, тоді як кредитні установи, залучені у корпоративну банківську діяльність, обізнані про ризики відмивання коштів та готові їх усувати. У цьому контексті, рівень вразливості до відмивання коштів, пов'язаної з корпоративним банкінгом, вважається помірно значним/значним (рівень 2/3).

Пом'якшувальні заходи:

Для Комісії:

- глибокий огляд транспозиції П'ятої директиви про боротьбу з відмиванням грошей з акцентуванням уваги на положеннях стосовно інформації про бенефіціарне право власності, включаючи взаємозв'язок реєстрів бенефіціарних власників на рівні ЄС;
- єдині практики електронної ідентифікації для фінансового сектора та запровадження стандартів для виконання зобов'язань щодо належної перевірки клієнтів з компаніями Reg-Tech;
- набрання чинності Директивою 2018/822/ЄС від 2020 року, згідно з якою посередники зобов'язані подавати інформацію про транскордонні податкові механізми своїм національним органам влади.

Для європейських органів нагляду:

- У контексті оновлення спільного висновку Спільного комітету Європейських органів нагляду щодо ризиків відмивання коштів та фінансування тероризму, Європейські органи нагляду мають забезпечити аналіз операційних ризиків ПВК/ФТ, пов'язаних з бізнесом/бізнес-моделлю у корпоративному банківському секторі.

Для держав-членів/компетентних органів:

- Органи влади повинні забезпечити проведення навчання та надання настанов щодо факторів ризику, акцентуючи увагу на непрямих ділових відносинах, офшорних професійних посередниках, клієнтах чи юрисдикціях, а також на складних структурах/структурах-оболонках.
- Тематичні перевірки для оцінки:
  - ефективності належної перевірки клієнтів та розширеної належної перевірки клієнтів, якщо вони застосовуються до юридичних суб'єктів та юридичних утворень, і виконання вимог щодо ідентифікації бенефіціарного власника.

5. Сектор приватного банкінгу

Продукт
Депозити на рахунках

Сектор
Кредитні установи — Приватний банкінг та управління приватним капіталом

Опис сценарію ризиків

Приватний банкінг є послугою, що надається кредитними установами та інвестиційними компаніями фізичним особам з високим чистим капіталом, членам їх родини та корпоративним суб'єктам. Загалом ці послуги адаптуються під кожного клієнта шляхом поєднання в одному пакеті декількох банківських та інших фінансових послуг. Наприклад, послуги приватного банкінгу можуть включати в себе сукупність банківських послуг (поточні рахунки, іпотеки та обмін валюти), послуги управління інвестиціями та консультації, фідуціарні послуги, послуги безпечного зберігання, страхування, бухгалтерського обліку, податкового планування та планування у сфері нерухомості, а також супутні послуги, такі як юридична підтримка.

Злочинці використовують приватний банкінг та послуги управління приватним капіталом для інвестування в акції з метою інтеграції злочинних доходів. З огляду на поєднання складних фінансових продуктів та послуг, а також багату клієнтську базу, яка іноді включає впливових політичних осіб, з часто складними структурами власності, цей сектор може також використовуватися для ухиленням від сплати податків.

Загальні зауваження

У цьому сценарії ризиків фінансові послуги стосуються інвестицій високої вартості, а не інвестицій фізичних осіб у роздрібні послуги.

Загроза

Фінансування тероризму

Оцінка загрози фінансування тероризму, пов’язаної з приватним банкінгом (управління приватним капіталом), не була розглянута як належить. Тому загроза фінансування тероризму не є частиною оцінки.

Висновки: не застосовується

Відмивання коштів

Оцінка загрози відмивання коштів, пов’язаної з приватним банкінгом (управління приватним капіталом), вказує на те, що цей сектор використовується у зв’язку з наступними предикатними злочинами: корупція і торгівля наркотиками, шахрайство та ухилення від сплати податків. Це зменшує «сферу дії» організованих злочинних організацій, які можуть покладатися на цей сценарій ризиків. Цей сценарій також вимагає певного рівня знань, що робить його менш легкодоступним і не дуже привабливим (фінансово нежиттєздатним). Приватний банкінг передбачає «високу вартість» послуг (потреба у достатній кількості коштів для доступу до послуг) і складніше встановлення ділових відносин. Однак деякі групи можуть використовувати фасилітаторів для отримання доступу до приватних банківських послуг через фіктивних осіб або юридичних суб’єктів.

Висновки: ґрунтуючись на вищезазначеному, рівень загрощи відмивання грошей, пов'язаної з приватним банкінгом, вважається значимим/дуже значимим (рівень 3/4).

Вразливість

Фінансування тероризму

Оцінка вразливості до фінансування тероризму, пов’язаної з приватним банкінгом (управління приватним капіталом), не була розглянута як належить. У цьому контексті, вразливість до фінансування тероризму не є частиною оцінки.

Висновки: не застосовується

Відмивання коштів

Оцінка вразливості до відмивання коштів, пов’язаної з приватним банкінгом, вказує на таке:

a) схильність до ризику

Поєднання складних фінансових продуктів та послуг, а також багата клієнтська база (яка іноді включає впливових політичних осіб) з часто складними структурами власності, роблять цей сектор вразливим для цілей відмивання коштів. Деякі запропоновані продукти та послуги також вважаються уразливими до відмивання коштів, зокрема, ті, що пов’язані з дотриманням податкових норм та плануванням. Однією з таких послуг є «агресивне» податкове планування. Більше того, цей сектор представляє більш високий географічний ризик з огляду на створення філій у деяких країнах, які не є членами ЄС, де необов’язково присутні режими ПВК/ФТ, що є еквівалентними законодавчій базі ЄС щодо ПВК/ФТ.

b) обізнаність про ризики

За даними підрозділів фінансової розвідки, приватний банкінг характеризується дуже низьким (майже відсутнім) рівнем звітування про підозрілі операції. Що стосується інвестиційних послуг, установи інколи стикаються з конфліктом між своїми комерційними цілями та необхідністю боротися з відмиванням коштів. Враховується компонент конкуренції. Однак для приватного банкінгу оцінка ризиків не завжди є достатньо точною, аби забезпечити обізнаність сектора про ризики, з якими він стикається, зокрема, ризики, пов’язані з шахрайством та ухиленням від сплати податків. Органи нагляду вважають, що компанії в цьому секторі не в достатній мірі пом’якшують ризик зловживання цим сектором для цілей ухилення від сплати податків.

c) законодавча база і перевірки

Приватний банкінг підпадаю під дію вимог щодо ПВК/ФТ на рівні ЄС. Більшість компетентних органів, які перевіряють провайдерів послуг приватного банкінгу, оцінили перевірки як такі, що не відповідають рівню належної перевірки клієнтів (верифікація особи клієнта, інформація про походження коштів, верифікація бенефіціарного права власності – зокрема, для юридичних осіб), моніторингу операцій та нормативно-правового дотримання. Вони пояснюють це тим, що (i) якість перевірок залежить від фінансової культури країни; і (ii) тим, що розуміння ризиків, які створює цей сектор, є різним у різних державах-членах.

Висновки: Високий ризик з огляду на крупні залучені суми, клієнтів високого ризику (впливові політичні особи) та юрисдикції потенційно високого ризику. Занепокоєння щодо обізнаності сектора про ризики з огляду на конкуренцію між постачальниками для залучення клієнтів високого ризику, в той час як результати тематичних перевірок свідчать про неналежні перевірки у певних сферах. Більше того, рівень звітування про підозрілі операції є низьким. У цьому контексті, рівень вразливості до відмивання коштів, пов'язаної з приватним банкінгом, вважається значним/дуже значним (рівень 3/4).

Пом'якшувальні заходи:

Для Комісії:

- глибокий огляд транспозиції П'ятої директиви про боротьбу з відмиванням грошей з акцентуванням уваги на положеннях стосовно інформації про бенефіціарне право власності, включаючи взаємозв'язок реєстрів бенефіціарних власників на рівні ЄС;

- єдині практики електронної ідентифікації для фінансового сектора та запровадження стандартів для виконання зобов'язань щодо належної перевірки клієнтів з компаніями Reg-Tech;

- набрання чинності Директивою 2018/822/ЄС від 2020 року, згідно з якою посередники зобов'язані подавати інформацію про транскордонні податкові механізми своїм національним органам влади.

Для європейських органів нагляду:

- Європейські органи нагляду повинні забезпечити проведення навчання для компетентних органів, акцентуючи увагу на спільному підході до перевірок та основних сфер ризику.

Для держав-членів/компетентних органів:

- Тематичні перевірки для оцінки:

    - ефективності належної перевірки клієнтів та розширеної належної перевірки клієнтів, якщо вони застосовуються до юридичних суб'єктів та юридичних утворень, і виконання вимог щодо ідентифікації бенефіціарного власника.

- Ризики, пов'язані з цим сектором, мають бути чітко викладені в оцінці ризиків відмивання коштів/фінансування тероризму компетентних органів. Компетентні органи повинні видати настанови щодо найкращих практик та забезпечити навчання для сектора.

- Компетентні органи повинні забезпечити використання систем та перевірок для зниження здатності компаній розробляти або рекомендувати продукти і послуги, які допомагають їх клієнтам вчиняти податкові злочини.

6. «Краудфандинг»

Продукт
«Краудфандинг»

Сектор
Платформи «краудфандингу»

Загальний опис сектора та відповідного продукту/діяльності

«Краудфандингом» є відкритий заклик до громадськості щодо збирання коштів для конкретного проекту. Платформами «краудфандингу» є веб-сайти, які передбачають взаємодію між організаціями із збирання грошових коштів та особами, зацікавленими у фінансовому внеску у проект. Через платформу можуть надаватися та збиратися фінансові внески.

Тип діяльності із збирання грошових коштів є різним у різних моделях «краудфандингу». Мають місце також відмінності у мотивації і типі учасників, а також у кінцевих відносинах між інвесторами/позикодавцями та шукачами/позичальниками. Використовуються різні моделі платформ «краудфандингу», і будь-яка класифікація є умовною, оскільки ринок розвивається та інтегрує нові технології у сферу надання послуг. П'ять основних категорій платформ «краудфандингу» включають:

- «краудфандинг» на основі інвестицій: компанії випускають пайові або боргові інструменти «крауд-інвесторам» через платформу;
- «краудфандинг» на основі кредитування (відомий також як «краудлендінг», рівноправне кредитування або ринкове кредитування): компанії або фізичні особи прагнуть отримати кошти від населення через платформи у формі кредитного договору;
- «краудфандинг» на основі торгівлі рахунками-фактурами: форма фінансування на основі активів, за якої підприємства продають неоплачені рахунки-фактури або дебіторську заборгованість, окремо або в комплекті, пулу інвесторів через онлайн-платформу,
- «краудфандинг» на основі винагороди: фізичні особи здійснюють пожертвування на користь проекту чи підприємства, очікуючи отримати натомість нефінансову винагороду, таку як товари чи послуги, на більш пізньому етапі в обмін на свій внесок;
- «краудфандинг» на основі пожертвування: фізичні особи жертвують грошові суми для досягнення більшого фінансування конкретного благодійного проекту, не отримуючи при цьому фінансової чи матеріальної віддачі.

Існує низка платформ, які поєднують різні моделі або на яких працює модель, яку неможливо одразу класифікувати за цими п'ятьма категоріями («гібридні моделі краудфандингу»). Однак вони, як правило, значно меншого масштабу, ніж основні.

Інша відповідна класифікація платформ «краудфандингу» залежить від того, чи є вони дозволеними або ні:

- Регульовані платформи «краудфандингу», які підпадають під дію чинної законодавчої ініціативи щодо фінансових послуг (тобто платформи на основі інвестицій та на основі кредитування), а отже є дозволеними.

- Нерегульовані платформи «краудфандингу», які виходять за межі законодавства про фінансові послуги (тобто «краудфандинг» на основі пожертвування, винагороди, споживчого кредитування). Сюди також включено веб-сайти, тобто платформи соціальних мереж, додатки для обміну повідомленнями або блоги з потенційно широкою аудиторією, що може дозволити їхнім користувачам здійснити публічний заклик щодо збирання коштів, але якщо сама платформа не сприяє цьому процесу.

Слід також враховувати той факт, що хоча платформи представляють та з'єднують відповідних сторін, фактичні грошові операції, як правило, здійснюються уповноваженими провайдерами платіжних послуг, що підпадають під дію законодавства про боротьбу з відмиванням грошей. Тому слід розрізняти регульований «краудфандинг», коли операції здійснюються через уповноважених провайдерів платіжних послуг (тобто шляхом інтеграції з PayPal або шляхом використання особистих банківських рахунків) на регульованих платформах «краудфандингу», які підпадають під додаткові вимоги щодо розкриття інформації, та нерегульований «краудфандинг», який наразі не підпадає під дію законодавства про фінансові послуги. Зокрема, у нерегульованій сфері платежі можуть здійснюватися також через менш прозорі засоби, тобто криптоактиви або жетони у формі передплачених сім-карт.

Загалом європейський ринок альтернативного фінансування у 2017 році збільшився до 10,44 млрд євро, що на 36 % більше, ніж у попередньому році. На ринку, як і раніше, домінує Сполучене Королівство, ринкова частка якого у 2016 році склала 68 % і становила 7,07 млрд євро, порівняно з 75 % у попередньому році. Решта європейського ринку складала загалом 3,37 млрд євро і досягла рівня 63 % у такому році. Це робить «краудфандинг» найважливішим субринком сектора альтернативного фінансування. За винятком Сполученого Королівства, країнами з найбільшими обсягами ринку у 2016 році були Франція, Німеччина, Нідерланди, Італія та Фінляндія.

Аналізуючи ринкову частку більш детально, рівноправне кредитування фізичних осіб має найбільшу ринкову частку (41 %), за якою слідує торгівля рахунками-фактурами (16 %), рівноправне кредитування підприємств (14 %), «краудфандинг» на основі нерухомості (8 %) та «краудфандинг» на основі власного капіталу (6 %).

Опис сценарію ризиків

Злочинці можуть створювати платформи збирання/накопичення коштів та їх переказу закордон для відмивання коштів або для фінансування терористичних атак. Це може бути здійснено шляхом створення регульованої платформи «краудфандингу», безпосередньо пов'язаної з фінансовою установою[38], або шляхом створення платформи за межами регульованого середовища, не пов'язаної з фінансовою установою, де платежі можуть здійснюватися у віртуальній валюті, картках електронних грошей тощо. Несанкціоновані платформи «краудфандингу» можуть бути створені в рамках фіктивних проектів для збирання коштів, які потім зніматимуться на території ЄС або переказуватимуться закордон. Цей метод може використовуватися для збирання коштів із законних джерел для фінансування тероризму або для збирання незаконних коштів від злочинної діяльності з використанням анонімних продуктів.

[38] Пов'язаної з банківським рахунком або з банківським партнерством.

Незаконне використання соціальних мереж («краудсорсинг») є ще одним різновидом сценарію ризиків. Зокрема, терористичні групи використовують соціальні мережі та інші Інтернет і мобільні платформи для отримання коштів, що згодом спрямовуються за допомогою різних платіжних засобів. Цей тип краудсорсингу не аналізується в цьому документі.

Загроза

Фінансування тероризму

Терористичні групи можуть мати намір використовувати методи «краудфандингу» для збирання коштів. Загалом, було виявлено декілька випадків, пов'язаних з (нерегульованими) платформами пожертвування, де використовувалися такі методи; зазвичай вони використовувалися для збирання менших сум. Крім того, підозрілу діяльність виявити легше, і це може стримувати терористичні групи використовувати цей метод з огляду на його небезпечність. Однак, якщо злочинці будуть більш методичними у своєму плануванні, це може дозволити їм створювати платформи збирання з можливістю здійснення більш анонімних операцій (використання підставних осіб або родичів), що робить цей метод більш привабливим. Правоохоронні органи виявили кілька випадків закликів щодо «краудфандингу» на основі пожертвування, посилаючись на надання «підтримки вдовам, мученикам, релігійним групам», намагаючись уникнути явного зв'язку з фінансуванням тероризму. Вартість пожертвувань є невисокою (10, 20, 50 доларів, причому більшість сум у доларах США). Правоохоронним органам складно ідентифікувати кінцевого одержувача та використання пожертвувань (доказ фінансування тероризму).

Висновки: Правоохоронні органи мають докази використання терористичними групами нерегульованих платформ «краудфандингу» на основі пожертвувань. Однак збирання або спрямування великих сум у такий спосіб є фінансово неможливим. Крім того, це може бути досить небезпечно порівняно з іншими видами послуг або вимагає складнішого планування для приховування незаконного наміру. У цьому контексті, рівень загрози фінансування тероризму, пов'язаного з «краудфандингом», вважається помірно значним (рівень 2).

Відмивання коштів

Оцінка загрози відмивання коштів, пов'язаної з «краудфандингом», вказує на те, що існує дуже мало або взагалі відсутні докази чи показники того, що злочинці використовують її для фактичного відмивання доходів, отриманих злочинним шляхом. Однак мають місце ситуації, коли компанія була заснована з метою її використання у злочинній діяльності з «краудфандингу», але це вимагає певного досвіду та може бути дорогим. Один виявлений випадок стосувався складної схеми Понці з використанням підроблених та фальшивих проектів. Це говорить про те, що такий сценарій може бути важкодоступним і вимагає доступу до платіжних процесів. Це може означати, що використання злочинних посередників може зробити цей сектор більш привабливим для відмивання коштів. Однак правоохоронні органи вважають, що цей сектор все ще використовується більше для шахрайського збирання коштів та шахрайства, а не для відмивання незаконних коштів.

Висновки: злочинці можуть мати чіткі наміри щодо використання цього методу, який необов'язково є привабливим і може бути затратним. У будь-якому разі метод вимагає певної експертизи, аби бути прибутковим. Дуже мало доказів того, що він використовується, хоча роль посередників не можна ігнорувати також. У цьому контексті, рівень загрози відмивання коштів, пов'язаної з «краудфандингом», вважається помірно значним (рівень 2)

Вразливість

Фінансування тероризму

Оцінка вразливості фінансування тероризму, що стосується «краудфандингу», вказує на те, що цей сектор не можна оцінювати окремо.

a) схильність до ризику

Рівень схильності до ризику змінюється, залежно від того, чи контролюється платформа «краудфандингу» як провайдер фінансових послуг або залишається нерегульованою (приватні ініціативи у мережі Інтернет). Аналогічно цьому, ризик фінансування тероризму також залежить від типу платформи. Нерегульовані платформи «краудфандингу» на основі пожертвувань представляють більш високий ризик неправильного використання для цілей фінансування тероризму, оскільки такі платформи виходять за межі фінансових установ та пруденційних органів нагляду в області боротьби з відмиванням коштів. Притаманний ризик краудфандингу є вищим, якщо платформи краудфандингу дозволяють використовувати віртуальні валюти або (анонімні) електронні гроші. Притаманний ризик також є вищим, якщо злочинці створюють платформи «краудфандингу» на основі пожертвувань, що дозволяють використовувати підставних осіб, родичів або фізичних осіб поза санкційними переліками.

b) обізнаність про ризики

Навіть якщо платформа «краудфандингу» регулюється як провайдер фінансових послуг, можуть бути відсутні знання про джерела коштів та ціль. Якщо вони надаються через нерегульовані платформи, послуги «краудфандингу» виходять за межі будь-якого моніторингу ПВК/ФТ. Компетентні органи влади, в тому числі на рівні ЄС, усвідомлюють, що існують ризики фінансування тероризму, але оцінка ризиків все ще є неповною у більшості державах-членах. Однак слід підкреслити, що якщо ці платформи будуть включені до переліку зобов'язаних суб'єктів, підрозділи фінансової розвідки отримуватимуть звіти про підозрілі операції.

c) законодавча база і перевірки

Що стосується бази ЄС щодо ПВК/ФТ, вона, як правило, не застосовується до платформ «краудфандингу» як така, але застосовується до конкретних видів послуг «краудфандингу», залежно від бізнес-моделі. Отже, не існує наскрізної бази, яка встановлює зобов'язання щодо ПВК/ФТ для таких послуг.

Платформи «краудфандингу» регулюються у деяких державах-членах, переважно в частині цінних паперів та кредитування, що означає, що платформи на основі пожертвувань не підпадають під дію зобов'язань щодо ПВК/ФТ. Деякі держави-члени включили платформи «краудфандингу» у своє законодавство, транспонуючи положення Директиви про платіжні послуги II. Однак компетентні органи вважають, що перевірки та заходи нагляду є слабкими, зокрема, тому що багато платформ фізично не розташовані на території, на якій вони функціонують, що знижує ефективність перевірок. У разі залучення кредитних та фінансових установ, ефективність перевірок зобов'язаних суб'єктів є нижчою, оскільки зобов'язані суб'єкти можуть розраховувати лише на більш обмежену інформацію для моніторингу операцій та застосовувати тривожні сигнали.

Висновки: сектор не є однорідним, і на рівень вразливості може впливати його взаємодія з іншими секторами. Здійснювані перевірки не узгоджені, оскільки не існує наскрізної бази, яка б розглядала ці питання, хоча новий регламент про європейських провайдерів послуг «краудфандингу» покращить таку базу. Існує певне занепокоєння щодо обізнаності сектора про ризики. У цьому контексті, рівень вразливості фінансування тероризму, пов'язаної з «краудфандингом», вважається помірно значним (рівень 2)

Відмивання коштів

Оцінка вразливості до відмивання коштів, пов'язаної з «краудфандингом», є аналогічною оцінці вразливості, пов'язаної з фінансуванням тероризму.

a) схильність до ризику

Рівень схильності до ризику відрізняється, залежно від того, чи пов'язаний «краудфандинг» безпосередньо з фінансовими установами або є перевагою приватних ініціатив у мережі Інтернет. В обох випадках використання віртуальних валют може збільшити ризик відмивання коштів. Залежно від типу платформи, послуги можуть сприяти здійсненню анонімних операцій. На платформах кредитування та цінних паперів можна зібрати більші суми, що робить ризик відмивання коштів вищим, ніж на платформах на основі пожертвувань. Однак ці платформи «краудфандингу» зазвичай є регульованими, а отже відповідають вимогам щодо розкриття інформації, та співпрацюють з платіжними або кредитними установами з метою здійснення платіжних операцій.

b) обізнаність про ризики

Проникнення на такі платформи злочинними організаціями також можна вважати додатковим фактором вразливості. Деякі правоохоронні органи та підрозділи фінансової розвідки вважають «краудфандинг» поширеним способом відмивання коштів. Навіть у разі залучення фінансової установи, бракує знань про джерела коштів, обсяг фінансування та його ціль. Якщо вони надаються через нерегульованих суб'єктів, послуги «краудфандингу» виходять за межі будь-якого моніторингу ПВК/ФТ. Компетентні органи влади, в тому числі на рівні ЄС, усвідомлюють існування ризиків відмивання коштів, але деякі з них вважають, що цей сектор має низький ризик, і не розглядають можливість включення платформ «краудфандингу» в якості зобов'язаних суб'єктів. Однак слід підкреслити, що якщо ці платформи включені до переліку зобов'язаних суб'єктів, підрозділи фінансової розвідки отримуватимуть звіти про підозрілі операції.

c) законодавча база і перевірки

Що стосується законодавчої бази ЄС щодо ПВК/ФТ, вона, як правило, не застосовується до платформ «краудфандингу» як така, але застосовується до конкретних видів послуг «краудфандингу», залежно від бізнес-моделі. Отже, не існує наскрізної законодавчої бази, яка визначає зобов'язання у сфері ПВК/ФТ для таких послуг.

Конкретні типи послуг «краудфандингу» у більшості випадків будуть підпадати під дію зобов'язань у сфері ПВК/ФТ, залежно від бізнес-моделі (наприклад, «краудфандинг» на основі інвестицій та кредитування). Деякі держави-члени включили платформи «краудфандингу» у своє законодавство шляхом транспозиції Директиви про ринки фінансових інструментів II та Директиви про платіжні послуги II. Однак на цьому етапі не всі держави-члени розглядають можливість включення платформ «краудфандингу» в якості зобов'язаних суб'єктів.

Навіть якщо платформи «краудфандину» вважаються зобов'язаними суб'єктами, на думку компетентних органів перевірки та заходи нагляду є слабкими, зокрема, тому що багато платформ фізично не розташовані на території, на якій вони функціонують, що зменшує ефективність перевірок. У разі залучення кредитних та фінансових установ, ефективність перевірок зобов'язаних суб'єктів є нижчою, оскільки зобов'язані суб'єкти можуть розраховувати лише на більш обмежену інформацію для моніторингу операцій та застосовувати тривожні сигнали.

Висновки: схильність до ризику є досить обмеженою, хоча у деяких конкретних бізнес-моделях «краудфандингу» можуть бути залучені великі суми. Здійснювані перевірки не узгоджені, оскільки не існує наскрізної бази, яка б розглядала ці питання. Якщо вони регулюються, такі платформи належним чином усвідомлюють свої ризики, і рівень звітування є належним. Здійснювані перевірки інколи все-таки є слабкими, особливо коли зобов'язані суб'єкти покладаються на обмежену інформацію для здійснення перевірок. Новий регламент щодо європейських бізнес-провайдерів з «краудфандингу» покращить цю законодавчу базу. У цьому контексті, рівень вразливості до відмивання коштів, пов'язаної з корпоративним банкінгом, вважається помірно значним (рівень 2).

Пом'якшувальні заходи:

Для держав-членів/компетентних органів:

- При застосуванні положень статті 4 П'ятої директиви про боротьбу з відмиванням грошей, яка розширює сферу дії зобов'язаних суб'єктів, держави-члени повинні врахувати необхідність визначення нерегульованих платформ «краудфандингу» як зобов'язаних суб'єктів, що підпадають під дію вимог у сфері ПВК/ФТ.

7. Обмін валют

Продукт
Конвертація коштів

Сектор
Пункти обміну валют

Опис сценарію ризиків

Злочинці конвертують свої кошти в іншу валюту для полегшення конвертації, переказу або відмивання коштів.

Загроза

Фінансування тероризму

Оцінка загрози фінансування тероризму, пов'язаної з обміном валют, вказує на те, що цей алгоритм дій використовується терористичними групами, особливо іноземними терористами-бойовиками. Конвертація EUR/USD є особливо привабливою для цих груп. Введення валюти у зони конфлікту є одним з основних способів фінансування руху іноземних терористів-бойовиків. З технічної точки зору, конвертація коштів не вимагає спеціального планування, знань чи досвіду і є досить легкодоступною. Хоча сам процес не передбачає збирання або переказ коштів, це є необхідним кроком для переміщення фізично «чистої» валюти (переважно готівкою). Терористичні групи можуть вважати, що обмін валют є настільки ж привабливим, як і збирання чи переказ коштів для фінансування їх діяльності.

Висновки: терористичні групи демонструють певний намір і здатність використовувати обмін валют для підтримання/здійснення своїх операцій. Цей сценарій не вимагає спеціального планування та експертних знань і активно використовується. У цьому контексті, рівень загрози фінансування тероризму, пов'язаної з обміном валют, вважається значним (рівень 3).

Відмивання коштів

Оцінка загрози відмивання коштів, пов'язаної з обміном валют, свідчить про те, що існують випадки, коли у пункти обміну валют проникають злочинні організації для здійснення своєї діяльності. Це особливо має місце у пунктах, які працюють в аеропортах і туристичних районах. Великі обсяги коштів можуть з легкістю конвертуватися, що полегшує доступ таких злочинних організацій до «чистої» валюти. Як і у випадку фінансування тероризму, обмін валют не вимагає спеціального планування та експертних знань для відмивання коштів. Однак наразі обсяг підозрілих операцій важко оцінити.

Висновки: хоча правоохоронним органам складно оцінити кількість випадків, цифри свідчать про те, що злочинні організації можуть використовувати обмін валют для відмивання доходів, одержаних злочинним шляхом. Цей сценарій не вимагає спеціального планування та експертних знань і активно використовується. У цьому контексті, рівень загрози фінансування тероризму, пов'язаної з обміном валют, вважається значним (рівень 3).

Вразливість

Фінансування тероризму

Уразливість при обміні валют пов'язана з переказом коштів. Існує два різні способи здійснення операцій:

- використання готівки для обміну та переказу коштів на вказаний банківський або платіжний рахунок;
- використання наміру для здійснення обміну валют та переказу коштів на банківський або платіжний рахунок.

a) схильність до ризику

Той факт, що більшість операцій здійснюється готівкою, підвищує рівень вразливості сектора. Більше того, потенційні операції, пов'язані з фінансуванням тероризму, зазвичай передбачають невеликі обсяги готівкових коштів, які важче виявити у пунктах обміну.

b) обізнаність про ризики

У деяких сценаріях ризику провайдери послуг з переказу грошових коштів асоціюються з пунктами обміну або навіть працюють у тих самих приміщень. У таких випадках системи попередження та тривожні сигнали, які застосовуються провайдерами послуг з переказу грошових коштів для виявлення операцій, пов'язаних з фінансуванням тероризму, застосовуються до попередньої операції з обміну валют. Негативний ефект полягає в тому, що пункти обміну валют покладаються на перевірки провайдерами послуг з переказу грошових коштів наявності фінансування тероризму. Сам пункт обміну валют не в змозі простежити всю операцію, виявити потенційно підозрілі операції та підтримувати повноцінні ділові відносини зі своїми клієнтами.

Обізнаність про ризики у секторі є високою, особливо коли пункти обміну валют близько розташовані до провайдерів послуг з переказу грошових коштів, але рівень звітування про підозрілі операції залишається низьким, за винятком особливих випадків, таких як конвертація у долари США, яка вимагається від країн високого ризику, що не не є членами ЄС (наприклад, Сирія).

c) законодавча база і перевірки

Пункти обміну валют підпадають під дію законодавчої бази щодо ПВК/ФТ на рівні ЄС. Органи нагляду вважають, що перевірки стосовно ефективності звітування про підозрілі операції загалом є неналежними або поганими, як і перевірки, пов'язані з ідентифікацією та верифікацією клієнтів. У цьому сенсі, нові технологічні розробки можуть стати важливим пом'якшувальним фактором для сектора у разі зростання кількості онлайн-платежів. Заходи нагляду здебільшого обмежуються документарними перевірками, а деякі тематичні перевірки здійснюються у відповідь на конкретні виявлені ризики. У разі застосування деякими юрисдикціями граничних значень для випадкових операцій, рівень вразливості є вищим, особливо для ризиків фінансування тероризму, коли низькі суми є нормою.

Висновки: Контроль у секторі є не дуже ефективним і покладається на суміжні сектори, такі як провайдери послуг з переказу грошових коштів та банки. Граничні значення для випадкових операцій можуть суттєво впливати на системи моніторингу та вимоги належної перевірки клієнтів, збільшуючи рівень вразливості до фінансування тероризму. У цьому контексті, рівень вразливості до фінансування тероризму, пов'язаної з обміном валют, вважається значним (рівень 3).

Відмивання коштів

Оцінка вразливості до відмивання коштів, пов'язаної з обміном валют, свідчить про таке:

a) схильність до ризику

Той факт, що більшість операцій здійснюється готівкою, впливає на рівень вразливості; такий вплив стає більш вираженим, якщо клієнт використовує купюри високого номіналу, які недостатньо контролюються. Іншими факторами, що підвищують ризик сектора, є використання цих послуг впливовими політичними особами або пунктами обміну валют, розташованими у прикордонних зонах. Основним фактором ризику є проникнення злочинних організацій у пункти обміну валют або агентства. Рівень ризику збільшується, якщо компанії мають неналежні інструменти для виявлення потенційно сумнівних агентів з обміну валют.

b) обізнаність про ризики

У деяких сценаріях ризику провайдери послуг з переказу грошових коштів асоціюються з пунктами обміну або навіть працюють у тих самих приміщеннях. У таких випадках системи попередження та тривожні сигнали, які застосовуються провайдерами послуг з переказу грошових коштів для виявлення операцій, пов'язаних з відмиванням коштів, застосовуються до попередньої операції з обміну валют. Негативний ефект полягає в тому, що пункти обміну валют покладаються на перевірки провайдерами послуг з переказу грошових коштів наявності випадків відмивання коштів. У контексті боротьби з відмиванням коштів, рівень звітування є різним у різних державах-членах і необов'язково передбачає подання звітів про підозрілі операції (переважно звіти про валютні операції).

Оцінки органами нагляду рівня ризику у секторі обміну валют є різними, коливаючись від дуже значного до незначного. Основні ідентифіковані поточні ризики включають: анонімність операцій, близькість до прикордонних регіонів і туристичних громад (мігранти, транскордонні працівники, шукачі притулку, туризм) та домінування готівкових операцій. Різні компетентні органи визначають їх як джерело найбільшої занепокоєності.

c) законодавча база і перевірки

Пункти обміну валют підпадають під дію законодавчої бази щодо ПВК/ФТ на рівні ЄС. Органи нагляду не вважають сектор обміну валют сектором високого ризику в цілому; відповідно до цієї оцінки, ресурси для здійснення нагляду за цим сектором є нижчими, ніж в інших секторах. Крім того, багато компетентних органів назвали чинними факторами ризику неналежні внутрішні перевірки, відсутність обізнаності про відповідні регуляторні умови і неналежну практику звітування щодо підозрілої діяльності, незважаючи на здійснення перевірок.

Ще одним фактором, який перешкоджає здійсненню належних перевірок у пунктах обміну, є граничне значення, яке може бути встановлене у різних країнах для застосування зобов'язань щодо належної перевірки клієнтів лише для випадкових операцій; у будь-якому разі більшість держав-членів застосовують граничні значення, нижчі за 15 000 євро.

Висновок: рівень обізнаності у секторі є досить нерівномірним, а здійснювані перевірки не є ефективними з огляду на низький рівень звітування. Компетентні органи не вважають, що правила та заходи нагляду є ефективними. У цьому контексті, рівень вразливості до відмивання коштів, пов'язаної з обміном валют, вважається значним (рівень 3).

Пом'якшувальні заходи:

Для держав-членів/компетентних органів

- Компетентним органам слід здійснити низку тематичних перевірок на місцях, зосереджуючи увагу на ризиках, які створюють агенти. Сфера дії таких тематичних перевірок має включати перевірку наявності у провайдерів послуг з переказу грошових коштів комплексної функції нагляду за агентами, включаючи ефективні системи моніторингу, перевірки на місцях та навчання.
- Держави-члени повинні усунути граничні значення для застосування належної перевірки клієнтів до випадкових операцій у секторі обміну валют з метою покращення моніторингу підозрілих операцій.

8. Сектор електронних грошей

Продукт
Електронні гроші

Сектор
Кредитні та фінансові установи

Загальний опис сектора та відповідного продукту/діяльності

«Електронні гроші» відповідно до другої Директиви про електронні гроші (EMD2, 2009/110/ЄС) означають грошову вартість, як представлено у вимозі до емітента, яка зберігається на електронному пристрої, в тому числі магнітному, випускається для отримання коштів з метою здійснення платіжних операцій та приймається фізичною або юридичною особою, відмінною від установи-емітента електронних грошей.

Основною характеристикою електронних грошей є їх попередня оплата. Це означає, що для того, щоб грошова вартість становила електронні гроші, вона має бути зарахована на рахунок, картку чи пристрій. Наприклад, електронні гроші можуть зберігатися на картках, на мобільних пристроях та на онлайн-акаунтах. Залежно від способу зберігання електронних грошей, їх можна класифікувати як «апаратні» або «серверні». Деякі продукти електронних грошей потребують ідентифікації власника; інші дозволяють власникам залишатися анонімними.

Сектор електронних грошей

Віднесення продуктів електронних грошей до першої категорії залежить від технології, яка використовується для зберігання грошової вартості: продукти можуть бути апаратними або програмними.

Що стосується апаратних продуктів, купівельна спроможність полягає у фізичному пристрої, такому як чіп-карта, з функціями захисту на основі апаратних засобів. Переказ грошової вартості зазвичай здійснюється за допомогою зчитувальних пристроїв, які не потребують підключення мережі у режимі реального часу до віддаленого сервера.

Програмні продукти мають спеціальне програмне забезпечення, яке функціонує на звичайних пристроях, таких як комп’ютери або планшети. Для уможливлення переказу грошової вартості, пристрій зазвичай потребує онлайн-з’єднання з віддаленим сервером, який контролює використання купівельної спроможності. Існують також схеми, що поєднують як апаратні, так і програмні функції.

Інші потенційні відмінності між продуктами електронних грошей можуть включати спосіб створення або випуску електронних грошей. Основна відмінність полягає в тому, чи можуть електронні гроші бути передплачені користувачем (платником) або третьою стороною від імені або на користь платника (наприклад, компанією у разі використання карток для корпоративних клієнтів або торговцем у схемах лояльності з кількома торговцями).

Продукти електронних грошей можуть бути перезавантаженими (для додання додаткової вартості після початкового випуску електронних грошей емітентом) або ні.

Те, до якої категорії відносяться електронні гроші, залежить від того, чи є продукт багатофункціональним або пов'язаний з платформою. Обидва типи можуть використовуватися у режимі онлайн, але останній дозволяє здійснювати покупки лише на одній платформі і не допускає переказів між фізичними особами. В обох випадках для завантаження продуктів електронних грошей потрібен банківський рахунок. Інша категорія включає передплачені картки або ваучери із звільненням від належної перевірки клієнтів: ці продукти можуть використовуватися у режимі онлайн або офлайн і можуть бути придбані готівкою.

Не всю грошову вартість, яка зберігається на електронному пристрої, можна вважати електронними грошами у контексті EMD2. Обмежені мережеві продукти, такі як подарункові картки та картки для проїзду у громадському транспорті, які можна використовувати лише з певним роздрібним торговцем або ланцюжком визначених роздрібних торговців, не підпадають під дію EMD2. Крім того, віртуальні валюти, такі як біткойни, не вважаються електронними грошима, оскільки вони не випускаються для отримання коштів.

Опис сектора

Систематична перевірка ринку в частині обсягів та вартості операцій з електронними грошима є складнішою. Незважаючи на те, що Європейський центральний банк (ЄЦБ) виступає центральним джерелом статистичних даних про вартість та обсяг операцій з електронними грошима, існують численні прогалини у даних. За даними ЄЦБ, це обумовлено головним чином тим, що лише держави-члени Єврозони повинні повідомляти статистичну інформацію, а решта держав-членів роблять це добровільно.

Хоча наявні статистичні дані ЄЦБ не дають повного уявлення про розмір ринку електронних грошей, вони видають вказівки щодо порядків величин, пов'язаних з розміром ринку, а також щодо змін у часі.

За даними ЄЦБ щодо ринку електронних грошей, у 2014 році платіжні операції з електронними грошима для 22 держав-членів, які надали дані про платіжні операції з електронними грошима, випущеними провайдерами платіжних послуг, які є резидентами ЄС, на суму 73 млрд євро. Ці 73 млрд євро включають 57 мільярдів євро в Люксембургу (PayPal, Amazon) і 13 мільярдів євро в Італії. Кількість операцій становила 2,09 млрд (у тому числі 1,5 млрд у Люксембургу та близько 300 млн в Італії). Ці дані не є повними, оскільки вони не включають декілька ринків за межами Єврозони, а тому недооцінюють фактичний розмір ринку ЄС. Середня вартість операцій на основі таких даних становила 35 євро. Платежі з використанням електронних грошей становили 3 % від загальної кількості електронних платіжних операцій в Єврозоні (ЄС-18). За п'ятирічний період з 2010 по 2014 роки кількість операцій з використанням електронних грошей у ЄС зросла у 2 рази, а їх вартість – у 2,5 рази.

На основі статистичних даних ЄЦБ ринок передплачених інструментів у 2014 році міг би скласти 19,3 млрд євро, з яких 13 млрд єіро припадали на італійські передплачені картки, які, по суті, розповсюджуються державним органом *Poste Italiane*, а 3,2 млрд євро – на ринок Сполученого Королівства, який є другим за розміром ринком в ЄС. Статистичні дані ЄЦБ не охоплюють обмежених мережевих ринків, включаючи ринок подарункових карток. Однак ці картки не підпадають під дію законодавства про ПВК/ФТ на рівні ЄС або на національному рівні, оскільки їх використання обмежується обмеженими мережами роздрібних торговців або автозаправними станціями (для паливних карток), а отже такі картки створюють низькі ризики відмивання коштів та фінансування тероризму.

Відповідні суб'єкти

Електронні гроші можуть випускатися кредитними установами; установи електронних грошей та жироустанови поштових відділень мають право випускати електронні гроші відповідно до національного законодавства. Електронні гроші також можуть випускатись Європейським центральним банком та національними центральними банками, якщо вони не діють в якості грошового органу або в якості інших державних органів. Держави-члени або їхні регіональні чи місцеві органи влади, діючи у рамках своїх державних повноважень, також можуть випускати електронні гроші.

Більшість емітентів електронних грошей знаходяться у Сполученому Королівстві та Бельгії, а також у Чехії, Південній Кореї, Латвії та Нідерландах.

Що стосується різних бізнес-моделей, у EMD2 передбачено три типи суб'єктів:

- емітент: суб'єкт, який «продає» клієнту електронні гроші (будь то фізична особа або підприємство) в обмін на платіж. Крім того, суб'єкт повинен мати дозвіл на випуск електронних грошей і підпадає під дію EMD2;

- дистриб'ютор: суб'єкт, відмінний від емітента, який може розповсюджувати або викуповувати електронні гроші від імені емітента (тобто він перепродає електронні гроші, видані емітентом, наприклад роздрібна точка продажу, яка продає передплачені картки);

- агент: суб'єкт, який діє від імені емітента електронних грошей, дозволяючи емітенту здійснювати діяльність з надання платіжних послуг (крім випуску електронних грошей) в іншій державі-члені без створення там філії.

На практиці ця різниця може використовуватися консультованими емітентами електронних грошей, насамперед, у контексті транскордонного надання послуг електронних грошей, при цьому вибрані емітенти використовують «партнерів з розповсюдження» для роботи в інших державах-членах[39].

Опис сценарію ризиків

Злочинці використовують характеристики та особливості деяких нових способів оплати, «безпосередньо» використовуючи дійсно анонімні продукти (тобто без будь-якої ідентифікації клієнта) або «опосередковано» шляхом зловживання неанонімними продуктами (тобто обхід заходів верифікації з використанням підроблених або викрадених ідентифікаційних даних чи підставних осіб або кандидатів тощо). Тим не менш, останній варіант є витратним, тому злочинцям простіше мати справу з посередниками у каналі доставки.

Злочинці можуть завантажувати декілька карток відповідно до моделі анонімної передплаченої картки. Це багаторазове перезавантаження може призвести до значних вартостей, які потім можуть бути буті перевезені закордон з обмеженою простежуваністю. Емітенти електронних грошей можуть відстежувати або контролювати операції, тільки якщо використосвуються гроші, що зберігаються на картках.

[39] Висновок Європейської служби банківського нагляду щодо характеру паспортних повідомлень стосовно агентів та дистриб'юторів відповідно до Директиви (ЄС) 2015/2366 (PSD2), Директиви 2009/110/ЄС (EMD2) та Директиви (ЄС) 2015/849 (AMLD) https://eba.europa.eu/documents/10180/2622242/EBA+Opinion+.pdf

Загроза

Фінансування тероризму

Продукти електронних грошей мають певні переваги перед готівковими коштами, якщо йдеться про здійснення онлайн-платежів, і використання таких продуктів не вимагає спеціальних знань. Беручи до уваги невеликі обсяги грошей, необхідних для здійснення терористичних атак, іноді може бути простішим сплатити за деякі продукти чи послуги (готелі, прокат автомобілів) за допомогою електронних грошей, аніж готівкою, навіть якщо злочинці стануть предметом належної перевірки клієнтів, оскільки суми платежів перевищують граничні значенні. З іншого боку, продукти електронних грошей є більш простежуваними, ніж готівкові кошти.

Коли злочинці надсилають гроші у зони конфлікту, використання продуктів електронних грошей може бути безпечнішим, але їх використання як платіжний засіб у цих країнах може бути складнішим, ніж використання готівкових коштів.

Правоохоронні органи зібрали докази того, що електронні гроші, завантажені на передплачені картки, використовуються для фінансування терористичної діяльності, зокрема для надання допомоги терористам у вчиненні атак (наприклад, оренда номера у готелі або прокат автомобіля). Однак загроза використання передплачених карток або електронних грошей для цієї мети не залежить від необхідності проходження належної перевірки клієнтів для отримання доступу до продуктів електронних грошей.

Підводячи підсумок, електронні гроші мають деякі переваги для фінансистів терористичної діяльності порівняно з готівкою. Хоча такі продукти дозволяють здійснювати більш дискретні платежі, порівняно з готівковими коштами, вони мають певні недоліки, якщо використовуються у зонах конфлікту або в частині уникнення відстеження платежів. Рівень загрози не залежить від граничних значень для застосування належної перевірки клієнтів, якщо злочинці не включені до санкційного переліку.

Висновки: електронні гроші, зокрема на передплачених картках, є привабливими для терористичних груп, оскільки забезпечують простий спосіб фінансування їх діяльності. З огляду на низькі використовувані обсяги грошей, вони є дискретним способом здійснення платежів. Однак готівка все ще є переважним способом надіслання грошей у зони конфлікту або для уникнення відстеження. Правоохоронні органи мають докази того, що такий алгоритм дій використовується, але загроза не залежить від граничних значень для застосування належної перевірки клієнтів. У цьому контексті, рівень загрози фінансування тероризму, пов'язаної з електронними грошима, вважається значним (рівень 3).

Відмивання коштів

Оцінка загрози відмивання коштів пов'язана з деякими продуктами на основі готівкових коштів, які можуть використовуватися злочинними організаціями, включаючи країни, які не є членами ЄС, через дистриб'юторів таких продуктів. Продукти електронних грошей мають деякі переваги перед готівковими коштами, якщо йдеться про переміщення таких грошей за межі ЄС або до інших держав-членів. Тим не менш, готівкові кошти залишаються переважним вибором таких груп.

Підрозділи фінансової розвідки виявили численні випадки зловживання електронними грошима (податкові шахрайства, торгівля наркотиками, проституція) шляхом придбання декількох передплачених карток. Правоохоронними органами були виявлені випадки, коли доходи від торгівлі наркотиками відмивали за допомогою передплачених карток. Передплачені картки дозволяють легко переміщувати великі суми. Однак, оскільки використання підставних осіб є

затратним для обходження граничних значень належної перевірки клієнтів та відмивання крупних грошових сум, простіше використовувати агентів, залучених у канал доставки продуктів електронних грошей.

Висновки: На відміну від фінансування тероризму, електронні гроші є привабливими для злочинних організацій з огляду на великі суми використовуваних грошових коштів, особливо коли їх завантажують на передплачені картки або ваучери, звільнені від належної перевірки клієнтів, які можна використовувати у режимі онлайн або офлайн і можна придбати за готівку. Однак з огляду на нижчі граничні значення, потрібен певний зв'язок з агентами або дистриб'юторами емітентів електронних грошей у їх каналах доставки. Тим не менш, злочинні організації надають перевагу використанню готівки, ніж використанню електронних грошей. У цьому контексті, рівень загрози відмивання коштів, пов'язаної з електронними грошами, вважається значним (рівень 3).

Вразливість

Фінансування тероризму

Оцінка вразливості до фінансування тероризму, пов'язаної з електронними грошами, свідчить про таке:

а) схильність до ризику

Сектор електронних грошей не є однорідним, з огляду на широкий асортимент продуктів, для яких рівень ризиків фінансування тероризму та відмивання коштів є абсолютно різним. Деякі продукти електронних грошей, які не пов'язані з поточним рахунком (продукти на основі готівкових коштів[40]), пропонують функції анонімності, подібні до функцій готівкових коштів, оскільки вони звільнені від належної перевірки клієнтів. Ризик фінансування тероризму може бути значним для таких специфічних продуктів електронних грошей з огляду на низькі обсяги, використовувані у терористичних атаках, і той факт, що вони пропонують дискретний спосіб здійснення платежів низького обсягу порівняно з готівковими коштами. Тим не менш, злочинці все ще вважають використання готівки переважною опцією з огляду на повну анонімність.

Ризик фінансування тероризму, пов'язаний з безготівковими електронними грошима, можна вважати аналогічним ризику, пов'язаному з іншими банківськими продуктами або кредитними картками. Незважаючи на те, що походження коштів є відомим, і на повну простежуваність платежів, злочинці можуть використовувати ці продукти в якості платіжного засобу, навіть якщо вони стануть предметом належної перевірки клієнтів. Це обумовлено тим, що більшість часу злочинці не перебувають у межах санкційного режиму.

Що стосується фінансування тероризму, продукти електронних грошей пропонують більш безпечний спосіб переміщення грошей до зон конфлікту для фінансування тероризму, але використання таких продуктів як платіжного засобу в цих районах може бути складнішим.

Притаманний ризик залежить головним чином від структури продукту, але навіть безготівкові електронні гроші можуть створювати значний ризик, якщо кошти є законними, злочинці не включені до санкційоного переліку, і необхідні обсяги грошей є низькими. Цікаво те, що фінансові санкції спрямовані на фізичних осіб або групи, які вже становлять загрозу, тоді як ризик часто створюють фізичні особи, які не підпадають під санкційний режим. У цьому сенсі, ризик фінансування тероризму не залежить від граничних значень або застосовуваних заходів належної перевірки клієнтів.

[40] Продукти грошових коштів, завантажені готівкою не на банківський рахунок або кредитну картку.

b) обізнаність про ризики

Рівень обізнаності сектора може вважатися високим, особливо після здійснення деяких терористичних атак, в яких використовувалися продукти електронних грошей. Однак органи нагляду все ще занепокоєні тим, чи будуть компанії електронних грошей, які продають продукти, звільнені від належної перевірки клієнтів, здатними здійснювати ефективний моніторинг та звітувати про підозрілі операції. З іншого боку, результати тематичних перевірок у секторі показали належний рівень перевірок та оцінки ризиків у перевірених компаніях. Більшість органів нагляду класифікують загальний ризик сектора як «помірно значний» або «значний».

Зростає кількість ініціатив, спрямованих на взаємодію з компетентними органами та правоохоронними органами; вони можуть сприяти підвищенню обізнаності про ризики у секторі та підвищенню ефективності.

c) законодавча база і перевірки

Електронні гроші підпорядковуються положенням щодо ПВК/ФТ на рівні ЄС. Відповідно до П'ятої директиви про боротьбу з відмиванням грошей, продукти електронних грошей користуватимуться перевагами режиму звільнення, що означає, що належна перевірка клієнтів не застосовуватимуться, якщо виконано певні умови. Крім того, граничні значення є нижчими, ніж ті, що передбачені у Четвертій директиві про боротьбу з відмиванням грошей, що пом'якшує анонімність певних продуктів. З іншого боку, Директиви про боротьбу з відмиванням грошей вимагають від емітентів електронних грошей здійснення достатнього моніторингу операцій для застосування звільнень від належної перевірки клієнтів.

Наявність ефективних перевірок стосовно фінансування тероризму може вимагати великої кількості персоналу у сфері ПВК/ФТ, що може впливати на бізнес-модель невеликих компаній електронних грошей та знизити ефективність їх систем моніторингу, навіть якщо вони мають належні програмні засоби для моніторингу операцій. У цьому сенсі, якщо йдеться про ризики фінансування тероризму, ефективність перевірок не залежить від застосовуваних заходів належної перевірки клієнтів і більше залежить від якості баз даних, що перевіряються, для виявлення операцій та клієнтів, пов'язаних з фінансуванням тероризму. Взаємодія сектора з компетентними органами та правоохоронними органами має вирішальне значення для підвищення ефективності та зменшення таких ризиків.

Висновки: Нижчі граничні значення, передбачені у П'ятій директиві про боротьбу з відмиванням грошей, зменшать анонімність найбільш ризикованих продуктів, а отже вразливість сектора. Обізнаність про ризики підвищилася, як підтвердили деякі органи нагляду, але все ще мають місце певні занепокоєння щодо ефективності їх систем моніторингу та звітування про підозрілі операції, пов'язані з діяльністю з фінансування тероризму. У цьому контексті, рівень вразливості до фінансування тероризму, пов'язаної з електронними грошима, вважається значним (рівень 3).

Відмивання коштів

Оцінка вразливості до відмивання коштів, пов'язаної з електронними грошима, свідчить про таке:

a) схильність до ризику

Серед широкого асортименту продуктів електронних грошей, продуктами, які є найбільш схильними до ризику відмивання коштів, є ті, що можна придбати за готівку. Використання цих продуктів окремо для цілей відмивання коштів є затратним з огляду на нижчі граничні значення та витрати на наймання підставних осіб для обходу граничних значень для застосування належної перевірки клієнтів. Однак, коли деякі посередники діють у каналі доставки продукту електронних грошей (дистриб'ютори, агенти), це може стати найслабшою частиною системи запобігання протидії відмиванню грошей, якщо компанії не в змозі здійснювати ефективний моніторинг мережі своїх дистриб'юторів.

Злочинці або фасилітатори можуть мати зовнішню угоду з цими агентами чи дистриб'юторами для придбання великої кількості передплачених карток та переміщення цих коштів через держави-члени або країни, які не є членами ЄС, або навіть для продажу такої кількості передплачених карток зі знижкою третім сторонам. Якщо компанії електронних грошей не здійснюють надійних перевірок мережі своїх дистриб'юторів і виявлять потенційних недобросовісних дистриб'юторів, такі дистриб'ютори будуть здатні уникнути заходів належної перевірки клієнтів та внести у систему підроблені документи аналогічно тому, як це відбувається з недобросовісними агентами компаній з переказу грошей. Як наслідок, ризик, притаманний моделям розповсюдження, визначається, насамперед, залежно від міри, якою електронні гроші розповсюджуються особами, відмінними від емітенту електронних грошей.

Притаманний ризик відмивання коштів є значно нижчим для решти продуктів електронних грошей, пов'язаних з банківським рахунком або платіжним рахунком.

b) обізнаність про ризики

Сектор покладається на використання технологій для перевірки продуктів електронних грошей і оцінює ризик відмивання грошей, що його становлять його продукти, навіть передплачені картки або ваучери на основі готівки, як «незначний» або «помірно значний». Емітент електронних грошей має доступ до продукту у будь-який момент і має ресурси для дезактивації карт у разі підозрілих операцій. Більшість органів нагляду оцінюють загальний ризик сектора як «помірно значний» або «значний». Різниця у сприйнятті між сектором та органами нагляду, головним чином, обумовлена різними поглядами на те, наскільки ефективними є перевірки емітентів електронних грошей в частині ПВК/ФТ. З іншого боку, в одній державі-члені ЄС, де було видано багато ліцензій, орган нагляду нещодавно здійснив тематичну перевірку у секторі та виявив, що перевірені компанії мають належний рівень перевірок та оцінки ризиків.

c) законодавча база і перевірки

Електронні гроші підпадають під дію положень щодо ПВК/ФТ на рівні ЄС. Відповідно до П'ятої директиви про боротьбу з відмиванням грошей, продукти електронних грошей користуються перевагами режиму звільнення, що означає, що вимоги щодо належної перевірки клієнтів не застосовуватимуться, якщо виконані конкретні умови. Крім того, граничні значення є нижчими, ніж ті, що передбачені у Четвертій директиві про боротьбу з відмиванням грошей, що пом'якшує анонімність певних продуктів. З іншого боку, Директиви про боротьбу з відмиванням грошей вимагають від емітентів електронних грошей здійснення достатнього моніторингу операцій для застосування звільнень від належної перевірки клієнтів.

Органи нагляду виявили слабкі сторони, зокрема, в ефективності моніторингу, ідентифікації підозрілих операцій, а також внутрішніх перевірках та нагляді. Однак цей сектор переважно покладається на моніторинг операцій як на інструмент пом'якшення ризиків, що включає ефективний контроль мережі дистриб'юторів. Однак варто зазначити, що контроль крупної мережі дистриб'юторів може потребувати додаткового персоналу на додаток до технологій, що збільшує рівень вразливості у невеликих компаніях електронних грошей.

Висновки: через вищий рівень анонімності продукти електронних грошей на основі готівки є більш вразливими, ніж інші продукти електронних грошей на основі банківських рахунків. Рівень обізнаності щодо відмивання коштів у секторі є високим, але органи нагляду все ще мають сумніви стосовно систем моніторингу, зокрема, у зв'язку з крупними мережами дистриб'юторів та продуктами електронних грошей на основі готівкових коштів. У цьому контексті, рівень вразливості до відмивання коштів, пов'язаної з електронними грошима, вважається помірно значним/значним (рівень 2/3).

Пом'якшувальні заходи:

Для держав-членів/компетентних органів:

- транспозиція положень П'ятої директиви про боротьбу з відмиванням грошей, пов'язаних з електронними грошима;
- тематичні перевірки на місцях з акцентуванням уваги на ризику, який створюють дистриб'ютори.

9. Переказ коштів

Продукт
Переказ коштів

Сектор
Кредитні та фінансові установи – Послуги переказу грошових коштів

Загальний опис сектора та відповідного продукту/діяльності

Переказ грошових коштів або грошовий переказ визначається відповідно до другої Директиви про платіжні послуги (PSD2) як платіжна послуга, коли кошти отримуються від платника без створення жодних платіжних рахунків на ім'я платника або одержувача платежу, з єдиною метою переказу відповідної суми одержувачу або іншому провайдеру платіжних послуг, який діє від імені одержувача, та/або коли такі кошти отримуються від імені одержувача і надаються одержувачу.

Основним прикладом переказів грошових коштів є послуга переказу, що пропонується крупними провайдерами мережі агентств (системи переказу грошових коштів (MVTS)), коли платник передає готівкові кошти агенту провайдера платіжних послуг, щоб вони були надані одержувачу платежу через іншого агента.

Статистичні дані

Грошові перекази – це платіжна послуга, яку можуть надавати провайдери платіжних послуг, включаючи кредитні установи, установи електронних грошей та уповноважені платіжні установи. Грошові перекази – це платіжна послуга, на надання якої найчастіше мають дозвіл уповноважені платіжні установи.

Відповідно до загальної статистики ЄЦБ, у 2017 році загальна сума грошових переказів, надісланих з держав-членів ЄС, становила 270 млрд євро, але ця цифра не включає Сполучене Королівство, Люксембург, Польщу, Словаччину, Данію, Кіпр та Фінляндію. Цей показник свідчить лише про незначне збільшення порівняно з 2016 роком (240 млрд євро).

Ринковий ландшафт показує, що існують різні типи провайдерів послуг з переказу грошових коштів. Це відображено у Директиві про платіжні послуги, яка передбачає існування «зареєстрованих провайдерів послуг з переказу грошових коштів» та «уповноважених провайдерів послуг з переказу грошових коштів».

Опис сценарію ризиків

Фінансування тероризму

Злочинці використовують послуги з переказу грошей та грошових коштів, що надаються фінансовими установами, для розміщення та/або переказу коштів у формі готівки або анонімних електронних грошей (операції, які не базуються на рахунках). Вони використовують послуги провайдерів послуг з переказу грошових коштів для швидкого переказу сум через юрисдикції, як правило, надаючи перевагу серії операцій незначної вартості, щоб уникнути тривожних сигналів.

Відмивання коштів

Злочинці можуть використовувати послуги провайдерів послуг з переказу грошових коштів для здійснення низки незаконних операцій. Такі операції перелічені нижче.

- Переказ коштів від законних та незаконних клієнтів. Агенти-шахраї зазвичай здійснюють операції, використовуючи підроблені ідентифікаційні дані та підроблені рахунки-фактури.

- Доходи від злочинної діяльності відмиваються через розрахункові системи у країні, яка не є членом ЄС (використовуючи паспорт). Провайдери послуг з переказу грошових коштів спрямовують кошти через дуже складні платіжні ланцюги з великою кількістю посередників та юрисдикцій, які беруть участь у схемі, що перешкоджає відстеженню незаконних коштів. Провайдери послуг з переказу грошових коштів, що працюють через платіжний ланцюг, часто встановлюють офіційні та/або неофіційні розрахункові системи (часто разом з методами відмивання коштів на основі торговельної діяльності), також перешкоджаючи відстеженню незаконних коштів.

- Крупні суми готівки розбиваються на менші суми, які є нижчими за граничні значення, для яких потрібні більш суворі заходи ідентифікації клієнтів.

- Доходи від злочинної діяльності розміщуються у фінансовій системі через регульованого провайдера послуг з переказу грошових коштів, який пропонує платіжні рахунки або подібні продукти. Злочинці можуть також використовувати таких регульованих провайдерів послуг з переказу грошових коштів для спрямування своїх коштів.

- Кошти розміщуються та/або переказуються шляхом грошових переказів. Ризики відмивання грошей/фінансування тероризму можуть бути особливо високими, якщо кошти, які мають бути переказані, надходять у формі готівки або анонімних електронних грошей.

Загроза

Фінансування тероризму

Оцінка загрози фінансування тероризму, пов’язаної з послугами переказу грошових коштів, свідчить про те, що терористичні групи періодично використовують цей метод. Правоохоронні органи та підрозділи фінансової розвідки зібрали вагомі докази того, що ці послуги використовуються для збирання та переказу коштів, що використовуються для підтримки фінансування терористичної діяльності у межах ЄС, зокрема для переказу коштів іноземними терористами-бойовиками або для іноземних терористів-бойовиків, які подорожують до/з зон конфлікту.

Провайдери послуг з переказу грошових коштів, залежно від їх організації, є легкодоступними, і терористи не потребують спеціальних знань чи методів для зловживання такими послугами для цілей фінансування терористичної діяльності. Терористів можуть більше приваблювати крупні провайдери послуг з переказу грошових коштів з огляду на їх глобальну мережу агентів, тоді як менші провайдери послуг з переказу грошових коштів можуть бути не настільки привабливими, оскільки вони зазвичай працюють в обмеженій кількості країн. Специфічною особливістю провайдерів послуг з переказу грошових коштів (див. частину про вразливість) є те, що вони

сприймаються як привабливі та безпечні.

Висновки: Провайдери послуг з переказу грошових коштів часто використовуються для фінансування терористичної діяльності і не потребують спеціальних знань чи планування. У цьому контексті, рівень загрози відмивання коштів, пов'язаної з послугами переказу грошових коштів, вважається значним (рівень 4).

Відмивання коштів

Організовані злочинні групи періодично використовують цей метод. Правоохоронні органи та підрозділи фінансової розвідки зібрали вагомі докази того, що ці послуги використовуються для збирання та переказу коштів, що використовуються для підтримки діяльності з відмивання коштів. Провайдери послуг з переказу грошових коштів, залежно від їх організації, є легкодоступними і не вимагають спеціальних знань чи методів для відмивання доходів від злочинної діяльності. Специфічною особливістю провайдерів послуг з переказу грошових коштів є те, що вони сприймаються як привабливі та безпечні. Зазвичай злочинці контактують з агентами, щоб відмити гроші організованої злочинної групи в обмін на відсоток від суми відмитих грошей. Агенти, пов'язані з цими злочинцями, зазвичай здійснюють фальшиві операції з підробленими ідентифікаційними даними клієнтів, якщо їм відомо про слабкі належні перевірки клієнтів в компанії, що надає послуги переказу грошових коштів. В іншому випадку вони можуть використовувати реальних клієнтів для додавання нових операцій.

Виходячи з принципу неексклюзивності, агенти можуть працювати на різні компанії одночасно. Це означає, що, якщо вони пов'язані із злочинцями, агенти можуть легко розділяти операції між компаніями з метою відмивання крупних сум; таку діяльність важко виявити для окремих компаній та компетентних органів.

Висновки: Провайдери послуг переказу грошових коштів часто використовуються для відмивання грошей і не потребують спеціальних знань чи планування. У цьому контексті, рівень загрози відмивання коштів, пов'язаної з послугами переказу грошових коштів, вважається дуже значним (рівень 4).

Вразливість

Фінансування тероризму

а) схильність до ризику

Покладання на операції на основі готівкових коштів та постійне використання таких послуг у зонах високого ризику призводять до високої схильності до ризиків. Якщо гроші використовуються для терористичних атак в ЄС, вищий ризик є наслідком надсилання незначних сум та не включення платників до санкційного переліку.

Сектор є вразливим до транскордонних зловживань з метою фінансування тероризму. Розслідування, проведені правоохоронними органами після останніх терористичних атак, наприклад, у Парижі та Сполученому Королівстві, підтвердили, що терористи використовували грошові перекази для одержання та переміщення коштів. На відміну від тих, хто відмиває гроші, особи, які мають намір фінансувати терористичну діяльність, необов'язково повинні приховувати свою особу і можуть використовувати законні джерела фінансування, часто у невеликих сумах. Крім того, ризик фінансування тероризму часто походить від осіб, які не підпадають під дію санкційного режиму.

Значний ризик відмивання коштів та фінансування тероризму у секторі послуг переказу

грошових коштів змусив банки прийняти політику «зниження ризиків» щодо послуг переказу коштів у деяких регіонах з вищим ризиком. Ця тенденція викликає занепокоєння, оскільки зниження ризиків у кінцевому рахунку може призвести до того, що послуги грошових переказів ставатимуть підпільними (тобто, неофіційні провайдери послуг, такі як послуги «хавала»). Також виникають занепокоєння щодо фінансового включення, оскільки послуги грошового переказу відіграють важливу роль для клієнтів, які мають обмежений доступ або взагалі не мають доступу до інших регульованих фінансових послуг.

b) обізнаність про ризики

На думку компетентних органів, рівень обізнаності про ризики у секторі є високим (з причини нещодавніх терористичних атак), але заходи, які вживають компанії для ідентифікації своїх клієнтів та верифікації їх особи, можуть бути менш вагомими у контексті боротьби з фінансуванням тероризму, ніж ефективний постійний моніторинг операцій. Правоохоронні органи зауважують, що більш крупні гравці частіше використовуються терористами, ніж менші, з огляду на наявність крупніших мереж агентів у різних країнах.

Боротьба з фінансуванням тероризму все ще стикається з перешкодами, коли компанії не мають доступу до відповідної інформації, якою часто володіють правоохоронні органи, що допомогла би їм виявити ризики, пов'язані з фінансуванням тероризму, до реалізації таких ризиків. Аналогічно, зусиллям правоохоронних органів щодо стримування терористичної діяльності і мереж може перешкоджати їх нездатність отримати інформацію про фінансові потоки, яку можуть надати лише компанії.

Більшість органів нагляду вважають загальний рівень ризику цього сектора значним або дуже значним, і понад 50 % компаній у секторі оцінюються як компанії дуже значного ризику.

c) законодавча база і перевірки

Зареєстровані та уповноважені провайдери послуг переказу грошових коштів підпорядковуються вимогам в області ПВК/ФТ на рівні ЄС. Ефективність здійснюваних перевірок органи нагляду оцінюють переважно як низьку. Компанії у секторі, особливо крупні компанії, покладаються на свої перевірки клієнтів та системи оповіщення для пом'якшення ризиків.

Ефективність діючих систем для виявлення підозрілих операцій, пов'язаних з фінансуванням тероризму, є невисокою, незважаючи на їх інтенсивність у галузі людських ресурсів. Крім того, ризик фінансування тероризму часто походить від осіб, які не підпадають під дію санкційного режиму. Як результат, необхідна тісніша співпраця між компаніями та правоохоронними органами, щоб вони стали більш ефективними у виявленні клієнтів, пов'язаних з терористичною діяльністю.

Висновки: Рівень вразливості до фінансування тероризму, пов'язаної з послугами переказу грошових коштів, є високим. Це пояснюється тим, що особливості операцій, пов'язаних з фінансуванням тероризму, нелегко виявити, незважаючи на людські та технічні ресурси, якими володіють компанії. Ефективність перевірок залежить від джерел інформації, що використовуються для перевірки операцій та клієнтів. Компанії та правоохоронні органи повинні покращити обмін інформацією, щоб посилити виявлення підозрілих операцій, пов'язаних з фінансуванням тероризму. У цьому контексті, рівень вразливості до фінансування тероризму, пов'язаної з послугами переказу грошових коштів, вважається значним/дуже значним (рівень 3/4).

Відмивання коштів

Вразливість до відмивання коштів, пов’язана з послугами переказу грошових коштів, не може бути оцінена без урахування того, що більшість провайдерів послуг переказу грошових коштів покладаються на агентів. Тому агенти є основним фактором схильності до ризиків для провайдерів послуг переказу грошових коштів.

a) схильність до ризику

У ряді випадків послуги провайдерів послуг переказу грошових коштів ґрунтуються на готівкових коштах та дозволяють здійснювати швидкі операції. З огляду на свої особливості та, зокрема, залежність від агентів, послуги переказу грошових коштів можуть надаватися у країнах з високим рівнем ризику, які не є членами ЄС, і можуть використовуватися клієнтами з високим ризиком, які повинні підлягати спеціальному моніторингу та перевіркам. Тому найпоширенішими ризиками у секторі послуг переказу грошових коштів є готівкомісткий характер послуги, висока швидкість та обсяг переказів (хоча окремі операції зазвичай є низькими) та перекази до юрисдикцій високого ризику.

Здійснення відповідної належної перевірки клієнтів може бути проблематичним з огляду на характер клієнтів, які зазвичай здійснюють поодинокі операції, а також з огляду на ризик того, що будуть використовуватися підставні особи для здійснення операцій (незважаючи на те, що це більш затратний метод відмивання грошей). Однак притаманний ризик є вищим, якщо компанії, які здійснюють переказ коштів, не мають надійних систем моніторингу для перевірки мереж роздрібних агентів, особливо у компаніях з крупними мережами роздрібних агентів.

Значний ризик відмивання коштів та фінансування тероризму у секторі послуг переказу грошових коштів змусив банки прийняти політику «зниження ризиків» щодо послуг грошового переказу у деяких регіонах з вищим ризиком. Ця тенденція викликає занепокоєння, оскільки зниження ризиків у кінцевому рахунку може призвести до того, що послуги грошових переказів ставатимуть підпільними (тобто, неофіційні провайдери послуг, такі як послуги «хавала»). Також виникають занепокоєння щодо фінансового включення, оскільки послуги грошового переказу відіграють важливу роль для клієнтів, які мають обмежений доступ або взагалі не мають доступу до інших регульованих фінансових послуг.

b) обізнаність про ризики

Рівень обізнаності про ризики у секторі можна вважати високим. Перевірки в цілому є ефективними, якщо вони фокусуються на ризику клієнта; однак, якщо йдеться про ризик відмивання коштів з боку недобросовісних агентів, то перевірки не є настільки ефективними у країнах ЄС. Крім того, у деяких країнах встановлені граничні значення для зобов’язань щодо належної перевірки клієнтів, які ускладнюють належний контроль агентів. У цьому сенсі, також варто зазначити, що сектор є дуже конкурентоспроможним і має низькі маржі прибутку, тому іноді має місце компроміс між прибутковістю та дотриманням норм. Зазвичай найбільш прибутковими є агенти, пов’язані з відмиванням коштів. Отже, якщо компанії не в змозі виявити чіткий зв’язок з такою діяльністю, вони вважають за краще мати у своїх мережах агента, але контролювати його (зазвичай встановлюючи кількісні обмеження щодо їх операцій), а не повідомляти про агента у відділ фінансової розвідки і таким чином розірвати комерційні відносини.

Обізнаність органів нагляду про такі ризики є високою. У своїх оцінках ризику деякі органи нагляду вказали на такі ризики, пов'язані з мережами агентів: неналежне управління агентами, навчання та моніторинг. Але більшість органів нагляду вважають обізнаність сектора неналежною або поганою.

Звітування про підозрілі операції підрозділам фінансової розвідки не завжди є ефективним, якщо

компанії звітують про великі кількості окремих операцій з клієнтами замість звітування про агентів або групи агентів, що здійснюють такі операції.

c) законодавча база і перевірки

Зареєстровані та уповноважені провайдери послуг переказу грошових коштів підпорядковуються вимогам щодо ПВК/ФТ на рівні ЄС. Через залежність від агентів, нагляд за сектором є дуже складним завданням. Компанії покладаються на нові технології та програмне забезпечення для здійснення надійної належної перевірки клієнтів та нагляду за агентами, але через специфічні особливості їх клієнтів такі заходи не завжди є ефективними. Провайдерам послуг з переказу грошових коштів потрібна підготовка для здійснення належної перевірки клієнтів, але така підготовка не є ефективною, якщо йдеться про усунення ризику, створюваного недобросовісними агентами.

Транскордонна співпраця наразі не працює належним чином, і органи нагляду не в змозі здійснювати належні перевірки та запровадити належний санкційний режим. У цьому разі одна з цілей Четвертої та П'ятої директив про боротьбу з відмиванням грошей полягає у посиленні співпраці між органами нагляду в області ПВК. У цьому контексті створення «колегій органів нагляду в області ПВК», якщо зобов'язані суб'єкти працюють у різних юрисдикціях, може покращити нагляд в ЄС.

Висновки: Притаманний ризик є високим, але обізнаність про ризики у компаніях зростає. Органи нагляду та компанії намагаються усунути ризик відмивання коштів, зосереджуючи свої дії на сферах підвищеної уразливості, таких як контроль агентів. Однак для зменшення вразливості все ще потрібні деякі поліпшення, такі як посилена співпраця в області нагляду та більш ефективна належна перевірка клієнтів і контроль агентів. У цьому контексті, рівень вразливості до відмивання коштів, пов'язаної з послугами переказу грошових коштів, вважається значним (рівень 3).

Пом'якшувальні заходи:

Для держав-членів/компетентних органів:

- Держави-члени повинні усунути граничні значення для випадкових операцій, застосовуючи належну перевірку клієнтів до всіх операцій, щоб компанії, які надають послуги з переказу грошових коштів, могли ефективно контролювати та виявляти підозрілі операції та підозрілих агентів, пов'язаних із особами, що відмивають кошти.

- Створити та просувати систему, в якій підозрілі агенти, про яких звітують компанії, що надають послуги з переказу грошових коштів, заносяться у базу даних, до якої мають доступ усі компанії у секторі. Це може обмежити або усунути діяльність підозрілих агентів.

- Компетентні органи повинні здійснювати тематичні перевірки на місцях, зосереджуючи увагу на ризиках, які створюють агенти. Сфера дії таких тематичних перевірок має включати перевірку наявності у провайдерів послуг з переказу грошових коштів комплексної функції контролю агентів, включаючи ефективні системи моніторингу, перевірки на місцях та навчання.

Для європейських органів нагляду:

- Заохочувати компетентні органи виділяти відповідні ресурси, пропорційні рівню ризиків, для здійснення перевірок послуг з переказу грошових коштів, фокусуючи увагу на контролі агентів.

Для Комісії:

Сприяти співпраці між правоохоронними органами та фінансовими установами для підвищення ефективності систем оповіщення про фінансування тероризму на наднаціональному рівні.

10. Незаконний переказ коштів – Система «хавала»

Продукт
Незаконний/неформальний переказ коштів через систему «хавала»

Загальний опис

«Хавала» – це система переказу грошових коштів, яка забезпечує здійснення переказу та отримання грошових коштів або еквівалентної вартості. Вона часто використовує зв'язки у конкретних географічних регіонах чи етнічних спільнотах. Такі переміщення вартості можуть регулюватися через торгові або готівкові підприємства, які займаються грошовими переказами. Вони часто функціонують у районах еміграційних громад. *«Хаваладари»* (ті, хто працюють з системою «хавала») часто займаються паралельною діяльністю, зокрема обмін валют, туристичні агентства або магазини мобільного зв'язку, або навіть працюють агентами офіційних провайдерів послуг грошових переказів. Термін «хавала» часто використовується для опису низки різних неформальних систем переказу коштів, які мають подібні властивості та працюють схожим чином, хоча і не є системою «хавала». Такі перекази коштів згідно із законодавством ЄС вважаються нерегульованими платіжними послугами, що означає, що вони є незаконними у межах ЄС. Неформальні системи переказу коштів, такі як *«хавала»*, можуть використовуватися для законних цілей, наприклад, для здійснення грошових переказів, а також для кримінальних цілей.

У 2013 році для опису такої діяльності Групою з розробки фінансових заходів боротьби з відмиванням грошей (FATF) був винайдений ширший термін «хавала та інші подібні провайдери послуг» (HOSSP). HOSSP – це субнабір неформальних послуг з переказу коштів; форми, відмінні від системи «хавала», включають «хунді», китайський підпільний банківський бізнес та обмін песо на чорному ринку. Неформальні системи переказу коштів використовуються для переміщення коштів без потреби у фізичному чи електронному переміщенні грошей.

HOSSP широко використовуються членами діаспор та міграційних громад для спрямування законних переказів до своєї країни походження. Одночасно з цим, запровадження більш жорстких положень щодо боротьби з відмиванням грошей у крупних фінансових установах також зробило неформальні системи переказу коштів та HOSSP ще привабливішими для організованих злочинних груп, які часто використовують їх для здійснення незаконних грошових переказів, тобто переказу крупних сум злочинних доходів або відмивання таких злочинних доходів, надаючи послуги заплутування слідів та переказу коштів у межах та за межами ЄС.

Платежі у системі «хавала» – це неформальні перекази коштів, які здійснюються без участі уповноважених фінансових установ. У принципі, гроші фізично не переміщуються від платника до одержувача. Натомість, як це часто трапляється у грошових переказах, це відбувається за рахунок компенсації балансів між хаваладаром платника та хаваладаром одержувача. Тобто, хаваладар з країни А (ХА) отримує кошти в одній валюті від платника і, в свою чергу, надає платнику код для цілей аутентифікації. Після цього він доручає кореспонденту країни В (ХВ) доставити еквівалентну суму у місцевій валюті визначеному бенефіціару, який повинен розкрити код для отримання коштів. Після переказу коштів ХА має зобов'язання перед ХВ, і врегулювання їх позицій здійснюється різними способами, будь то фінансовими або у формі товарів та послуг.

Як правило, всі оператори, що надають платіжні послуги, як визначено у пункті 6 Додатка I другої Директиви про платіжні послуги (PSD2), мають бути належним чином зареєстровані та врегульовані. Такі провайдери повинні отримати статус уповноважених платіжних установ. Нещодавні значні зусилля правоохоронних органів безперечно показали, що нерегульований та підпільний характер неформальних систем переказу коштів HOSSP зробив їх переважним вибором злочинців для відмивання коштів.

Хоча хаваладари мають бути зареєстровані та належним чином ліцензовані відповідно до Директиви про платіжні послуги, такі провайдери платіжних послуг часто приймають рішення здійснювати такі перекази нерегулярно, поза межами звичайної банківської системи та без належного ліцензування. Це означає, що вони обходять свої зобов'язання щодо боротьби з відмиванням коштів та уникають обов'язкового нагляду відповідно до положень щодо протидії відмиванню коштів. Часто органам влади не вистачає засобів для виявлення таких мереж та належного забезпечення виконання такими провайдерами зобов'язань, передбачених у другій Директиві про платіжні послуги та Директиві про боротьбу з відмиванням грошей.

Опис сценарію ризиків

На відміну від усіх інших систем грошових переказів, в основі системи «хавала» лежить мережа основних суб'єктів (хаваладари), пов'язаних лише принципами довіри з огляду на певні географічні регіони, родини, племена, етнічні спільноти, національності, комерційну діяльність тощо. Хаваладари розраховуються за операціями один з одним протягом тривалого періоду часу шляхом здійснення чистого розрахунку через банківські канали, торговельну діяльність або готівковими коштами. Це означає, що на відміну від усіх інших систем переказів, кошти не переказуються за кожну окрему операцію. Натомість кожен день вони використовують місцевий пул готівкових коштів, що містить гроші, які вже наявні у системі, для здійснення платежу бенефіціару. По закінченні встановленого періоду (як правило, через 2-3 місяці) виплачується лише чиста сума. Хаваладари агрегують місяці коштів, отриманих через окремих суб'єктів, що надають послуги переказу, а потім здійснюють розрахунки. Необхідно підкреслити, що законні та ліцензовані послуги переказу коштів також надаються таким чином.

Мережа «хавала» також використовує деякі унікальні методи:

- двосторонній розрахунок: «зворотна хавала» між двома хаваладарами;
- багатосторонній розрахунок: тристоронні, чотиристоронні або інші домовленості між кількома хаваладарами в одній мережі;
- розрахунок за допомогою торговельних операцій, зазвичай із застосуванням методу відмивання грошей на основі торговельної діяльності (відвантаження еквівалентної вартості через торговельні операції, такі як товари, погашення заборгованості або рахунок-фактура на ту саму вартість, яку вони мають сплатити, недооцінення або переоцінення суми у рахунку-фактурі, подвійне виставлення рахунка-фактури, обмін песо на чорному ринку тощо);
- розрахунок готівкою через транскордонних кур'єрів готівкових коштів, банківські послуги та канали грошових послуг.

Для задоволення виключно злочинних потреб створюються спеціальні мережі «хавала»; вони використовуються для розміщення та заплутування слідів одержаних злочинним шляхом коштів та сплати еквівалентної вартості на вимогу в інших країнах. Такі мережі, як відомо, використовують методи, описані вище. Крім того, для цілей власного захисту мережі «хавала» використовують наступні методи:

- швидкі перекази готівки;

- автентифікація через чип (звичайною особливістю злочинних передач готівкових грошей є використання унікального серійного номера на банкноті, який діє як засіб ідентифікації, та найпростіша квитанція за передачу);
    - розміщення за схемою «зозулене смурфування» (cuckoo smurfing) (форма відмивання грошей, пов'язана з альтернативними системами грошових переказів, при яких злочинні кошти переказуються через рахунки нічого не підозрюючих осіб, які очікують справжніх коштів або платежів з-за кордону).

Усі ці методи є унікальними для системи «хавала» та є відомими тривожними сигналами діяльності «хавала» для правоохоронних органів ЄС.

Такі злочинні мережі «хавала» також мають певну структуру, що складається з:

- контролерів або грошових брокерів – вони укладають угоду з організованими злочинними групами щодо збирання брудної готівки та доставки її вартості до обраного місця призначення;
- координаторів – це посередники, які працюють на контролера та керують особами, що збирають кошти;
- осіб, що збирають кошти – вони збирають брудні гроші у злочинців та розпоряджаються ними;
- відправників – вони отримують та відправляють гроші, отримані особою, що збирає кошти (як правило, оператором грошових послуг).

Загроза

Обсяги застосування системи *«хавала»* в ЄС невідомі.

Відомо, що система *«хавала»* асоціюється з деякими видами діяльності певних етнічних спільнот (Індія, Афганістан, Пакистан, Іран, Об'єднані Арабські Емірати, Сомалі та Китай), які є поширеними в ЄС. Прикладами таких видів діяльності є туристичні агентства, ломбарди, точки продажу мобільних телефонів та SIM-карт, пункти поповнення мобільних карт, продуктові магазини, імпорт/експорт, а також різні види суміжного бізнесу, такі як манікюрні салони, перукарні, салони краси, магазини квітів.

Європолу відомо також про декілька розслідувань в області відмивання коштів на суми у декілька мільйонів євро за участі злочинної системи «хавала».

Будь-які прямі потоки грошей/вартості між відправником та одержувачем, які могли би відстежити правоохоронні органи, відсутні. Це робить практично неможливим відстеження потоку грошей/вартості у мережі «хавала», навіть у разі вилучення бухгалтерських книг – вони, як правило, зашифровані, і все частіше розміщуються на хмарних серверах, розташованих у юрисдикціях, що не є партнерами. Така непрозорість приваблює злочинців.

Правоохоронні органи виявили певне перетинання формальних та неформальних систем переказу коштів, зокрема, при використанні «зозуляного смурфування» (cuckoo smurfing). З іншого боку, *хаваладари* можуть відмивати крупні суми готівки для різноманітних доходів від злочинної діяльності (торгівля наркотиками, ухилення від сплати податків, фінансування тероризму тощо). Особа, яка збирає кошти/хаваладар отримує комісію у розмірі від 2 % до 10 %.

Вразливість

Такі незаконні перекази коштів згідно із законодавством ЄС вважаються нерегульованими платіжними послугами, що означає, що вони є незаконними у межах ЄС. У контексті звіту про наднаціональну оцінку ризиків немає спеціальної оцінки вразливості для незаконних послуг.

Пом'якшувальні заходи:

Для держав-членів/компетентних органів:

- Створення спільних груп з розробки фінансових заходів боротьби з відмиванням грошей. Забезпечення співпраці між фінансовим сектором та державними установами щодо обміну результатами розслідування для запобігання відмиванню коштів (що також може поширюватися на послуги «хавала»).
- Здійснення заходів з нагляду для перевірки того, що зобов'язані суб'єкти, особливо суб'єкти, які надають послуги з переказу грошових коштів, здійснюють перевірки для виявлення хаваладарів, використовуючи зареєстрованих агентів як прикриття для залучення клієнтів, щоб запропонувати їм послуги системи «хавала».

11. Платіжні послуги

Продукт
Платіжні послуги

Сектор
Кредитний та фінансовий сектор

Загальний опис сектора та відповідного продукту/діяльності

Продукти платіжних послуг

Платіжні послуги регулюються переглянутою Директивою про платіжні послуги (2015/2366) (PSD2). Вони перелічені у Додатку I до PD2 та охоплюють широкий спектр послуг, включаючи:

- послуги, що уможливлюють розміщення або зняття готівки з платіжного рахунка (готівкові депозити розглядаються в окремому розділі цього звіту);

- грошові перекази (також висвітлюються в іншому розділі цього звіту);

- здійснення платіжних операцій, таких як кредитні перекази або прямі списання;

- виконання платіжних операцій через платіжні картки або аналогічні пристрої;

- випуск платіжних інструментів;

- набуття платіжних операцій.

«Платіжна операція» визначається як акт, ініційований платником чи від його імені або одержувачем розміщення, переказу або зняття коштів, незалежно від будь-яких основних зобов'язань між платником та одержувачем.

PSD2 охоплює додаткові платіжні послуги, які з'явилися протягом останніх років у процесі цифровізації послуг. Ці послуги називаються послугами ініціювання платежів та інформаційними послугами рахунків. При оцінці відповідного ризику відмивання коштів мають значення лише послуги ініціювання платежів.

Послуги ініціювання платежів дозволяють споживачам оплачувати свої покупки шляхом здійснення простого кредитного переказу замість оплати кредитною карткою (близько 60 % населення ЄС не має кредитної картки). Провайдер послуг з ініціювання платежів може перевіряти, чи є на рахунку споживача достатньо коштів для здійснення платежу. Він повідомляє продавцю, що платіжне доручення було ініційовано успішно. Виходячи з цього, веб-продавець може прийняти рішення про відвантаження товару або надання послуги до того, як буде зарезервована сума на його рахунку. PSD2 охоплює такі нові платежі, враховуючи можливі проблеми щодо конфіденційності, відповідальності та безпеки таких операцій.

PSD2 набрала чинності 13 січня 2018 року. Станом на 8 лютого 2019 року 25 держав-членів повідомили про повну транспозицію Директиви, дві (Мальта та Іспанія) – про часткову транспозицію, а в Румунії Директива ще не транспонована.

Не всі платежі регулюються PSD2. Ця Директива не застосовується до готівкових платежів або платежами на основі паперових чеків. Платіжні операції, здійснювані провайдером електронних комунікаційних мереж, у межах певної вартості також виключаються із сфери дії Директиви.

Переважна більшість платежів здійснюється в електронній формі. Загальна кількість безготівкових платежів в ЄС збільшилася на 7,9 % і становила 134 млрд євро у 2017 році порівняно з попереднім роком:

- платежі кредитними та дебетовими картками становили 52 % від усіх операцій;
- кредитні перекази становили 24 %, а прямі списання – 19 %;
- кількість кредитних переказів зросла на 5,5% і досягла 32,1 млрд євро.

Кількість карток з платіжною функцією в ЄС збільшилася у 2017 році на 2,0 % і досягла 812 мільйонів. При загальній кількості населення в ЄС 513 мільйонів, це становило близько 1,6 платіжних карток на одного жителя ЄС. Кількість операцій з картками зросла на 11,2 % і досягла 69,2 мільярдів на загальну вартість 3,1 трильйони. Це відповідає в середньому приблизно 44 євро на карткову операцію.

Єдиний європейський простір платежів (SEPA)

Єдиний європейський простір платежів (SEPA) спрямований на гармонізацію та інтеграцію платіжних ринків по всій Європі за допомогою одного набору платіжних інструментів в євро: кредитних переказів, прямих списань та платіжних карток, загальних стандартів та практик і гармонізованої законодавчої бази. SEPA охоплює понад 520 мільйонів людей у 28 державах-членах ЄС та шести країнах, які не є членами ЄС (Ісландія, Ліхтенштейн, Монако, Норвегія, Сан-Марино та Швейцарія).

Роздрібні платіжні системи

Роздрібні платіжні системи в ЄС передбачають платежі, що здійснюються громадськістю, на відносно низьку суму, у великому обсязі та з обмеженнями у часі. У 2017 році в цілому в ЄС існувало 43 роздрібні платіжні системи. За цей рік цими системами було оброблено близько 57 мільярдів операцій, що нараховує 44,0 трильйони євро. Близько 22 з цих систем було розміщено в Єврозоні, де вони обробили майже 42 мільярди операцій у 2017 році (тобто 73 % від загальної кількості в ЄС), покривши вартість у розмірі 31,6 трлн євро (тобто 72 % від загальної кількості в ЄС).

Системи платежів крупними сумами

Системи платежів крупними сумами призначені в основному для обробки термінових або крупних міжбанківських платежів, але деякі з них також здійснюють велику кількість роздрібних платежів. Протягом 2017 року 12 систем здійснили 842 мільйони платежів на загальну суму 702 трлн євро в ЄС. Дві основні системи платежів крупними сумами в Єврозоні (TARGET2 та EURO1/STEP1) здійснили 143 мільйони операцій на суму 528 трлн євро у 2017 році, тобто 75 % від загальної вартості.

Провайдери платіжних послуг

Банки є учасниками національних та міжнародних платіжних систем. Близько 122 мільярдів безготівкових платежів було здійснено негрошовими фінансовими установами у 2016 році на рівні ЄС-28. Більше половини (60 мільярдів) з них були картковими платежами, тоді як приблизно чверть – кредитними переказами (31 мільярд) або прямими списаннями (25 мільярдів).

У межах ЄС платіжні послуги можуть надаватися не лише кредитними установами. Вони також можуть надаватися установами електронних грошей, установами поштового зв'язку та регіональними чи місцевими органами влади, якщо вони не виступають в якості державних органів. Крім того, з прийняттям першої Директиви про платіжні послуги у 2007 році було введено нову організацію – «платіжні установи». Вони можуть надавати лише платіжні послуги; їм заборонено приймати депозити або випускати електронні гроші. Відповідно до другої Директиви про платіжні послуги були введені нові категорії провайдерів платіжних послуг: провайдери послуг з ініціювання платежів та провайдери послуг з надання доступу до інформації по рахункам користувачів. Вони можуть надавати виключно послуги ініціювання платежів та інформацію про рахунки.

Впровадження платіжних установ посилило конкуренцію на ринку платежів з 2009 року.

Більшість провайдерів платіжних послуг все ще складається з кредитних установ.

Що стосується менших гравців, то в усьому ЄС (станом на 2012 рік) було:

- 568 уповноважених платіжних установ;
- 2 203 малих платіжних установ (платіжних установ, яким дозволено надавати лише платіжні послуги в країні, де вони отримали ліцензію); та
- 71 установа електронних грошей.

Розподіл платіжних установ (уповноважених платіжних установ та малих платіжних установ) є висококонцентрованим, у кожному випадку декілька країн складають переважну більшість таких установ у ЄЕП. На Сполучене Королівство припадає 39,4 % усіх уповноважених платіжних установ ЄЕП, а на Сполучене Королівство разом із Іспанією (8,1 %), Італією (7,9 %), Німеччиною (6,5 %), Нідерландами (4,9 %) та Швецією (4,3 %) припадає 71 % усіх уповноважених платіжних установ в ЄЕП. Що стосується малих платіжних установ, то 44,8 % зареєстровано у Польщі, а 43,6 % – у Сполученому Королівстві. На Сполучене Королівство також припадало 42,2 % усіх установ електронних грошей в ЄЕП.

Більш загальні дані про кількість фінансових установ, що надають платіжні послуги в ЄС, можна знайти у звіті про статистику платежів ЄЦБ за 2017 рік: http://sdw.ecb.europa.eu/servlet/desis?node=1000001384.

Опис сценарію ризиків

Злочинці використовують банківську та фінансову систему для спрямування своїх коштів через банківські рахунки, банківські кредитні та дебетові перекази, мобільні платежі (між фізичними особами) та платіжні послуги у мережі Інтернет.

Загроза

Фінансування тероризму

Оцінка загрози фінансування тероризму, пов'язаної з платіжними послугами, вказує на те, що терористичні операції на основі рахунків використовуються для зберігання та переказу коштів та оплати послуг чи продуктів, необхідних для здійснення операцій, зокрема у разі обробки і через мережу Інтернет. Згідно з дослідженнями щодо фінансування терористичних осередків європейських джихадистів, формальна банківська система є одним із шести методів, які найбільш часто використовуються терористичними групами. Більшість терористичних осередків, розташованих в Європі, отримували певний дохід з легальних джерел – зазвичай через офіційну банківську систему – і використовують банківські рахунки та кредитні картки як для своєї повсякденної економічної діяльності, так і для витрат, пов'язаних з атаками. З огляду на елементи, що базуються на рахунках, намір терористичних груп покладатися на цей сценарій ризику є більш обмеженим. Однак їх здатність використовувати його є досить високою. Платіжні послуги дозволяють здійснювати транскордонні операції, які можуть покладатися на різні механізми ідентифікації (залежно від національного законодавства), що може призвести до використання терористами фальшивої особистості. Це означає, що правоохоронні органи не можуть відстежувати джерела або бенефіціара операції. Використання платіжних послуг вимагає конкретних навичок, але, на думку правоохоронних органів, ці навички є широко розповсюдженими в терористичних групах і не становлять перешкод (платежі через мобільний телефон/Інтернет є досить простими). Але відповідна сума залишається досить обмеженою.

Висновки: терористичні групи використовують платіжні послуги для фінансування терористичної діяльності. Вони покладаються на ІТ-навички для обходу вимог щодо ідентифікації та не потребують конкретних знань для доступу до цього каналу, що є досить привабливим та безпечним. Тим не менш, відповідні суми залишаються досить обмеженими. У цьому контексті, рівень загрози фінансування тероризму, пов'язаної з платіжними послугами, вважається значним (рівень 3).

Відмивання коштів

Оцінка загрози відмивання коштів, пов'язаної з платіжними послугами, вважається подібною до оцінки загрози, пов'язаної з депозитами на рахунках. Цей сценарій ризиків стосується як розміщення, так і зняття коштів (тобто депозитів на рахунку та використання цього рахунка). Він часто використовується злочинцями, а також родичами/близькими особами, що розширює сферу аналізу наміру та здатності.[41] Кошти, що використовуються у платіжних послугах, мають незаконне походження. Для цього потрібно певне планування та знання того, як працюють банківські системи.

[41] Що стосується наміру та здатності, див. виноску 34.

За даними правоохоронних органів, провайдери платіжних послуг можуть використовуватися грошовими мулами або підпорядковуватися кримінальному контролю:

> Наприклад, провайдери платіжних послуг були досліджені декількома державами-членами ЄС. Провайдер платіжних послуг, зареєстрований в одній державі-члені ЄС, зареєструвався як емітент електронних грошей в іншій юрисдикції і отримав таким чином ліцензію на використання паспорта. До провайдера платіжних послуг звернулася кримінальна структура, яка вимагала здійснювати торгівлю у мережі Інтернет. Провайдер платіжних послуг надав клієнту касові термінали. Термінали були вивезені з Європи та використані в операціях обміну песо на чорному ринку. Інформація, зібрана у ході розслідувань, продемонструвала, що провайдер платіжних послуг не здійснював жодного моніторингу клієнта, що могло призвести до ідентифікації ризику, оскільки заявлений малий інтернет-бізнес призвів до накопичення кількох мільйонів євро за обмежений період часу. Касові термінали також не контролювалися, оскільки вони фізично не були присутніми в ЄС на момент розміщення замовлення. До цього ж провайдера платіжних послуг також звернулася інша кримінальна структура в іншій державі-члені ЄС. Злочинна структура контролювала підставні туристичні підприємства, які використовувались для здійснення готівкових внесків за рахунок доходів від продажу кокаїну. Такі підприємства стали клієнтами провайдера платіжних послуг і попросили випустити їм банківські картки (оскільки провайдер платіжних послуг є емітентом карток Visa та Mastercard). Картки були вивезені з Європи, а готівка знята в Колумбії.

Висновки: організовані злочинні групи використовують цей метод досить часто, оскільки він є легкодоступним, незважаючи на необхідність певних знань та планування для приховування походження коштів. Однак, коли злочинні структури поглинають провайдерів платіжних послуг, ризик відмивання коштів може бути вищим. У цьому контексті, рівень загрози відмивання грошей, пов'язаної з платіжними послугами, вважається значним (рівень 3).

Вразливість

Фінансування тероризму

Оцінка вразливості до фінансування тероризму, пов'язаної з платіжними послугами, має деякі спільні риси з оцінкою вразливості до фінансування тероризму, пов'язаної з роздрібними платіжними послугами.

a) схильність до ризику

Схильність до ризику є по суті високою з огляду на характеристики платіжних послуг, оскільки вони передбачають дуже значні обсяги продуктів та послуг. Хоча платежі, як правило, не є анонімними (оскільки вони пов'язані з ідентифікованим рахунком), вони можуть взаємодіяти з дуже значною кількістю клієнтів або країн з вищим ризиком, включаючи транскордонне переміщення коштів. Вони також взаємодіють з новими способами оплати (мобільний телефон/Інтернет), що може підвищити рівень схильності до ризику, оскільки вони передбачають непрямі ділові відносини.

b) обізнаність про ризики

Обізнаність про ризики є загалом належною, оскільки сектор видав настанови щодо виявлення відповідних тривожних сигналів стосовно фінансування тероризму. Це підтверджується належним рівнем звітування, оскільки сектор має необхідні інструменти для виявлення таких ризиків. Однак належна перевірка клієнтів та показники ризику не завжди є достатніми для виявлення зв'язку з терористичною діяльністю з огляду на законне походження коштів. Підрозділи фінансової розвідки та правоохоронні органи також добре обізнані про вразливості сектора та активно займаються їх усуненням.

c) законодавча база і перевірки

Платіжні послуги включені до законодавчої бази щодо ПВК/ФТ на рівні ЄС. Ця база існує вже багато років, і перевірки вважаються в цілому ефективними. Що стосується законодавчої бази, вона охоплює кредитні та платіжні установи однаковою мірою. Подібно до депозитів на рахунках, здійснювані перевірки, як правило, вважаються ефективними, однак перевірка санкцій не замінює ефективних перевірок протидії фінансуванню тероризму. Фінансові санкції спрямовані на фізичних осіб або групи, які, як відомо, вже становлять загрозу, тоді як ризик фінансування тероризму часто походить від фізичних осіб, які не підпадають під санкційний режим. Ось чому перевірки щодо ПВК/ФТ на основі ризиків та, зокрема, моніторинг операцій, є ключовими для ефективної боротьби з фінансуванням тероризму.

Банки та платіжні установи зазвичай не мають доступу до відповідної інформації, яка часто зберігається правоохоронними органами, що допомогла би їм виявити ризики, пов'язані з фінансуванням тероризму, до того, як вони будуть реалізовані. Аналогічно, зусиллям правоохоронних органів щодо стримування терористичної діяльності і мереж може перешкоджати їх нездатність отримати інформацію про фінансові потоки, яку можуть надати лише компанії. Наразі існують ініціативи на національному та наднаціональному рівнях для перевірки того, як правоохоронні органи можуть надавати компаніям більш конкретну та змістовну інформацію щодо осіб, які становлять інтерес, дозволяючи компаніям зосередити моніторинг операцій на таких особах.

Висновки: схильність до ризику може вважатися досить високою (значний рівень операцій). Сектор демонструє належний рівень обізнаності про вразливість до ризиків і може встановити відповідні тривожні сигнали. Законодавча база і перевірки є основою належного звітування. Однак залишковий ризик є високим з огляду на залежність від поточних перевірок заходів протидії фінансуванню тероризму на основі перевірки санкцій. У цьому контексті, рівень вразливості до фінансування тероризму, пов'язаної з платіжними послугами, вважається значним (рівень 3).

Відмивання коштів

Оцінка вразливості до відмивання коштів, пов'язаної з платіжними послугами, має деякі спільні риси з оцінкою вразливості до відмивання коштів, пов'язаної з роздрібними платіжними послугами.

a) схильність до ризику

Схильність до ризику є по суті високою з огляду на характеристики платіжних послуг, які часто передбачають дуже значні обсяги коштів. Хоча платежі, як правило, не є анонімними (оскільки вони пов'язані з ідентифікованим рахунком), вони можуть взаємодіяти з дуже значною кількістю клієнтів або країн з вищим ризиком, включаючи транскордонне переміщення коштів. Вони також взаємодіють з новими способами оплати (мобільний телефон/Інтернет), що може підвищити рівень схильності до ризику, оскільки вони передбачають непрямі ділові відносини.

b) обізнаність про ризики

Компетентні органи констатували розбіжності між банківськими та платіжними установами, при чому останні є менш обізнаними про ризики відмивання коштів. На думку більшості компетентних органів загальний рівень ризику платіжних установ є значним або дуже значним; зокрема, так вважають органи влади, які здійснюють нагляд за найбільшою кількістю платіжних установ. Потенційне зловживання новими технологіями, такими як мобільні платежі для полегшення рівноправних грошових переказів, розглядається компетентними органами як новий ризик (див. розділ про віртуальні валюти). Наразі моніторинг є недостатнім, як при відкритті платіжного рахунка (вхідна точка), так і під час обробки операцій.

c) законодавча база і перевірки

Платіжні послуги включені до законодавчої бази щодо ПВК/ФТ на рівні ЄС. Що стосується законодавчої бази, вона охоплює однаковою мірою банківські та платіжні установи. Залежність від операцій на основі рахунків означає, що законодавча база зазвичай застосовується до банківського сектора та до сектора платіжних установ. Ця база існує вже багато років, і перевірки вважаються в цілому ефективними. Платіжні установи покладаються на банківський контроль для пом'якшення свого ризику відмивання коштів, але деякі системи оповіщення у банках є недостатньо надійними для виявлення підозрілих готівкових операцій, які згодом передаються платіжними установами.

Висновки: Схильність сектора ризику та його обізнаність про ризики є досить схожими до схильності до ризику та обізнаності про ризики у секторі депозитів на рахунках. Що стосується законодавчої бази, вона охоплює однаковою мірою банківські та платіжні установи. Однак здійснювані перевірки є менш ефективними при роботі з платіжними установами. У цьому контексті, рівень вразливості до відмивання коштів, пов'язаної з платіжними послугами, вважається значним (рівень 3).

Пом'якшувальні заходи:

Для Комісії:

- уточнення та створення загальної бази для електронної ідентифікації та належної перевірки клієнтів;
- виявлення ризиків, пов'язаних з Fin-Tech, та встановлення стандартів для їх пом'якшення;
- здійснення картографічного дослідження та аналіз банківських практик на території ЄС, а також оцінка будь-яких наступних кроків;
- сприяння співпраці між правоохоронними органами та фінансовими установами для підвищення ефективності систем оповіщення про фінансування тероризму на наднаціональному рівні.

Для держав-членів/компетентних органів:

- Держави-члени повинні гарантувати, що органи нагляду проводитимуть низку тематичних перевірок на місцях, орієнтованих на оцінку ризиків платіжних установ, та забезпечать ефективність їх систем оповіщення.
- Крім того, компетентні органи повинні забезпечити подальшу обізнаність про ризики та показники ризиків, пов’язаних з фінансуванням тероризму.
- Держави-члени повинні усунути граничні значення для випадкових операцій, застосовуючи належну перевірку клієнтів до всіх операцій, щоб платіжні установи могли ефективно контролювати та виявляти підозрілі операції.

12. Віртуальні валюти та інші віртуальні активи

Продукт
Віртуальні валюти та інші віртуальні активи

Сектор
Віртуальні валюти та інші віртуальні активи – Провайдери послуг

Загальний опис сектора та відповідного продукту/діяльності

Визначення

П'ята директива про боротьбу з відмиванням грошей (AMLD5) вперше ввела у законодавство ЄС визначення віртуальної валюти, яке вона описує як «цифрове представлення вартості, яка не випускається ані центральним банком, ані державним органом влади, необов'язково закріплюється за паперовою валютою, але приймається фізичними чи юридичними особами як платіжний засіб і може передаватися, зберігатися або продаватися в електронній формі».[42] П'ята директива про боротьбу з відмиванням грошей визначає зобов'язаних суб'єктів для цілей ПВК/ФТ провайдерами, які надають послуги обміну між віртуальними валютами та паперовими валютами та провайдерами гаманців віртуальної валюти. У жовтні 2018 року FATF внесено зміни до своїх стандартів та розширено Рекомендацію 15 (нові технології) до «віртуальних активів» та «провайдерів послуг у сфері віртуальних активів». Поправка до Рекомендації 15 вимагає від країн та юрисдикцій регулювання провайдерів послуг у сфері віртуальних активів для цілей ПВК/ФТ, їх ліцензування або реєстрування та включення до ефективних систем моніторингу та забезпечення відповідності заходам, передбаченим Рекомендаціями FATF.

Крім того, віртуальні активи наразі визначаються у глосарії FATF як «цифрове відображення вартості, що може бути продана або інакше передана цифровим методом з метою здійснення оплати або інвестування. Віртуальні активи не включають в себе цифрове відображення фіатних валют, цінних паперів та інших фінансових активів, які вже охоплені в інших Рекомендаціях FATF».

Нове визначення FATF є ширшим, ніж визначення «віртуальної валюти» у П'ятій директиві про боротьбу з відмиванням грошей.

Більше того, в результаті змін, юрисдикціям рекомендується мати у межах зобов'язань щодо ПВК/ФТ будь-яку фізичну чи юридичну особу (не охоплену в інших положеннях Рекомендацій FATF), яка, як бізнес, здійснює один або декілька наступних заходів або операцій для або від імені іншої фізичної чи юридичної особи:

- обмін між віртуальними активами та фіатними валютами;
- обмін між однією або кількома іншими формами віртуальних активів;
- передача віртуальних активів;
- збереження або адміністрування віртуальних активів чи інструментів, що дозволяють контролювати віртуальні активи; та
- участь у наданні фінансових послуг, що стосуються пропозиції емітента та/або продажу віртуального активу.

[42] У Преамбулі (10) П'ятої директиви про боротьбу з відмиванням грошей пояснюється, що віртуальні валюти не слід плутати з (між іншим): електронними грошима у контексті EMD2, а також коштами у контексті PSD2: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L0843&from=EN.

Зацікавлені сторони

На ринку віртуальних валют/віртуальних активів залучені різні зацікавлені сторони, основними з яких є:

- **провайдери гаманців:** користувачі криптовалют можуть володіти рахунками віртуальних валют/віртуальних активів на своїх власних пристроях або доручити провайдеру гаманців утримувати та адмініструвати їх (в електронному гаманці) та забезпечувати огляд операцій користувача (через веб-сервіс або телефонний сервіс). Існує три типи провайдерів гаманців:

  - провайдери апаратних гаманців, які надають користувачам конкретні апаратні рішення для приватного зберігання їх криптографічних ключів;
  - провайдери програмних гаманців, які надають користувачам програмні додатки, що дозволяють їм отримувати доступ до мережі, надсилати та отримувати криптовалюти та зберігати свої криптографічні ключі на місцевому рівні; та
  - провайдери зберігальних гаманців, які приймають на зберігання в режимі онлайн криптографічні ключі користувача (включаючи гаманці з багатьма підписами).

  На відміну від провайдерів програмних гаманців (які надають додатки або програми, що працюють на апаратних засобах користувачів – комп'ютер, смартфон, планшет тощо, та мають доступ до публічної інформації з розповсюджуваної бухгалтерської книги та доступ до мережі), провайдери зберігальних гаманців приймають на зберігання публічний та приватний ключ користувача. Це є аналогічним традиційному банку, який надає особистий рахунок.

  Гаманці можуть зберігатися в режимі онлайн («гаряче зберігання») або в режимі офлайн («холодне зберігання»), при цьому останні забезпечують більший захист.

  Лише провайдери зберігальних гаманців («організації, які надають послуги щодо захисту приватних криптографічних ключів від імені своїх клієнтів, а також послуги володіння, зберігання та передачі віртуальних валют») є зобов'язаними суб'єктами згідно з П'ятою директивою про боротьбу з відмиванням грошей.

  Провайдери апаратних та програмних гаманців не захищають ключі від імені своїх клієнтів, але надають їм інструменти для захисту своїх криптовалют; це створює можливості для можливих заходів, пов'язаних з ВК/ФТ;

- **платформи обміну** (особа чи організація, що здійснюють обмін віртуальних валют/віртуальних активів на фіатну валюту, фіатної валюти на віртуальні валюти/віртуальні активи, кошти або інші типи віртуальних валют/віртуальних активів): ці платформи (*обмінники* у світі віртуальних валют/віртуальних активів) можуть приймати широкий спектр платежів, включаючи готівку, кредитні перекази, кредитні картки та інші віртуальні валюти/віртуальні активи. Вони включають касові апарати.

  Подібно до традиційних валютних бірж, крупні біржі віртуальних валют забезпечують загальну картину змін у ціні обміну віртуальної валюти та її волатильності. Деякі платформи пропонують такі послуги, як послуги конвертації для торговців, які приймають платежі у формі віртуальних валют, але бояться амортизації та хочуть негайно конвертувати їх у (національну) фіатну валюту. Пята директива про боротьбу з відмиванням грошей охоплює лише обмін віртуальних валют на фіатну валюту, а не на інші віртуальні валюти/віртуальні активи;

- **користувач** (фізична чи юридична особа, яка отримує суму віртуальних валют та використовує її для придбання реальних або віртуальних товарів чи послуг, або для пересилання грошових переказів іншій особі (для особистого користування) або яка володіє віртуальною валютою для інших цілей, наприклад інвестиції): зазвичай користувачі отримують віртуальну валюту одним з наступних способів:
    - в результаті обміну (або, для більшості централізованих віртуальних валют, безпосередньо від суб'єкта, що управляє схемою) з використанням фіатних валют або іншої віртуальної валюти;
    - шляхом вжиття конкретних заходів, таких як реагування на просування, здійснення онлайн-опитування та «майнінгу» (використання спеціального програмного забезпечення для використання складних алгоритмів для перевірки операцій у системі віртуальних валют); та/або
    - від організації, яка управляє схемами, емітента або інших користувачів, які діють для інших цілей, ніж їх торгівельна, комерційна або професійна діяльність;
- **майнери:** у децентралізованих схемах віртуальних валют майнери використовують складні алгоритми для отримання невеликих сум віртуальних валют. Майнери, як правило, працюють анонімно, з будь-якої точки світу і підтверджують операції з віртуальними валютами. Коли група майнерів контролює більше половини загальної обчислювальної потужності, що використовується для створення блоків віртуальних валют, вона може перешкоджати операціям, наприклад. шляхом відхилення операцій, підтверджених іншими майнерами. Майнери групуються у пули (Antpool, F2Pool, BitFury, BTCC Pool, BW.COM тощо). Більшість з них наразі знаходиться в Китаї; та
- **особи, які здійснюють первинну пропозицію монет:** Нещодавно прийняте FATF визначення провайдера послуг у сфері віртуальних активів охоплює «участь у фінансових послугах та їх наданні, пов'язаних з пропозицією емітента та/або продажем віртуального активу». Особи, які пропонують монети – це фізичні особи чи організації, які пропонують монети користувачам криптовалют під час первинного випуску монет або за рахунок оплати (наприклад, шляхом «краудсейлу»), або безкоштовно (наприклад, як частина конкретної програми реєстрації, наприклад, Stellar), як правило, для фінансування подальшого розвитку монет або підвищення їх початкової популярності. Особою, яка пропонує монети, може бути та сама особа, що і винахідник монет, або інша фізична особа чи організація.

П'ята директива про боротьбу з відмиванням грошей розширила зобов'язання щодо боротьби з відмиванням грошей до «провайдерів, які здійснюють обмін послуг між віртуальними валютами та фіатними валютами» (платформи обміну), та провайдерів зберігальних гаманців, але не охоплює всі заходи, пов'язані з віртуальними активами, про які йдеться у новому визначенні FATF провайдерів послуг у сфері віртуальних активів, зокрема, обміни віртуальних активів на віртуальні активи та первинні пропозиції монет (див. Розділ **«Чинне законодавство та перевірки»** нижче).

Ринок віртуальних валют/віртуальних активів в ЄС

Складно зібрати офіційні дані про ринок віртуальних валют. Наведені нижче оцінки базуються на інформації з різних веб-сайтів, які відстежують обсяги обміну та ціни або проводять дослідження. Оцінки учасників ринку, як правило, є нижчими, ніж статистичні дані, знайдені у мережі Інтернет. Отже, наступні статистичні дані повинні відображати високі, але збалансовані оцінки:

Загальна кількість гаманців віртуальних валют у світі	13 млн (Q4 2015)[43] – 7,4 млн у Q4 2014
Кількість гаманців віртуальних валют в ЄС	Приблизно 3 млн
Кількість користувачів віртуальних валют у світі[44]	1-4 млн
Кількість користувачів віртуальних валют в ЄС	Приблизно 500 000
Кількість майнерів віртуальних валют у світі	100 000[45]
Кількість майнерів віртуальних валют в ЄС	10 000 (за оцінками)
Кількість провайдерів програмних гаманців віртуальних валют у світі	> 500 (за оцінками)
Кількість зберігачів віртуальних валют у світі	> 100 (за оцінками)
Кількість зберігачів віртуальних валют в ЄС	> 20 (за оцінками)
Кількість платформ обміну у світі	> 100
Кількість платформ обміну в ЄС	> 28
Кількість касових апаратів у світі[46]	571
Кількість касових апаратів в ЄС	> 100
Кількість щоденних операцій з віртуальними валютами	> 125 000 (тільки біткойн – для 2015)
Кількість продавців, які приймають біткойни	110 000 (Q4 2015) – 80 000 у Q4 2014
Ринкова капіталізація віртуальних валют	7 млрд євро

Опис сценарію ризиків

Відмивання коштів: Віртуальні активи створюють ризик ВК/ФТ з огляду на легкість передачі віртуальних активів у різні країни, а також відсутність узгодженого контролю та заходів запобігання на глобальному рівні. Злочинці використовують системи віртуальних валют/віртуальних активів для переказу коштів або придбання товарів анонімно (фінансування у формі готівки або фінансування третіми особами шляхом віртуальних обмінів).

Фінансування тероризму: Віртуальні валюти/віртуальні активи, як правило, передбачають непрямі відносини з клієнтами та можуть допускати анонімне фінансування чи покупки (фінансування у формі готівки або фінансування третіми особами шляхом віртуальних обмінів, в яких джерело фінансування не визначено належним чином). Вони також можуть допускати анонімні перекази, якщо відправник та одержувач не були ідентифіковані належним чином.

Загроза

Діяльність, пов'язана з віртуальними валютами/віртуальними активами, представляє зростаючу загрозу відмивання коштів/фінансування тероризму. Підрозділи фінансової розвідки у

[43] ;http://www.coindesk.com/state-of-bitcoin-blockchain-2016/ див. слайд 8.
[44] Принаймні, одна операція на місяць.
[45] http://bravenewcoin.com/news/the-decline-in-bitcoins-full-nodes/
[46] http://coinatmradar.com/ (консультації 4 лютого 2016 року).

глобальній мережі FATF спостерігають зростання кількості звітів про підозрілі операції, пов'язані з віртуальними валютами/віртуальними активами; і таке зростання може пришвидшитися для підрозділів фінансової розвідки ЄС після закінчення терміну транспозиції Директиви про боротьбу з відмиванням грошей.[47]

Європол розглядає біткойни як віртуальні валюти/віртуальні активи, які вибирають більшість злочинців, проте очікує більш виражений перехід до використання віртуальних активів із збільшеною анонімністю, які забезпечують більшу конфіденційність, швидший час операцій, нижчі комісійні операцій та меншу волатильність цін.

Використання інших монет із більшою конфіденційністю повільно усуне потребу у спеціальних послугах змішування. Дві найбільші послуги змішування вже припинили своє функціонування (у 2017 році). Обмінники наразі можуть пропонувати операції обміну віртуальних валют/віртуальних активів на віртуальні валюти/віртуальні активи, які приховують сліди операції, і використовуються децентралізовані змішувачі.

Певна низка проблем виникає з послуг віртуальних валют/віртуальних активів, які надаються злочинцями або невідповідними організаціями:

- оператори використовують злочинні гроші, щоб створити компанію віртуальних валют/віртуальних активів, яка вносить злочинні гроші або незаконно отримані віртуальні валюти/віртуальні активи у касовий апарат;
- фізичні особи купують/продають великі обсяги віртуальних валют/віртуальних активів за будь-який актив «поза біржею» (без посередництва), не реєструючись як провадйери послуг віртуальних валют/віртуальних активів та не рекламуючи свої послуги; та
- провайдери платіжних послуг, що пропонують криптовалюти, спочатку одержали пропозицію лише для біткойну, проте мав місце перехід до підтримки декількох віртуальних валют/віртуальних активів. Вони часто реєструються в юрисдикціях із «сприятливими» регуляторними положеннями.

Правоохоронні органи також стикаються з особливими труднощами у збиранні інформації, якщо обмін віртуальних валют/віртуальних активів відбувається в іншій країні, ніж та, в якій знаходиться платник/одержувач платежу (який сам може знаходитися у будь-якій країні світу).

Багато країн занепокоєні зловживанням первинними пропозиціями монет та, в більш широкому плані, недостатньою обізнаністю емітентів токенів щодо своїх зобов'язань стосовно ПВК/ФТ, особливо в юрисдикціях, які не вимагають від підприємств підтримувати фізичну присутність для цілей реєстрації та ліцензування.

Фінансування тероризму

За результатами оцінки, терористичні групи можуть бути зацікавлені у використанні віртуальних валют/віртуальних активів для фінансування терористичної діяльності. Одержано повідомлення про обмежену, але зростаючу кількість випадків, пов'язаних з віртуальними валютами.[48] Егмонтська група підрозділів фінансової розвідки виявила терористичні групи, які використовують віртуальні валюти, і відомо, що групи надавали інструкції в мережі Інтернет (в тому числі через Twitter) щодо використання віртуальних валют/віртуальних активів.

[47] Підрозділ фінансової розвідки у Люксембургу зафіксував на 70 % збільшення кількості звітів про підозрілі операції, подані стосовно використання віртуальних активів у період між 2017 та 2018 роками.

[48] Деякі випадки пожертвування шляхом «краудфандингу», що вимагається для біткойнів, посилаючись на «підтримку вдовам, мученикам, мусульманським групам», намагаючись уникнути чіткого зв'язку з фінансуванням тероризму та поради консультуючи щодо використання касових автоматів для біткойнів.

Висновки: Правоохоронні органи володіють інформацією, відповідно до якої терористичні групи можуть використовувати віртуальні валюти для фінансування терористичної діяльності. Отже, рівень загрози фінансування тероризму, пов'язаної з віртуальними валютами, вважається значним (рівень 3).

Відмивання коштів

Оцінка загрози відмивання коштів, пов'язаної з віртуальними валютами/віртуальними активами, вказує на те, що організовані злочинні організації можуть використовувати їх для одержання доступу до «чистих грошових коштів» (оплата та виплата). Не тільки кіберзлочинці використовують віртуальні валюти/віртуальні активи – інші організовані злочинні групи, такі як торговці наркотиками, використовують їх для переміщення та відмивання доходів від злочинної діяльності. Віртуальні валюти/віртуальні активи дозволяють таким групам отримувати доступ до готівки анонімно та приховувати сліди операцій. Злочинці можуть набувати приватні ключі для електронних гаманців або знімати готівку з касових автоматів.

Висновки: Зростаюча кількість розслідувань стосується використання віртуальних валют та віртуальних активів злочинними організаціями (не лише кіберзлочинцями). Отже, рівень загрози відмивання коштів, пов'язаної з віртуальними валютами, вважається значним (рівень 3).

Вразливість

Фінансування тероризму

Оцінюючи вразливість до фінансування тероризму, пов'язану з провайдерами віртуальних валют/віртуальних активів, ми повинні мати на увазі, що, хоча ЄС розпочав регулювати віртуальні активи/віртуальні валюти, ризики їх зловживання для фінансування тероризму тільки почали з'являтися.

a) схильність до ризику

У разі анонімного використання, віртуальні валюти дозволяють швидко здійснювати операції без розголошення особи «власника». Вони надаються через мережу Інтернет, а транскордонний елемент є найбільш очевидним фактором ризику, оскільки він передбачає взаємодію із зонами високого ризику або клієнтами високого ризику, які не можуть бути ідентифіковані. Це може змінитися, якщо будуть запроваджені нові стандарти FATF, оскільки вони зобов'язуватимуть провайдерів послуг у сфері віртуальних активів реєструватися у місці їх заснування чи реєстрації (юридичні особи) або в юрисдикції, в якій знаходиться місце їх діяльності (фізичні особи). Тим не менш, використання віртуальних валют/віртуальних активів поширюється швидкими темпами, і очікується, що кількість операцій значно збільшиться найближчим часом.

b) обізнаність про ризики

Цей компонент вразливості до фінансування тероризму важко оцінити комплексно – тоді як «провайдери, що надають послуги обміну між віртуальними валютами та фіатними валютами» і провайдери зберігальних гаманців наразі є зобов'язаними суб'єктами на рівні ЄС, це (ще) не стосується всіх провайдерів віртуальних валют/віртуальних активів. Більше того, компетентні органи та підрозділи фінансової розвідки помітили у своїх зв'язках із сектором, що рівень обізнаності про ризики фінансування тероризму залишається досить низьким, хоча сектор вимагає прийняття відповідної законодавчої бази щодо ПВК/ФТ.

Віртуальні активи є одним з найважливіших ризиків, що виникає майже у всіх секторах, з огляду на:

- відсутність знань та розуміння, що заважає компаніям та компетентним органам здійснювати належну оцінку впливу;

- прогалини або неясності у застосуванні існуючих нормативних положень;
- потенційну схильність фінансових та кредитних установ до підвищених ризиків відмивання коштів та фінансування тероризму, пов'язаних з віртуальними валютами/віртуальними активами, коли вони виступають посередниками або платформами обміну між віртуальними валютами/віртуальними активами та фіатними валютами (за відсутності належної оцінки ризиків); та
- в інвестиційному секторі – обробку операцій у мережі Інтернет з обмеженими перевірками ідентифікації та верифікації клієнтів.

Сектор ще недостатньо організований, і важко знайти належні інструменти для надання йому відповідної інформації для підвищення рівня обізнаності.

c) законодавча база і перевірки

П'ята директива про боротьбу з відмиванням грошей представила перше визначення ЄС щодо віртуальних валют та розширила зобов'язання щодо протидії відмиванню коштів до «провайдерів послуг з обміну між віртуальними валютами та фіатними валютами» та провайдерів зберігальних гаманців. На додаток до звичайної належної перевірки клієнтів, держави-члени повинні забезпечити реєстрацію цих нових зобов'язаних суб'єктів. Вони також повинні вимагати від компетентних органів забезпечення того, щоб в цих суб'єктах управлінські функції виконувались лише належними особами або були їхніми бенефіціарними власниками.

Останні зміни у стандартах FATF щодо віртуальних активів означають, що визначення віртуальних валют у П'ятій директиві про боротьбу з відмиванням грошей може бути занадто вузьким, оскільки воно не охоплює інші види віртуальних активів.

Крім того, можуть мати місце прогалини, які мають бути заповнені стосовно різних видів діяльності провайдерів послуг у сфері віртуальних активів, які не охоплені законодавчою базою ЄС:

- провайдери зберігальних гаманців, які не захищають ключі від імені своїх клієнтів, а лише надають їм інструменти для захисту своїх криптовалют, наприклад, провайдери апаратних гаманців та провайдери програмних гаманців;
- обміни віртуальних валют або віртуальних активів на інші віртуальні валюти або віртуальні активи; та
- «участь у наданні фінансових послуг, пов'язаних з пропозицією емітента та/або продажем віртуального активу», зокрема, у випадках, коли особа, яка пропонує розміщення монет, є тією самою особою, що і винахідник монет, або іншою особою чи організацією.

Висновки: Найбільш вагомим фактором вразливості для провайдерів віртуальних валют та віртуальних активів є те, що вони можуть не повною мірою регулюватися в ЄС. Після впровадження, П'ята директива про боротьбу з відмиванням грошей значно покращить ситуацію, зробивши провайдерів гаманців та провайдерів послуг обміну між віртуальними валютами та фіатними валютами зобов'язаними суб'єктами, гарантуючи, що вони будуть зареєстровані і що лише відповідні та належні особи виконуватимуть функції управління або є бенефіціарними власниками. Ця законодавча база має бути впроваджена, і необхідно розглянути можливість її розширення до інших провайдерів послуг у сфері віртуальних активів, таких як особи, які здійснюють первинну пропозицію монет, та провайдери послуг обміну між віртуальними валютами. Схильність до ризику є дуже високою з огляду на характеристики віртуальних валют (у мережі Інтернет, транскордонні та анонімні). Нарешті, сектор наразі недостатньо організований, щоб отримати настанови або відповідну інформацію щодо вимог в області ПВК/ФТ. Отже, рівень вразливості до фінансування тероризму, пов'язаної з віртуальними валютами, вважається значним/дуже значним (рівень 3/4).

Відмивання коштів

Оцінка вразливості до відмивання коштів, пов'язаної з провайдерами віртуальних валют, починається з тих самих умов, що і оцінка вразливості, пов'язаної з фінансуванням тероризму. Ці умови частково регламентовані в ЄС, і дуже мало доказів зловживання віртуальними валютами для відмивання коштів. Однак це не перешкоджає здійсненню оцінки потенційних вразливостей. Хоча розслідування майже не призводять до притягнення до кримінальної відповідальності, ризик існує і його можна проаналізувати.

a) схильність до ризику

Як зазначалося вище, у разі анонімного використання, віртуальні валюти дозволяють швидко здійснювати операції без розголошення особи «власника». Вони здійснюються через мережу Інтернет, і транскордонний елемент є найбільш очевидним фактором ризику, оскільки він передбачає взаємодію із зонами високого ризику або клієнтами високого ризику (чорний інтернет), які не можуть бути ідентифіковані. На етапі конвертації, використання готівки також стає новим елементом вразливості. Нові правила П'ятої директиви про боротьбу з відмиванням грошей вирішать цю проблему, розширивши законодавчу базу в області ПВК/ФТ до «провайдерів, що надають послуги з обміну між віртуальними валютами та фіатними валютами». Однак канали доставки залишаються децентралізованими, що збільшує схильність до ризику (зокрема, касові апарати дозволяють знімати або конвертувати віртуальні валюти).

b) обізнаність про ризики

Це нова технологія, і рівень обізнаності про ризики у секторі намагається не відставати. Цей сектор дедалі більше потребує законодавчої бази, в якій віртуальні валюти підпорядковуватимуться вимогам щодо ПВК/ФТ. Підрозділи фінансової розвідки не можуть виявляти та аналізувати ризики лише на основі блокчейну. Вони не можуть встановити, які суми зберігаються в електронних гаманцях та визначити походження/одержувача коштів.

c) законодавча база і перевірки

П'ята директива про боротьбу з відмиванням грошей додасть платформи обміну віртуальними валютами та провайдерів зберігальних гаманців до переліку зобов'язаних суб'єктів та зробить їх предметом належної перевірки клієнтів та обов'язкової реєстрації. Як і у разі фінансування тероризму, можуть знадобитися поліпшення для забезпечення того, що всі провайдери віртуальних валют/віртуальних активів відповідатимуть вимогам щодо ПВК/ФТ.

На початку 2019 року, у світлі останніх змін у рекомендаціях FATF щодо віртуальних активів,

Європейський орган з цінних паперів та ринків та Європейська служба банківського нагляду опублікували звіти про відповідність чинної законодавчої бази ЄС в частині первинних пропозицій монет та криптоактивів. Вони закликають переглянути сферу застосування Директиви про боротьбу з відмиванням грошей з огляду на нові визначення віртуальних активів та провайдерів послуг у сфері віртуальних активів (FATF 2018). Нові міжнародні стандарти вимагають додаткового регулювання надання таких інших послуг у сфері віртуальних активів і адаптування поточного визначення віртуальних валют для охоплення ширших реалій, що охоплюються терміном «віртуальні активи». Анонімність деяких операцій у сфері віртуальних валют також залишається головним фактором ризику, який можна усунути.

Висновки: П'ята директива про боротьбу з відмиванням грошей повинна значною мірою посилити моніторинг ризиків, пов'язаних з провайдерами послуг у сфері віртуальних активів, але вона ще не впроваджена. Законодавча база також може бути розширена до провайдерів послуг у сфері віртуальних активів, які ще не охоплені (наприклад, особи, які здійснюють первинну пропозицію монет, та провайдери послуг з обміну між віртуальними валютами), та узгоджена з новими стандартами FATF. Схильність до ризику має і надалі вважатися дуже високою з огляду на характеристики віртуальних валют (у мережі Інтернет, транскордонні та анонімні). Тому рівень вразливості до фінансування тероризму, пов'язаної з віртуальними валютами, вважається значним/дуже значним (рівень 3/4).

Пом'якшувальні заходи:

- Комісія повинна оцінити відповідні способи доопрацювати своєї законодавчої бази, щоб забезпечити, що віртуальні валюти/віртуальні активи та всі провайдери послуг у сфері віртуальних валют/віртуальних активів будуть належним чином охоплені зобов'язаннями щодо протидії відмиванню коштів.
- Компетентні органи повинні уважно стежити за розвитком подій у цій галузі та визначити, чи потрібні зміни у національних законодавчих та нормативних базах щодо ПВК/ФТ.
- У 2022 році Комісія випустить звіт про імплементацію П'ятої директиви про боротьбу з відмиванням грошей та про зусилля держав-членів щодо впровадження стандартів FATF.
- Комісія наразі здійснює оцінку нормативної бази щодо фінансових послуг, аби переконатися, що вона ефективно застосовується до віртуальних активів, які підпадають під її дію, а також вивчає, чи гарантовані законодавчі дії для віртуальних активів, які наразі не підпадають під дію нормативної бази щодо фінансових послуг, оскільки вони створюють майже ті самі ризики, що були вказані у рекомендаціях, опублікованих Європейською службою банківського нагляду органом та Європейським органом з цінних паперів та ринків у січні 2019 року.
- Комісія продовжуватиме захищати узгоджену міжнародну нормативну базу щодо віртуальних валют/віртуальних активів, спираючись на свої зусилля у G20 та органах із встановлення міжнародних стандартів. Комісія продовжує брати активну участь у роботі FATF та приєдналася до останньої контактної групи приватного сектора FATF, яка була створена для подальшого контролю за впровадженням нових стандартів щодо віртуальних валют/віртуальних активів.
- У контексті звіту про наднаціональну оцінку ризиків, Комісія продовжуватиме моніторинг ризиків, які створює Fin-Tech, обмін криптовалют на криптовалюту та використання віртуальних валют/віртуальних активів для придбання товарів високої вартості.

13. Позики підприємствам

Продукт
Кредитна позика

Сектор
Кредитний та фінансовий сектор (включаючи страхові компанії)

Опис сценарію ризиків

Злочинці погашають позики підприємствам коштами, одержаними злочинним шляхом (іноді використовуючи кредитні картки для легітимізації джерел коштів). Кредити надають злочинним коштам вигляд легітимності.

Загроза

Фінансування тероризму

Оцінка загрози фінансування тероризму, пов'язаної з позиками підприємствам, вказує на те, що було виявлено лише декілька випадків їх використання терористичними організаціями як засобу збирання коштів. Як правило, організації не мають права на такі позики (надто низький рівень заробітної плати, кошти, що надходять із соціальних виплат). У деяких випадках суб'єкти, на яких накладаються санкції (організації, включені до санаційного переліку), намагаються використовувати позики підприємствам для фінансування терористичної діяльності через компанії-оболонки, але для цього потрібен високий рівень досвіду та знань.

Висновки: Є дуже мало доказів того, що злочинці використовують/мають намір використовувати цей метод. Тому рівень загрози фінансування тероризму, пов'язаної з позиками підприємствам, вважається незначним (рівень 1).

Відмивання коштів

У ході оцінки загрози відмивання коштів, пов'язаної з позиками підприємствам, виявлено дуже мало доказів того, що злочинці мають намір використовувати цей сценарій ризику, який вони вважають непривабливим. Більшість фіктивних позик є особливістю шахрайських схем (наприклад, дві компанії беруть фіктивну позику і використовують банк для переказу коштів); вони необов'язково використовуються для відмивання доходів, одержаних злочинним шляхом. Було проведено розслідування деяких випадків позик між компаніями-співучасниками в рамках широкомасштабної системи відмивання коштів, але вони насправді не передбачали допомоги з боку фінансового сектора.

Висновки: Є дуже мало доказів того, що злочинці використовують/мають намір використовувати цей метод. Тому рівень загрози відмивання коштів, пов'язаної з позиками підприємствам, вважається помірно значним (рівень 2).

Вразливість

Фінансування тероризму

Оцінка вразливості до фінансування тероризму, пов'язаної з позиками підприємствам, розглядалася разом із схемами відмивання коштів, пов'язаними з позиками підприємствам.

Висновки: Рівень вразливості до фінансування тероризму вважається незначним (рівень 1).

Відмивання коштів

Оцінка вразливості до відмивання коштів, пов'язаної з позиками підприємствам, свідчить про таке:

a) схильність до ризику

Основний ризик, який створюють ці продукти, полягає в їх можливому достроковому погашенні компаніями, іноді готівкою (за рахунок коштів, одержаних від збільшення капітальних операцій невідомого походження).

b) обізнаність про ризики

Складається враження, що фінансові установи є досить обізнаними про ризик шахрайства, який може виникнути у зв'язку з позиками підприємствам. Вони звертають особливу увагу на ризик, пов'язаний з підробленою документацією або фіктивними ідентифікаційними даними, оскільки вони мають бути впевнені в тому, що зможуть повернути кошти. Рівень вразливості є нижчим, якщо погашення готівкових коштів не приймається. Деякі конфлікти інтересів виникають у разі погашення безнадійних кредитів.

c) законодавча база

Позики підприємствам підпадають під дію законодавчої бази в області ПВК/ФТ на рівні ЄС. Принаймні, у банківському секторі здійснювані перевірки вважаються такими, що відповідають обсягу операцій.

Висновки: Рівень вразливості до відмивання коштів вважається помірно значним (рівень 2).

Пом'якшувальні заходи:

Для держав-членів/компетентних органів:

- Тематичні перевірки небанківських операторів з акцентуванням уваги на системах моніторингу для виявлення дострокового погашення позик.

14. Споживчі кредити та позики на невеликі суми

Продукт
Кредитна позика

Сектор
Кредитний та фінансовий сектор

Опис сценарію ризиків

Терористи/організовані злочинні групи використовують (короткострокові, на невеликі суми, але під високі відсотки) споживчі кредити до заробітної плати або студентські позики. Позики надаються на відносно низькі суми, що дозволяє отримати доступ до коштів, джерела яких неможливо відстежити доти, поки гроші не будуть переказані.

Терористи/організовані злочинні групи використовують кредитні картки для зняття готівки з касових автоматів, створюючи негативне сальдо рахунка. Вони зникають з коштами без наміру відшкодування «примусового» кредиту.

Цей тип позики також може використовуватися для відмивання доходів, одержаних від злочинної діяльності. Позики використовуються для купівлі товарів високої вартості (наприклад, автомобілі, ювелірні вироби), а потім погашаються достроково.

Загроза

Фінансування тероризму

Оцінка загрози фінансування тероризму, пов’язаної із споживчим кредитом та позиками на невеликі суми, вказує на те, що терористичні групи використовують цей метод для фінансування подорожей іноземних терористів-бойовиків до країн високого ризику, що не є членами ЄС. Найпоширенішим продуктом є споживчий кредит. Залучення позик на невеликі суми полягає в тому, що вони необов'язково вимагають високого рівня знань або планування. Однак вони можуть користуватися послугами експертів, якщо національне законодавство вимагає спеціальної документації, яку деякі терористичні групи можуть підробити.

Висновки: Споживчий кредит та позики на невеликі суми є привабливими для терористичних груп, які досить часто використовували/використовують цей метод. Деякі юрисдикції можуть встановлювати умови для одержання доступу до споживчого кредиту або позик на невеликі суми, але це не є перешкодою для терористичних організацій. Тому рівень загрози фінансування тероризму, пов’язаної з позиками на невеликі суми, вважається значним (рівень 3).

Відмивання коштів

Ці продукти пропонують менший потенціал відмивання коштів, ніж інші фінансові продукти, але злочинні організації використовують їх для фінансування купівлі товарів високої вартості, а потім погашаються позики готівковими коштами.

Висновки: Споживчий кредит та позики на невеликі суми не є настільки ж привабливими для злочинних організацій, як й інші фінансові продукти, але вони можуть використовуватися опосередковано для відмивання доходів, одержаних внаслідок злочинної діяльності. Операції зазвичай здійснюються на незначні суми, але деякі злочинні групи можуть розбивати крупні суми на декілька операцій. Тому рівень загрози відмивання коштів, пов'язаної з позиками на невеликі суми, вважається помірно значним (рівень 2).

Вразливість

Фінансування тероризму

Оцінка вразливості до фінансування тероризму, пов'язаної із споживчим кредитом/позиками на невеликі суми, свідчить про таке:

a) схильність до ризику

Хоча продукти є досить поширеними, вони загалом передбачають невеликі суми, не залучають клієнтів високого ризику або клієнтів з країн високого ризику та підлягають спеціальним перевіркам фінансовими установами. Однак такі суми можуть використовуватися для терористичної діяльності, тому ризик фінансування тероризму не слід ігнорувати. Ризик може бути більшим стосовно банківських установ, які спеціалізуються на швидких споживчих кредитах, або стосовно телекомунікаційних компаній, які пропонують ці продукти.

b) обізнаність про ризики

Таке припущення щодо низької схильності до ризику нівелюється тим, що з огляду на невеликі суми сектор недостатньо обізнаний про ризики фінансування тероризму. Крім того, як і у випадку з позиками підприємствам, сектор більше обізнаний про ризики шахрайства, аніж про ризики фінансування тероризму, тому малоймовірно, що у секторі будуть ініційовані тривожні сигнали фінансування тероризму. Наявні ІТ-системи необов'язково здатні виявити підроблені документи. У разі залучення фінансових установ, перевірки на фінансування тероризму можна вважати надійними, але нові учасники ринку, такі як телекомунікаційні компанії, не підпадають під дію зобов'язань щодо ПВК/ФТ, є менш обізнаними про ризики та мають менш ефективні системи моніторингу. Підрозділи фінансової розвідки зауважили, що звіти про підозрілі операції іноді подаються надто пізно, що фактично робить неможливим подальше розслідування, оскільки сліди можливої терористичної діяльності вже обірвалися.

c) законодавча база і перевірки

Незважаючи на те, що споживчий кредит/позики на невеликі суми охоплюються законодавчою базою в області ПВК/ФТ на рівні ЄС, національне законодавство значною мірою відрізняється в частині вимог до документації. Деякі держави-члени вимагають подання спеціальних документів, а інші – ні. Якщо кредит надається банком, ризики необов'язково повністю пом'якшуються, оскільки кошти, внесені на банківський рахунок, можуть бути зняті з банкомату без перевірки. Можуть виникати нові ризики, якщо позики надаються з непрямою ідентифікацією особи.

Подібно до інших фінансових продуктів, вразливість до фінансування тероризму є вищою, якщо клієнти, пов'язані з терористичними групами, не включені до санкційних переліків, а тому не ініціюють попередження та тривожні сигнали у банківському секторі. Правоохоронним органам та компаніям слід тісніше співпрацювати з метою виявлення потенційних клієнтів, які створюють ризик фінансування тероризму, перш ніж вони вчинять терористичні акти.

Висновки: Обсяг операцій та суми під загрозою зазвичай є низькими, але це не зменшує ризику фінансування тероризму. Неефективні системи оповіщення та перевірки (незважаючи на наявні ІТ-ресурси) додають збільшують уразливість до фінансування тероризму. Деякі нові учасники ринку є менш обізнаними про ризики фінансування тероризму, ніж банківський сектор. Відмінності між національними законодавчими базами демонструють, що спроможність компетентних органів та підрозділів фінансової розвідки виявляти підозрілі операції є обмеженою, особливо якщо позики надаються нефінансовими суб'єктами. Тому рівень вразливості до фінансування тероризму, пов'язаної з позиками на невеликі суми, вважається значним (рівень 3).

Відмивання коштів

Оцінка вразливості до відмивання коштів, пов'язаної із споживчим кредитом/позиками на невеликі суми, свідчить про таке:

a) схильність до ризику

Незважаючи на невеликі суми, рівень вразливості може бути високим, якщо компанії у секторі не мають належних систем моніторингу для виявлення пов'язаних операцій або якщо клієнти можуть погасити позики готівковими коштами. Низькі граничні значення платоспроможності для одержання права на отримання позик можуть впливати на вимоги щодо належної перевірки клієнтів у разі фінансових установ. Ризик є вищим, якщо позики надходять від нефінансових установ, на які не поширюється дія зобов'язань щодо ПВК/ФТ.

Компетентні органи виявили ризики шахрайства, що походять з каналів доставки, які часто залучають агентів, яких компаніям важко контролювати. Компетентні органи також занепокоєні ризиком зловживання кредитними картками, ризиками, пов'язаними з грошовими мулами та муловими рахунками, та переказом коштів від кіберзлочинності чи шахрайства у мережі Інтернет.

b) обізнаність про ризики

Як і у випадку фінансування тероризму, припущення щодо низької схильності до ризику нівелюється тим, що з огляду на невеликі суми сектор недостатньо обізнаний про ризики фінансування тероризму. Однак складається враження, що обізнаність про ризики більше спрямована на ризики шахрайства, ніж на ризики відмивання коштів. Отже, тривожні сигнали відмивання коштів необов'язково будуть ініційовані у секторі, особливо у разі дострокового погашення. У разі залучення фінансових установ, перевірки на відмивання коштів можна вважати надійними, але нові учасники ринку, такі як телекомунікаційні компанії, не підпадають під дію зобов'язань щодо ПВК/ФТ, є менш обізнаними та мають менш ефективні системи моніторингу.

c) законодавча база і перевірки

Незважаючи на те, що споживчий кредит/позики на невеликі суми охоплюються законодавчою базою щодо ПВК/ФТ на рівні ЄС, національне законодавство значною мірою відрізняється в частині вимог до документації. Деякі держави-члени вимагають надання спеціальних документів, а інші – ні. Якщо позика надається банком, ризики необов'язково повністю пом'якшуються, оскільки кошти, внесені на банківський рахунок, можуть бути зняті з касового автомату без перевірки. Може виникнути додатковий ризик, якщо будуть залучені нові компанії Fin-Tech, з огляду на непрямі взаємовідносини з клієнтами.

Висновки: Хоча обсяг операцій та суми під загрозою обмежують схильність до ризику сектора, рівень вразливості є вищим, якщо позики надаються небанківськими установами. Відмінності між національними законодавчими базами вказують на те, що здатність компетентних органів та підрозділів фінансової розвідки виявляти підозрілі операції є обмеженою, особливо якщо позики надаються нефінансовими суб'єктами. Тому рівень вразливості до відмивання коштів, пов'язаної з позиками на невеликі суми, вважається помірно значним (рівень 2).

Пом'якшувальні заходи:

Для Комісії:

- Поліпшення співпраці між зобов'язаними суб'єктами (переважно фінансовими установами) та правоохоронними органами з метою підвищення ефективності систем моніторингу фінансування тероризму.

Для держав-членів/компетентних органів:

- Тематичні перевірки у секторі з акцентуванням уваги на оцінці систем моніторингу для виявлення дострокового погашення позик.

15. Іпотечний кредит та забезпечені активами позики на великі суми

Продукт
Іпотечний кредит

Сектор
Кредитний та фінансовий сектор

Опис сценарію ризиків

Відмивання коштів: Злочинці маскують та інвестують доходи від злочинної діяльності шляхом інвестування у нерухомість. Доходи використовуються для депозитів, погашень та дострокових погашень.

Фінансування тероризму: Злочинці використовують (середньо/довгострокові, під низькі відсотки) забезпечені активами позики на великі суми/іпотечні кредити для фінансування злочинної діяльності. Позики беруться на відносно великі суми, що дозволяє отримати доступ до коштів, джерела яких неможливо відстежити доти, поки гроші не будуть переказані.

Загроза

Фінансування тероризму

Оцінка загрози фінансування тероризму, пов'язаної з іпотечним кредитом, свідчить про те, що терористичні групи вважають цей метод дуже складним для використання і важкодоступним. Лише у кількох фактичних випадках терористичні організації використовували його для збирання коштів. Цей метод не відповідає їх потребам, оскільки вимагає наявності глибоких знань і технічних навичок для підготовки складної документації. Крім того, метою іпотечного кредитування є надання третім особам доступу до коштів, тому це не забезпечує терористичні організації легким та швидким доступом до коштів, якщо вони не вибудують відносин співучасті з такою третьою стороною.

Висновки: Іпотечний кредит вимагає високого рівня знань та досвіду для розуміння продукту і підготовки відповідної документації (підроблені документи). Він не є привабливим, оскільки передбачає співучасть третьої сторони (одержувача коштів). Тому рівень загрози фінансування тероризму, пов'язаної з іпотечним кредитом, вважається незначним (рівень 1).

Відмивання коштів

Оцінка загрози відмивання коштів, пов'язаної з іпотечним кредитом, вказує на те, що цей метод часто використовується організованими злочинними групами. Вони належним чином підготовлені для надання підробленої документації, а структура іпотеки (із залученням третіх осіб) допомагає їм приховати реального одержувача коштів. Іпотечний кредит являє собою легкий спосіб дати можливість злочинцям володіти кількома видами нерухомого майна та приховати справжній масштаб своїх активів. Цей метод все ще використовується для етапу інтеграції (здебільшого для менших сум, оскільки він не потребує складних операцій). Однак він частіше використовується у поєднанні з приховуванням особи бенефіціарного власника нерухомого майна за складним ланцюжком права власності.

Висновки: У контексті відмивання коштів, іпотечний кредит є засобом, якому надають перевагу злочинні організації. Він дозволяє їм приховувати обсяг активів та бенефіціарне право власності. Він вимагає помірного рівня знань. Отже, рівень загрози відмивання коштів, пов'язаної з іпотечним кредитом, вважається значним (рівень 3).

Вразливість

Фінансування тероризму

Оцінка вразливості до фінансування тероризму, пов'язаної з іпотечним кредитом, вказує на те, що він не є вразливим до ризиків фінансування тероризму – правоохоронними органами виявлено небагато випадків такої діяльності (за наявності). Перевірки на фінансування тероризму та обізнаність про ризики є аналогічними тим, що пов'язані з банківськими операціями.

Висновки: Незначний (рівень 1)

Відмивання коштів

Оцінка вразливості до відмивання коштів, пов'язаної з іпотечним кредитом, свідчить про таке:

a) схильність до ризику

Притаманний ризик може бути високим з огляду на зв'язок із сектором нерухомості, який злочинні організації використовують для відмивання доходів від своєї діяльності за допомогою операцій високої вартості. У разі залучення кредитних установ, ризик може бути нижчим, але він також пов'язаний з клієнтами високого ризику (наприклад, впливовими політичними особами) і може передбачати транскордонні перекази коштів.

b) обізнаність про ризики

Обізнаність кредитних установ може вважатися високою, а перевірки – надійними. Крім того, інші суб'єкти в цьому секторі (наприклад, нотаріуси) можуть допомогти у пом'якшенні ризику. Тим не менш, банки можуть зіткнутися з конфліктом інтересів, якщо внаслідок слабких перевірок клієнти високого ризику зможуть погашати крупні іпотечні кредити або безнадійні позики.

Рівень вразливості є вищим, коли операції з нерухомістю та пов'язані з ними іпотечні кредити передбачають переказ коштів з банківського рахунка у державі-члені зі слабшими перевірками на відмивання коштів для клієнтів високого ризику. Це обумовлено горизонтальною вразливістю заходів нагляду.

Рівень звітування є належним, а підрозділи фінансової розвідки та правоохоронні органи добре обізнані про вразливості у секторі.

c) законодавча база і перевірки

Іпотечний кредит включений до законодавчої бази щодо ПВК/ФТ на рівні ЄС. Перевірки вважаються досить ефективними, якщо іпотечний кредит надається кредитними установами. Крім того, ризики пом'якшуються іншими учасниками процесу (наприклад, нотаріусами).

Висновки: Якщо надані банками, продукти іпотечного кредитування є настільки ж вразливими, як і депозити на рахунках. Взаємодія із сектором нерухомості загалом збільшує вразливість, проте інші учасники операцій, такі як нотаріуси, можуть зменшити її. Тому рівень вразливості до відмивання коштів, пов'язаної з іпотечним кредитом, вважається помірно значним (рівень 2).

Пом'якшувальні заходи:

Для держав-членів/компетентних органів:

- Тематичні перевірки у секторі з акцентуванням уваги на оцінці систем моніторингу для виявлення дострокового погашення позик та на ефективності заходів належної перевірки клієнтів, особливо у разі залучення клієнтів високого ризику з третіх країн.

16. Страхування життя

Продукт
Страхування життя

Сектор
Сектор страхування

Загальний опис сектора та відповідного продукту/діяльності

Компанії зі страхування життя пропонують низку інвестиційних продуктів, з гарантіями або без них, і включають в якості компонента страхування страхові виплати на випадок смерті. З огляду на валові передплачені премії, переважними напрямками діяльності зі страхування життя в ЄЕП є страхування життя з інвестиційною складовою та індексоване страхування, інші види страхування життя та страхування прибутку.

Відповідно до статистичної бази даних ЄЦБ, загальна вартість активів страхових компаній Єврозони у 3-му кварталі 2018 року становила 7 984 млрд євро, з яких близько 3 305 млрд євро припадало на компанії із страхування життя (1 125 млрд євро – на компанії, відмінні від компаній зі страхування життя, 579 млрд євро – на компанії з перестрахування і 2 974 млрд євро – на універсальні страхові компанії).

За даними, опублікованими Європейською організацією страхування та пенсійного забезпечення, у 2017 році страхування життя в ЄС становило 876,2 млрд євро.

На додаток до Директиви про боротьбу з відмиванням грошей, спеціальні положення спрямовані на пом'якшення ризиків, пов'язаних з використанням компаній із страхування життя як інвестиційного механізму. У статті 59 Директиви 2009/138/ЄС (Платоспроможність II) (відповідно, стаття 323 Делегованого регламенту Комісії (ЄС) 2015/35) передбачається оцінка того, чи існують обґрунтовані підстави підозрювати, що у зв'язку із запропонованим придбанням (відповідно, кваліфікована частка участі акціонерів або членів, які мають кваліфіковану частку участі у спеціальній юридичній особі) здійснюється/здійснювалося відмивання коштів або фінансування тероризму чи було зроблено спробу здійснення відмивання коштів або фінансування тероризму, або що запропоноване придбання (відповідно, кваліфікована частка участі) може збільшити ризик цього.

Опис сценарію ризиків

Злочинці використовують шахрайство, пов'язане з продуктами страхування життя, для фінансування своєї діяльності. Поліси страхування життя можуть бути погашені достроково для генерування одноразових сум, особливо якщо прибуток може бути переказаний.

Ризики відмивання коштів та фінансування тероризму у страховій галузі стосуються, зокрема, страхування життя та продуктів ануїтету. Вони дозволяють клієнту вносити кошти у фінансову систему та, можливо, приховувати їх злочинне походження, або фінансувати незаконну діяльність. Відповідні сценарії ризиків, як правило, передбачають інвестиційні продукти у страхування життя (а не продукти, пов'язані зі страховими виплатами на випадок смерті як такі).

Ризики можуть виникати, коли:

1. страховик * приймає виплату премії готівкою (це не є звичайною практикою);
2. страховик відшкодовує премії, у разі скасування страхового полісу або відмови від нього, на рахунок, який не є джерелом первинного фінансування (належить

стороні, яка не є страхувальником);

3. страховик взагалі не здійснює належної перевірки «знай свого клієнта» та, зокрема, не встановлює джерело інвестицій;
4. страховик продає страхові поліси, що можуть бути передані іншій особі (рідко);
5. інвестиційні операції передбачають участь довірчих фондів, власників мандатів тощо;
6. страховик продає виготовлену під замовлення продукцію, якщо інвестор диктує базовий інвестиційний або портфельний склад; та/або
7. страховик спочатку продає невеликий інвестиційний поліс, а інвестор здійснює подальші крупні інвестиції, не проходячи додаткової належної перевірки «знай свого клієнта».

У вищезазначених сценаріях 2, 4 та 6 вище існує прямий та непрямий ризик фінансування тероризму.

У всіх перелічених вище сценаріях існує ризик відмивання коштів. Злочинці використовують сценарії ризиків 1, 6 і 7 для розміщення, 2 і 4 для заплутування слідів та 2, 4, 6 і 7 для інтеграції.

* *У всіх перелічених вище сценаріях можуть бути задіяні страховик, його агент або посередник. Для простоти, ми називаємо їх усіх «страховиком».*

Загроза

Фінансування тероризму

Оцінка загрози фінансування тероризму, пов'язаної зі страхуванням життя, вказує на те, що терористичні групи мають обмежений інтерес до цього методу. Він вимагає спеціальних знань про продукт та його особливості. Договори страхування життя не є легкодоступними, і заявки потребують великої кількості супровідної документації, що, ймовірно, відверне терористичні групи. Іноземні терористи-бойовики можуть оформити страхування життя та вимагати повернення коштів на користь членів їх родини у разі їх самогубства або гибелі. Однак законодавство держав-членів або поліси андеррайтингу страхових компаній часто не передбачають таких умов, тому ризик не є таким високим.

Висновки: Правоохоронні органи мають обмежені докази зловживання страхуванням життя для цілей фінансування тероризму. Необхідність знань та досвіду планування роблять цей метод менш привабливим. Тому рівень загрози фінансування тероризму, пов'язаної із страхуванням життя, вважається помірно значним (рівень 2).

Відмивання коштів

Оцінка загрози відмивання коштів, пов'язаної зі страхуванням життя, свідчить про те, що цей метод може використовуватися організованими злочинними групами, але щоб приховати доходи від злочинної діяльності потрібні складні домовленості (банківський рахунок, «загорнутий» у страховий поліс, кілька рахунків у третіх країнах, завантажених готівкою та використовуваних в якості забезпечення кредитної позики, надіслання грошей для полісу страхування життя). Випадки існують, але їх небагато, і того, щоб страхування життя стало привабливим варіантом, потрібне складне планування та глибокі знання.

Висновки: Виявлено деякі випадки зловживання страхуванням життям з метою відмивання коштів, але вони, як правило, є результатом застосування складних схем. Тому рівень загрози відмивання коштів, пов'язаної із страхуванням життя, вважається помірно значним (рівень 2).

Вразливість

Фінансування тероризму

Оцінка вразливості до фінансування тероризму, пов'язаної із страхуванням життя, свідчить про таке:

a) схильність до ризику

Зловживання страхуванням життя здебільшого передбачає анонімне розміщення коштів, а не їх зняття. Однак схильність до ризику здається обмеженою з огляду на обсяг відповідних операцій. Більшість компетентних органів оцінюють загальний рівень ризику фінансування тероризму як низький або помірно значний. Вони вважають, що схильність сектора до ризиків фінансування тероризму, які виникають унаслідок здійснення транскордонних операцій та діяльності, є незначним.

b) обізнаність про ризики

Складається враження, що цей сектор зовсім не обізнаний про ризики фінансування тероризму. Більшість звітів про підозрілі операції надсилаються досить пізно, оскільки страховики в області страхування життя схильні чекати на зняття коштів, перш ніж розглядати, чи є вони підозрілими. Зазвичай страховики мають доступ до значно меншої кількості інформації про своїх клієнтів, ніж інші сектори (наприклад, банки), що зменшує їх здатність будувати комплексні профілі ризиків клієнтів. Відсутність операцій означає, що підозріла діяльність виявлена переважно на основі «незвичної поведінки», а ризик фінансування тероризму визначається на початку відносин.

c) законодавча база і перевірки

Страхування життя включено до законодавчої бази щодо ПВК/ФТ на рівні ЄС.

Компетентні органи оцінюють якість перевірок у цьому секторі як здебільшого належну або прекрасну. У разі виявлення слабких місць, вони були пов'язані переважно з якістю як оцінок ризиків підприємства в цілому, так і оцінок індивідуальних ризиків, а також з відповідними недоліками в частині моніторингу та ідентифікацією і звітування про підозрілі операції.

Висновки: Рівень обізнаності про ризики у секторі є низьким, при цьому схильність до ризиків є низькою також. Було виявлено дуже мало випадків з огляду на обмежену привабливість продукту. Тому рівень вразливості до фінансування тероризму, пов'язаної із страхуванням життя, вважається низьким/помірно значним (рівень 1-2).

Відмивання коштів

Оцінка вразливості до відмивання коштів, пов'язаної із страхуванням життя, свідчить про таке:

a) схильність до ризику

Зловживання страхуванням життя здебільшого передбачає анонімне розміщення коштів, а не їх зняття. Однак схильність до ризику здається обмеженою з огляду на обсяг відповідних операцій. Більшість компетентних органів оцінюють загальний рівень ризику відмивання коштів як низький або помірно значний. Вони вважають, що схильність сектора до ризиків відмивання коштів, що виникають унаслідок здійснення транскордонних операцій та діяльності, є незначним.

b) обізнаність про ризики

Цей сектор є добре обізнаним з ризиками відмивання коштів. Однак страховики зазвичай мають доступ до значно меншої кількості інформації про своїх клієнтів, порівняно з іншими секторами (наприклад, банки), що зменшує їх здатність будувати комплексні профілі ризиків клієнтів. Така відсутність операцій означає, що підозріла діяльність виявлена переважно на основі «незвичної поведінки», а ризик відмивання коштів визначається на початку відносин.

c) законодавча база і перевірки

Послуги здебільшого надаються через банківські рахунки, які зазвичай є предметом ефективних перевірок. Компетентні органи оцінюють якість перевірок у цьому секторі як здебільшого належну або прекрасну. У разі виявлення слабких місць, вони були пов'язані переважно з якістю як оцінок ризиків підприємства в цілому, так і оцінок індивідуальних ризиків, а також з відповідними недоліками в частині моніторингу та ідентифікацією і звітуванням про підозрілі операції.

Подібно до інших секторів, рішення Fin-Tech та Reg-Tech стають дедалі більш поширеними у цьому секторі. Вони вважаються новим ризиком декількома компетентними органами, занепокоєними щодо недостатньої обізнаності про (а іноді й відсутності) нормативні вимоги щодо ПВК/ФТ, що застосовуються до рішень Reg-Tech та послуг FinTech. Відповідний новий ризик, ідентифікований компетентними органами – це перехід сектора на веб-платформи страхування та відповідні проблеми, пов'язані з рахунками, відкритими без фізичної присутності клієнта.

Висновки: Страхування життя наразі належним чином регулюється, і сектор, здається, цілком усвідомлює ризики відмивання грошей. Здійснювані перевірки виконуються правильно. Тому рівень вразливості до відмивання грошей, пов'язаної із страхуванням життя, вважається низьким/помірно значимим (рівень 1-2). Якщо продукти страхування життя використовуються як інвестиційні продукти для управління приватним капіталом або інших інвестиційних послуг, слід враховувати відповідний рівень ризику.

Пом'якшувальні заходи:

На цьому етапі не подаються жодні додаткові пропозиції.

17. Види страхування, відмінні від страхування життя

Продукт
Види страхування, відмінні від страхування життя

Сектор
Сектор страхування

Загальний опис сектора та відповідного продукту/діяльності

Поліси страхування життя, як правило, мають короткостроковий характер і слугують захистом від несподіваних збитків, таких як пошкодження майна. З огляду на валові передплачені премії, переважними напрямками діяльності в області страхування, відмінного від страхування життя, є страхування життя, яке пов'язано з відповідальністю за автомобільні транспортні засоби, пожежі та інші збитки майна та медичні витрати.

Відповідно до статистичної бази даних ЄЦБ, загальна вартість активів страхових компаній Єврозони у 3-му кварталі 2018 року становила 7 984 млрд євро, з яких близько 3 305 млрд євро припадало на компанії із страхування життя (1 125 млрд євро – на компанії, відмінні від компаній зі страхування життя, 579 млрд євро – на компанії з перестрахування і 2 974 млрд євро – на універсальні страхові компанії).

Страхові премії на найбільшому ринку страхування, відмінному від страхування життя, ринку автомобільного страхування у 2017 році становили 137,5 млрд євро, згідно з даними, опублікованими Insurance Europe, за яким слідує ринок страхування майна (101,5 млрд євро), ринок страхування від нещасних випадків (36,1 млрд євро) та ринок страхування загальної відповідальності (40,1 млрд євро); страхові премії за медичне страхування склали 131,5 млрд євро.

Спеціальні положення спрямовані на пом'якшення ризиків, пов'язаних із володінням акцій страхових компаній. У статті 59 Директиви 2009/138/ЄС (Платоспроможність II) (відповідно, стаття 323 Делегованого регламенту Комісії (ЄС) 2015/35) передбачається оцінка того, чи існують обґрунтовані підстави підозрювати, що у зв'язку із запропонованим придбанням (відповідно, кваліфікована частка участі акціонерів або членів, які мають кваліфіковану частку участі у спеціальній юридичній особі) здійснюється/здійснювалося відмивання коштів або фінансування тероризму чи було зроблено спробу здійснення відмивання коштів або фінансування тероризму, або що запропоноване придбання (відповідно, кваліфікована частка участі) може збільшити ризик цього.

Опис сценарію ризиків

Злочинці вчиняють шахрайство, пов'язане зі страхуванням на робочому місці, страхуванням автомобілів тощо, для фінансування своєї діяльності.

Відмивання коштів може мати місце у контексті та як мотив страхового шахрайства, пов'язаного із страхуванням, відмінним від страхування життя, наприклад, якщо це призводить до подання вимоги про повернення частини інвестованих незаконних коштів. Відповідні сценарії ризику, як правило, передбачають часті страхові премії та скасування. Ризики можуть виникати або реалізовуватися, якщо страховик*:

1. приймає страхові премії готівкою, хоча це не є звичайною практикою;
2. відшкодовує страхові премії, у разі скасування або відмови від полісу страхування, на рахунок, який не є джерелом первинного фінансування (належить стороні, яка не

є страхувальником).

Особи, які відмивають кошти, прагнуть використовувати сценарій 1 для розміщення та сценарій 2 для замітання слідів/інтеграції.

* *У наведених вище прикладах у процес може бути залучений страховик або його агент чи посередник. Для простоти, ми називаємо їх усіх «страховиком».*

Загроза

Фінансування тероризму

Аналогічно, ризик фінансування тероризму пов'язаний із страховими шахрайствами для одержання доступу до джерел доходу для терористичної діяльності. Такі схеми виявлені, наприклад, у страхуванні на робочих місцях та страхуванні автомобілів. Навряд чи можна стверджувати, що цей метод не має жодної актуальності, і деякі докази його використання були зібрані після терористичних атак, але він вимагає певного планування та важливих документальних свідчень, які роблять його відносно непривабливим для терористичних груп. Однак для порівняння, ми можемо стверджувати, що він представляє той самий рівень загрози фінансування тероризму, що і той, що стосується страхування життя.

Висновки: Правоохоронні органи мають обмежені докази зловживання страхуванням, відмінним від страхування життя, для цілей фінансування тероризму. Для нього потрібні знання та досвід планування, які роблять його відносно непривабливим. Тому рівень загрози фінансування тероризму, пов'язаної із страхуванням, відмінним від страхування життя, вважається помірно значним (рівень 2).

Відмивання коштів

Оцінка загрози відмивання коштів, пов'язаної із страхуванням життя (наприклад, страхування автомобілів чи страхування на робочих місцях), вказує на те, що, на відміну від фінансування тероризму, зловживання відмиванням коштів передбачає використання складних схем, які роблять сценарій ризику недостатньо безпечним чи привабливим. Правоохоронні органи не мають конкретних доказів того, що страхування, відмінне від страхування життя, використовується для відмивання доходів, одержаних злочинним шляхом.

Висновки: Страхування, відмінне від страхування життя, не використовується для цілей відмивання коштів, оскільки воно вимагає певного планування та знань, які роблять його відносно непривабливим. Тому рівень вразливості до відмивання коштів, пов'язаної із страхуванням, відмінним від страхування життя, вважається незначним/таким, що не має значення (рівень 1).

Вразливість

Фінансування тероризму

Оцінка вразливості до фінансування тероризму, пов'язаної із страхуванням, відмінним від страхування життя (наприклад, страхування автомобілів або страхування на робочих місцях), вказує на те, що можуть мати місце два випадки:

(i) незадекларовані роботи у шахрайстві в області роздрібній торгівлі автомобілями/страхуванням автомобілів: кошти від шахрайської діяльності надсилаються шляхом переказу готівки; та

(ii) автомобілі підпалюють для отримання страхової виплати.

a) схильність до ризику

Схильність до ризику є обмеженою, оскільки йдеться про величезні суми грошей, і до коштів не можна отримати доступ без попередньої ідентифікації.

b) обізнаність про ризики

Загалом, страхування, відмінне від страхування життя, є більш вразливим, ніж страхування життя, тому що сектор необов'язково є обізнаним про ризики (належна перевірка клієнтів не здійснюється і не ведеться облік), а спеціальні тривожні сигнали фінансування тероризму чи відмивання коштів не завжди ініціюються. Емітенти полісів страхування, як правило, приділяють більше уваги на момент виплати, коли ризик сприймається як більш високий.

c) законодавча база і перевірки

Страхування, відмінне від страхування життя, не підпадає під дію законодавчої бази щодо ПВК/ФТ на рівні ЄС. Якщо держави-члени мають чинні нормативні положення, перевірки (у деяких випадках, пов'язані із самодекларацією), здається, працюють задовільно.

Висновки: У багатьох державах-членах законодавство призвело до проведення перевірок та підвищення обізнаності у секторі. Однак все ж таки є певні недоліки у виявленні підозрілих транзакцій та звітуванні. Тому рівень вразливості до фінансування тероризму, пов'язаної із страхуванням, відмінним від страхування життя, вважається помірно значним (рівень 2).

Відмивання коштів

Оцінка вразливості до відмивання коштів, пов'язаної із страхуванням, відмінним від страхування життя (наприклад, страхування автомобілів або страхування на робочих місцях), свідчить про таке:

a) схильність до ризику

Здебільшого страхування, відмінне від страхування життя, не використовується для відмивання коштів у більш широкому контексті шахрайства (підроблені інвестиції, одноденна компанія).

b) обізнаність про ризики

Реалізація належної перевірки клієнтів не є поширеною у ЄС, але коли у держав-членів створена система протидії відмиванню грошей для страхування, відмінного від страхування життя, вони зазначають, що зобов'язані суб'єкти, як правило, не застосовують жодну належну перевірку клієнтів взагалі.

Однак, враховуючи кількість відповідних випадків, немає жодних доказів того, що це збільшує ризик відмивання грошей.

c) законодавча база і перевірки

Немає жодних вимог ЄС щодо включення страхування, відмінного від страхування життя, до сфери ПВК/ФТ. Законодавча база страхування, відмінного від страхування життя, не залежить від національного законодавства.

Висновки: Було виявлено небагато випадків, коли страхування, відмінне від страхування життя, використовувалося для відмивання коштів. Як правило, це робиться в рамках ширшої схеми шахрайства. Тому рівень вразливості до відмивання коштів, пов'язаної із страхуванням, відмінним від страхування життя, вважається незначним (рівень 1)/таким, що не має значення.

Пом'якшувальні заходи:

На цьому етапі не подаються жодні додаткові пропозиції.

18. Послуги відповідального зберігання

Продукт
Послуги відповідального зберігання

Сектор
Кредитний та фінансовий сектор, а також охоронні компанії

Опис сценарію ризиків

Злочинці орендують декілька (комерційних чи банківських) послуг відповідального зберігання для зберігання крупних сум валюти, грошових інструментів або активів високої вартості до їх конвертації у валюту для розміщення у банківській системі. Аналогічно, вони можуть відкрити декілька рахунків для відповідального зберігання для зберігання великі кількості цінних паперів до їх продажу та конвертації у валюту, грошові інструменти, вихідні перекази коштів або їх комбінацію для розміщення у банківській системі. Зони вільної торгівлі можуть використовуватися для приховування незаконної діяльності та надходжень від неї.

Загроза

Фінансування тероризму

Загроза фінансування тероризму, пов'язана з послугами відповідального зберігання, не вважається актуальною. Тому вони не є частиною оцінки.

Висновки: Не має значення

Відмивання коштів

Оцінка загрози відмивання коштів, пов'язаної з послугами відповідального зберігання, вказує на те, що особливістю такого сценарію ризику є те, що активи зберігаються та необов'язково конвертуються. Як результат, це може бути фінансово непривабливим. Однак це дозволяє приховати доходи від злочину без ризику їх виявлення. За даними правоохоронних органів, такі «сплячі» депозитні системи дедалі частіше використовуються для безпечних депозитів та вилучення активів з фінансової системи.

Точні дані важко отримати, тому що послуги відповідального зберігання також використовуються для родичів. Це додатковий аспект загрози відмивання коштів, оскільки особа, яка внесла кошти, необов'язково є особою, яка їх знімає.

Суб'єкти ринку, крім банків, також надають такі послуги (об'єкти зберігання), що розширює спектр інструментів, доступних злочинним організаціям, та підвищує рівень загрози.

Висновки: Багато держав-членів помітили тенденцію до зростання випадків використання цього методу злочинними організаціями для приховування доходів, одержаних злочинним шляхом. Послуги відповідального зберігання є досить привабливими, оскільки не вимагають спеціальних знань та є досить надійним інструментом для ухилення від сплати податків чи перевірок в області протидії відмиванню грошей. Тому рівень загрози відмивання коштів, пов'язаної з безпечними депозитами, вважається значним (рівень 3).

Вразливість

Фінансування тероризму

Вразливість до фінансування тероризму, пов'язана з послугами відповідального зберігання, не вважається особливо актуальною. Тому вразливість до фінансування тероризму не є частиною оцінки.

Висновки: Не має значення

Відмивання коштів

Оцінюючи вразливість до відмивання коштів, пов'язану з безпечними депозитами, слід розрізняти послуги, що надаються кредитними установами, та послуги, що надаються небанківськими організаціями (об'єкти зберігання).

a) схильність до ризику

В обох випадках схильність до ризику є високою, оскільки крупні суми грошових коштів можуть бути під загрозою. Цей рівень схильності до ризику може бути більшим у разі участі клієнтів високого ризику.

b) обізнаність про ризики

Основні аспекти належної перевірки клієнтів застосовуються до послуг відповідального зберігання, що надаються кредитними установами. Деякі компетентні органи застосовують активний підхід у цьому секторі, але банки залишаються вразливими щодо вмісту сейфів. Як правило, вони не мають інформації про розміщені в них кошти. Приватні компанії, які надають такі послуги, не всі відповідають вимогам ПВК/ФТ, деякі приймають готівкові платежі за оренду сейфів. Інше питання полягає в тому, чи виникає ризик фінансування тероризму під час зберігання або лише після внесення коштів у реальну економіку. З точки зору правоохоронних органів, чим більше зберігається коштів, тим простіше підтримувати анонімність операції.

c) законодавча база і перевірки

Послуги відповідального зберігання та притулки вільних зон як такі не включаються до законодавчої бази щодо ПВК/ФТ на рівні ЄС. Однак послуги відповідального зберігання, що надаються кредитними та фінансовими установами, включаються у законодавчу базу, що застосовується до таких зобов'язаних суб'єктів. Підприємства, що надають послуги відповідального зберігання, перелічені у пункті 14 Додатка I до Директиви 2013/36/ЄС, підпадають під дію правил щодо ПВК/ФТ. Однак на практиці фінансові установи можуть бути не в змозі виконати свої зобов'язання з моніторингу та оцінити джерело коштів, оскільки вони не володіють інформацією про вміст сейфів. Крім того, це не стосується комерційних компаній, що надають послуги зберігання, або інших об'єктів зберігання, які можуть використовуватися для надання подібних послуг. У деяких країнах певні послуги зберігання/безпеки в цілому регулюються та контролюються як такі.

Висновки: Якщо надаються кредитними та фінансовими установами, послуги відповідального зберігання підлягають вимогам належної перевірки клієнтів та перевіркам. Однак встановити точне джерело коштів не завжди можливо, і поточний моніторинг може мати «сліпі плями», оскільки фінансова установа зазвичай не володіє інформацією про вміст. Крім того, безпечні депозити можуть бути доступні сторонам, крім початкового клієнта, що збільшує вразливість. Ринок фрагментується з появою приватних підприємств та інших послуг комерційного зберігання/безпеки. Тому рівень вразливості до відмивання коштів вважається помірно значним/значним (рівень 2-3).

Пом'якшувальні заходи:

Для держав-членів/компетентних органів:

- Тематичні перевірки у секторі з акцентуванням уваги на ефективності вимог щодо належної перевірки клієнтів у фінансових та нефінансових установах, які пропонують послуги відповідального зберігання.

НЕФІНАНСОВІ ПРОДУКТИ

1. Створення юридичних суб'єктів та юридичних утворень

Продукт/Послуга
Створення юридичних суб'єктів та юридичних утворень

Сектор
Особи, які надають послуги з управління довірчими фондами та компаніями, юристи, податкові консультанти/бухгалтери/аудитори, консультанти з питань структури капіталу та галузевої стратегії, консультанти та провайдери послуг з питань злиття і поглинання та консультанти з питань бізнес-стратегій («професійні посередники»)

Загальний опис сектора та відповідного продукту/діяльності

Особи, які надають послуги з управління довірчими фондами та компаніями, юристи, податкові консультанти/бухгалтери та консультанти з питань структури капіталу та галузевої стратегії, консультанти та провайдери послуг з питань злиття і поглинання та консультанти з питань бізнес-стратегій надають широкий спектр послуг фізичним та юридичним особам для комерційних підприємств та управління капіталом.

Четверта директива про боротьбу з відмиванням грошей вимагає, щоб суб'єкти ідентифікували бенефіціарного власника при встановленні ділових відносин та вживали відповідних заходів на основі ризиків для верифікації особи бенефіціарних власників, як визначено у частині 6 статті 3.

На додаток до законодавства про боротьбу з відмиванням грошей у вказаних нижче директивах ЄС стосовно закону про компанії передбачені загальні правила заснування товариств з обмеженою відповідальністю, особливо що стосується вимог до капіталу та розкриття інформації. Європейське законодавство про компанії частково кодифіковане у Директиві 2017/1132/ЄС[49] стосовно деяких аспектів законодавства про компанії, і держави-члени продовжують застосовувати окремі закони про компанії, які час від часу приводяться у відповідність до директив та норм ЄС.

Директива 2017/1132/ЄС охоплює такі питання:

1. **Розкриття інформації** про документи компанії, чинність зобов'язань компанії та їх анулювання. Директива застосовується до всіх публічних та приватних компаній з обмеженою відповідальністю.
2. **Формування** публічних компаній з обмеженою відповідальністю та правил щодо **збереження та зміни їх капіталу**. Директива встановлює мінімальну вимогу до капіталу для публічних компаній з обмеженою відповідальністю ЄС у розмірі 25 000 євро.

49

3. Вимоги до розкриття інформації для **іноземних філій** компаній. Директива охоплює компанії ЄС, які заснували філії в іншій країні ЄС, або компанії з країн, які не є державами-членами ЄС, що засновують філії в ЄС.

Крім того, Директива 2009/102/ЄС[50] стосовно законодавства про компанії щодо приватних товариств з обмеженою відповідальністю з єдиним учасником забезпечує законодавчі вимоги для заснування **компанії з єдиним учасником** (в якій всі акції належать одному акціонеру). Директива охоплює приватні товариства з обмеженою відповідальністю, але країни ЄС можуть прийняти рішення поширити Директиву на публічні товариства з обмеженою відповідальністю. Вона замінює Директиву 89/667/ЄЕС (Дванадцята директива Ради стосовно законодавства про компанії).

- Ця Директива також забезпечує законодавчу основу для заснування **компанії з єдиним учасником** (в якій всі акції належать одному акціонеру). Директива охоплює приватні товариства з обмеженою відповідальністю, але країни ЄС можуть прийняти рішення поширити її на публічні товариства з обмеженою відповідальністю. Вона замінює Директиву 89/667/ЄЕС.

Правила щодо формування, вимоги до капіталу та розкриття інформації доповнюються стандартами бухгалтерського обліку та фінансової звітності.[51]

Включені до переліку компанії також мають відповідати певним **вимогам щодо прозорості**.[52]

Опис сценарію ризиків

Злочинці створюють складні структури, що включають багато юрисдикцій, зокрема офшорні юрисдикції з таємними ланцюгами права власності, як правило, через компанії-оболонки,[53] коли власник іншої компанії чи іншої юридичної структури зареєстрований в іншому місці. Кандидати призначаються і зобов'язані лише очолювати компанію, приховуючи зв'язок із справжнім бенефіціарним власником. Залучаючи офшорні компанії, злочинці можуть залишатися анонімними, повертати кошти, отримані від злочинної діяльності, у правову економіку та вчиняти податкові шахрайства, ухилятися від сплати податків та інші дії, що шкодять державному бюджету або приховують джерела коштів.

Це передбачає створення «непрозорих структур», які визначаються як структури, в якій приховується справжня особа кінцевого(-их) бенефіціарного(-их) власника(-ів) суб'єктів та юридичних утворень, наприклад, шляхом використання номінальних директорів. У таких випадках складається враження, що бенефіціарним власником компанії є директор. Такі схеми використовуються офшорними юрисдикціями зі слабкими законодавчими базами в області відмивання коштів/фінансування тероризму, які залучають значні інвестиції. Обсяг світового утримуваного офшорного капіталу у 2017 році становив приблизно 8,2 трлн доларів США, що на 6 % більше, ніж у попередньому році у доларовому еквіваленті.[54] За попередньою оцінкою, обсяг офшорного капіталу, утримуваного резидентами ЄС, у 2016 році становив 1,6 трлн доларів

---

[50] Директива 2009/102/ЄС Європейського Парламенту та Ради від 16 вересня 2009 року стосовно законодавства про компанії щодо приватних товариств з обмеженою відповідальністю з єдиним учасником (Текс має значення для ЄЕП); OB L 258, 01.10.2009, с. 20-25.

[51] Звітування компанії: https://ec.europa.eu/info/business-economy-euro/company-reporting-and-auditing/company-reporting_en.

[52] Ринки цінних паперів: https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-markets/securities- markets_en.

[53] Огляд компаній-оболонок у Європейському Союзі: http://www.europarl.europa.eu/RegData/etudes/STUD/2018/627129/EPRS_STU(2018)627129_EN.pdf.

[54] Звіт щодо глобального капіталу 2018 Бостонської консультаційної групи: http://image-src.bcg.com/Images/BCG- Seizing-the-Analytics-Advantage-June-2018-R-3_tcm9-194512.pdf.

США.[55]

Загальні зауваження

У такому сценарії ризиків оцінка охоплює таких юридичних суб'єктів, як компанії, корпоративні структури, фонди, асоціації, некомерційні організації, благодійні організації та подібні структури. Вона також охоплює довірчі фонди та інші юридичні утворення з подібною структурою або функціями (наприклад, *fiducie, treuhand, fideicomiso*…). Оцінка ризиків стосується характеру діяльності, а не структури як такої. Цей підхід не заперечує специфіку юридичних суб'єктів порівняно з юридичними утвореннями (останні не мають правосуб'єктності та здебільшого є договірними відносинами). Однак, що стосується характеру послуги (тут створення структури), ці специфічні особливості не мають суттєвого значення: юридичні суб'єкти та юридичні утворення можна використовувати однаково для приховування справжніх бенфіціарних власників. Злочинці обирають тип структури, залежно від правового середовища певної юрисдикції, свого досвіду та як їх зручно. Організовані злочинні групи можуть легко створювати всі ці структури, і всі вони можуть стати засобами для створення непрозорих і складних схем, що ускладнюють ідентифікацію реального власника та реального походження коштів.

Загроза

Фінансування тероризму

Злочинці мають намір створювати непрозорі структури, які можуть обійти будь-які обмежувальні заходи. Оцінка загрози фінансування тероризму, пов'язаної зі створенням юридичних суб'єктів та юридичних утворень, вказує на те, що терористичні організації можуть мати труднощі зі створенням таких структур. Це обумовлено тим, що ці терористичні організації зазвичай включені до санкційоного переліку. Чим більше терористична організація хоче приховати особу свого бенефіціарного власника, тим складнішим має бути процес. Для створення цих структур необхідні знання як внутрішніх, так і міжнародних регулятивних та податкових норм, що передбачає високий рівень досвіду, який можуть надати лише професійні посередники. Тим не менш, правоохоронні органи та підрозділи фінансової розвідки визначили кілька простих методів, за допомогою яких злочинці використовують банківські рахунки та професійних посередників для швидкого і легкого створення структур для збирання грошових коштів з метою фінансування терористичної діяльності. Тому здатність створювати юридичних суб'єктів та юридичні утворення є актуальною для загрози фінансування тероризму, хоча правоохоронними органами зареєстровано лише обмежену кількість таких випадків.

Висновки: Виявлено небагато випадків використання цих методів для фінансування тероризму. Це може бути обумовлено тим, що високий рівень необхідних технічних навичок та знань відвертає терористичні організації, які надають перевагу простішим та більш доступним рішенням. Тому рівень загрози фінансування тероризму, пов'язаної зі створенням юридичних структур, вважається помірно значним (рівень 2).

[55] Дослідження ECOPA та CASE, яке готується до випуску: *«Оцінка міжнародного ухилення від сплати податків фізичними особами» (Estimating International Tax Evasion by Individuals).*

Відмивання коштів

Оцінка загрози відмивання коштів, пов'язаної зі створенням юридичних суб'єктів та юридичних утворень, вказує на те, що цей інструмент майже виключно використовується для приховування бенефіціарного права власності. З точки зору витрат, створення юридичного суб'єкта або юридичного утворення є досить простим і може бути здійснено у режимі онлайн. Компанії-оболонки зі звичайною заявленою діяльністю та без операцій є дуже поширеними. Компанії-оболонки, які вже функціонують кілька років, акції яких передаються новим акціонерам, коштують дорожче, але й більш затребувані злочинцями. Фонди також є привабливими, оскільки компетентні органи не здійснюють контролю над коштами. У всіх таких суб'єктів відсутня реальна економічна діяльність. Можуть знадобитися певні витрати або вищий рівень знань/планування, якщо злочинні організації вдаються до послуг посередників для створення складніших структур, наприклад, залучаючи більше ніж одну юрисдикцію, аби краще приховати справжню особу власників. Для створення таких структур необхідні знання як внутрішніх, так і міжнародних регулятивних та податкових норм, що передбачає високий рівень знань, який можуть надавати лише професійні посередники. Складні ланцюги права власності у різних країнах збільшують непрозорість схеми відмивання коштів. Однак, що стосується створення самої структури, якщо використання посередників є достатнім для приховування бенефіцірної власності, це є привабливим і досить безпечним методом відмивання доходів, одержаних злочинним шляхом.

На думку підрозділів фінансової розвідки та правоохоронних органів, цей метод часто використовується злочинними організаціями. Одна організована злочинна група може використовувати декілька типів професійних посередників, залежно від поставленої задачі. Це є основною особливістю у більшості випадках, повідомлених Європолу, де схеми відмивання коштів здійснюються за допомогою професіоналів у різних сферах, як правило, юристів та бухгалтерів. Наприклад, радники з економічних питань розробляють механізм інтеграції одержаних злочинним шляхом коштів у правову фінансову систему, а юристи шукають юридичне обґрунтування для такої діяльності. Це пояснює складність діючих механізмів відмивання коштів та необхідність експертних знань для їх формування та уникнення виявлення.

Висновки: Хоча створення юридичних суб'єктів чи юридичних утворень не може бути відокремлено від самої підприємницької діяльності, цей сценарій ризику вважається привабливим інструментом для відмивання доходів, одержаних злочинним шляхом. Тому рівень загрози відмивання коштів, пов'язаної із створенням юридичних структур, вважається значним/дуже значним (рівень 3/4).

Вразливість

Фінансування тероризму

Оцінка вразливості до фінансування тероризму, пов'язаної зі створенням юридичних суб'єктів або юридичних утворень, свідчить про таке:

а) схильність до ризику

Одним з аспектів схильності до ризику є те, що юридичні суб'єкти та юридичні утворення за певних обставин можуть легко створюватися дистанційно та без спеціальних вимог до ідентифікації (через незахищені канали доставки). Процес може бути повністю анонімним, і терористичні групи, розташовані у зонах підвищеного ризику, можуть мимоволі користуватися послугами професійних посередників для створення структури без законної цілі. За інших обставин, непряме створення структур може передбачати залучення послуг професійних посередників, які знаходяться за межами ЄС. У такому разі вхідною точкою для ідентифікації особи бенефіціарного власника залишається фінансова установа, відповідальна за відкриття банківського рахунка. Нарешті, деякі посередники або треті сторони можуть надавати спеціальні послуги для приховування бенефіціарного права власності, що впливає на професію в цілому, змушуючи її вважати такою, що сприяє створенню таких схем фінансування тероризму.

b) обізнаність про ризики

Загалом, складається враження, що професійні посередники усвідомлюють ризики зловживання їх послугами за незаконними запитами щодо створення юридичних суб'єктів та юридичних утворень. Ризик використання таких структур для приховування беенфіціарного власника є добре відомим. Однак, враховуючи той факт, що у контексті фінансування тероризму для створення юридичних суб'єктів та юридичних утворень все ще можуть використовуватися законні кошти, тривожні сигнали не спрацьовують належним чином. До створення таких структур може бути залучено декілька професійних секторів, і компетентні органи не завжди в змозі забезпечити належний контроль таких професійних секторів.

c) законодавча база і засоби контролю

Бухгалтери, аудитори, податкові радники та юристи (з 2001 року), особи, які надають послуги з управління довірчими фондами та компаніями, (з 2005 року) та консультанти з питань структури капіталу та галузевої стратегії, консультанти і провайдери послуг з питань злиття і поглинання та консультанти з питань бізнес-стратегій (з 2005 року) підлягають вимогам ЄС щодо протидії відмиванню коштів.

Виходячи з рівня звітування про підозрілі операції, компетентні органи вважають, що здійснювані перевірки є недостатніми, а елементи, зібрані на початку ділових відносин, недостатньо розроблені для виявлення та аналізу ризиків фінансування тероризму, пов'язаних зі створенням юридичних суб'єктів або юридичних утворень.

Держави-члени ЄС мають різні регуляторні та податкові режими, які можуть використовуватися терористичними організаціями. Приведення у виконання вимог щодо ідентифікації бенефіціарного власника на початку ділових відносин залишається важливим викликом для зацікавлених суб'єктів. Незважаючи на те, що дуже складно пов'язати компанії-оболонки з їх власниками, експерти з питань безпеки та правоохоронці погоджуються, що компанії-оболонки чи інші юридичні суб'єкти, такі як довірчі фонди, становлять загрозу національній безпеці. Вони майже унеможливлюють пошук людей, які фактично фінансують терористичну та іншу злочинну діяльність, і можуть бути ідеальними засобами для фінансування діяльності терористів.[56]

Що стосується консультантів з питань структури капіталу та галузевої стратегії, консультантів та провайдерів послуг з питань злиття і поглинання та консультантів з питань бізнес-стратегій, немає інформації про те, як вони контролюються компетентними органами та чи відповідають вони вимогам щодо протидії відмиванню коштів та фінансуванню тероризму.

[56] «Ці американські компанії приховують особу торговців наркотиками, мафіозі та терористів» (These U.S. companies hide drug dealers, mobsters and terrorists), Мелані Хікен та Блейк Елліс, CNN Money, 9 грудня 2015 року.

Висновки: Хоча це необов'язково є найбільш використовуваним методом для фінансування тероризму, рівень вразливості до фінансування тероризму, пов'язаної із створенням юридичних структур, вважається значним/дуже значним (рівень 3/4).

Відмивання коштів

Оцінка вразливості до відмивання коштів, пов'язаної зі створенням юридичних суб'єктів або юридичних утворень, свідчить про таке:

a) схильність до ризику

Головним аспектом схильності до ризику є те, що юридичні суб'єкти та юридичні утворення за певних обставин можуть легко створюватися дистанційно та без спеціальних вимог до ідентифікації (через незахищені канали доставки). Процес може бути повністю анонімним, і терористичні групи, розташовані у зонах підвищеного ризику, можуть мимоволі користуватися послугами професійних посередників для створення структури без законної цілі. За інших обставин, непряме створення структур може передбачати залучення послуг професійних посередників, які знаходяться за межами ЄС. У такому разі вхідною точкою для ідентифікації особи бенефіціарного власника залишається фінансова установа, відповідальна за відкриття банківського рахунка. Нарешті, деякі посередники або треті сторони можуть надавати спеціальні послуги для приховування бенефіціарного права власності, що впливає на професію в цілому, змушуючи її вважати такою, що сприяє створенню таких схем фінансування тероризму

b) обізнаність про ризики

Складається враження, що як особи, які надають послуги з управління довірчими фондами та компаніями, так і юристи/податкові консультанти усвідомлюють ризики незаконних запитів щодо створення юридичних суб'єктів та юридичних утворень. Ризик використання таких структур для приховування бенефіціарного власника є добре відомим. Однак все ще мають місце значні недоліки у приведенні до виконання. Це має місце, коли у створенні структур беруть участь декілька зобов'язаних суб'єктів, і коли застосування належної перевірки клієнтів, включаючи того, хто є бенефіціарним власником, покладається на фінансовий сектор, який не завжди добре протистоїть ситуаціям, коли бенефіціарний власник добровільно приховується.

Мають місце також значні недоліки у розумінні суб'єктами своїх зобов'язань щодо протидії відмиванню коштів або навіть знаннях про такі зобов'язання. Це особливо стосується використання юридичних утворень загального права, таких як довірчі фонди, які є менш прозорими правовими структурами, незнайомими країнам цивільного законодавства та невідомими у їхньому національному законодавстві або використовуваними як інвестиційні фонди/підприємства. Навіть якщо доступні настанови щодо застосування вимог для протидії відмиванню коштів до юридичних утворень у цих юрисдикціях цивільного законодавства – та щодо застосування належної перевірки клієнтів – все ще важко отримати належний огляд таких правових структур. Це особливо стосується правових угод загального права, укладених у країнах, які не є членами ЄС.

Обізнаність про ризики консультантів в області структури капіталу та галузевої стратегії, консультантів та провайдерів послуг в області злиття і поглинання та консультантів в області бізнес-стратегій неможливо оцінити, оскільки немає інформації про те, чи застосовують вони вимоги щодо ПВК/ФТ.

c) законодавча база і засоби контролю

Законодавча база: Бухгалтери, аудитори, податкові радники та юристи (з 2001 року), особи, які надають послуги з управління довірчими фондами та компаніями, (з 2005 року) та консультанти з питань структури капіталу та галузевої стратегії, консультанти і провайдери послуг з питань злиття і поглинання та консультанти з питань бізнес-стратегій (з 2005 року) підлягають вимогам ЄС щодо протидії відмиванню коштів.

Чинна законодавча база ЄС вимагає: (і) здійснення ідентифікації бенефіціарного власника до встановлення ділових відносин; та (іі) створення державами-членами центрального реєстру даних про бенефіціарне право власності корпоративних та інших юридичних суб'єктів, зареєстрованих на території кожної держави-члена.

Тим не менш, держави-члени ЄС все ще мають різні регуляторні та податкові норми, які можуть використовуватися терористичними організаціями. Ці організації можуть користуватися перевагами більш м'яких законодавчих вимог в області ПВК/ФТ для ідентифікації бенефіціарних власників юридичних суб'єктів та юридичних утворень або національними режимами, які не передбачають податок на доходи фізичних чи корпоративних осіб.

Засоби контролю: Компетентні органи влади та підрозділи фінансової розвідки звернули вагу на причетність офшорних юрисдикцій, де здатність правоохоронних органів здійснювати розслідування залежить від наявності угод про взаємну правову допомогу з такими юрисдикціями. Наслідком цього є те, що за відсутності угоди про взаємну правову допомогу процес ідентифікації бенефіціарного права власності стикається з перешкодами.

Запроваджено ІТ-інструменти для швидкого та анонімного створення корпоративних структур без участі державного органу. У разі юридичних утворень, деякі з них можуть бути створені неофіційно, що створює додаткові перешкоди для перевірок.

Що стосується консультантів в області структури капіталу та галузевої стратегії, консультантів та провайдерів послуг в області злиття і поглинання та консультантів в області бізнес-стратегій, немає інформації про те, як компетентні органи контролюють їх та чи відповідають вони вимогам щодо ПВК/ФТ.

Висновки: Схильність до ризику відмивання коштів, пов'язаного зі створенням юридичних суб'єктів чи юридичних утворень, вважається значною з огляду на існуючий рівень анонімності та характеристики клієнтів та залучених галузей, зокрема, коли основні чи спрощені ІТ-інструменти використовуються без залучення державного органу. Рівень обізнаності про ризики професійних посередників здається досить задовільним, хоча кількість звітів про підозрілі операції залишається дуже низькою.[57]

[57] У звіті FATF за 2013 рік зазначається, що *«рівень звітування юридичного сектора навряд чи буде на такому самому рівні, що і у фінансових установах. Існує значна різниця в обсязі операцій, здійснюваних юристами у порівнянні з фінансовими установами. Крім того, рівень участі в кожній операції, який впливає на базу, на якій може виникнути та бути оціненою підозра, суттєво відрізняється.»* Відповідно, на сторінці 24 звіту визначено *«більш релевантне порівняння»* для юридичного сектора, можливо, з іншими встановленими нефінансовими підприємствами і професіями, *«особливо тими, що надають професійні послуги»*, з яких *«звіти юристів в середньому становили 10 %, коливаючись від менше 1% до 20%»*. Звіт включає вибірку звітів про підозрілі операції для юристів та встановлених нефінансових підприємств і професій у 2010 та 2011 роках для ряду країн.

Навіть після транспозиції державами-членами Директив ЄС про боротьбу з відмиванням грошей та призначення встановлених нефінансових підприємств і професій, з 2001 року багатьом державам-членам досі не вистачає надійної законодавчої бази в області ПВК/ФТ, і складається враження, що положення розуміються невірно. Законодавча база не адаптована до ризику (бенефіціарне право власності визначається після створення структури, а не раніше), а необхідні перевірки були введені лише нещодавно у Четвертій та П'ятій директивах про боротьбу з відмиванням грошей. Тому рівень вразливості до відмивання коштів, пов'язаної із створенням юридичних суб'єктів, юридичних утворень та некомерційних організацій/благодійних фондів, вважається значним/дуже значним (рівень 3/4).

Пом'якшувальні заходи:

Незважаючи на значні покращення у прийнятті та реалізації стандартів Групи з розробки фінансових заходів боротьби з відмиванням грошей (FATF) та схваленні державами-членами роботи Організації економічного співробітництва та розвитку щодо прозорості протягом останніх років, необхідність подальшого підвищення загальної прозорості економічного та фінансового середовища ЄС є зрозумілою. Ми не можемо ефективно запобігати відмиванню коштів та фінансуванню тероризму, якщо навколишнє середовище не буде ворожим до злочинців, які шукають притулку для своїх фінансів шляхом використання непрозорих структур. Цілісність фінансової системи ЄС залежить від прозорості корпоративних та інших юридичних суб'єктів, довірчих фондів та подібних юридичних утворень. Основними принципами заходів ЄС є виявлення та розслідування випадків відмивання коштів та запобігання їх виникненню. Підвищення прозорості може стати потужним стримуючим фактором.

З моменту підготовки першого звіту щодо Наднаціональної оцінки ризиків (SNRA), ЄС переглянув свою законодавчу базу щодо ПВК/ФТ для пом'якшення ризиків, пов'язаних з відмиванням коштів та фінансуванням тероризму. У 2015 році ЄС прийняв модернізовану регулятивну базу, яка охоплює:

- **Директиву (ЄС) 2015/849** про запобігання використанню фінансової системи для відмивання грошей або фінансування тероризму (Четверта директива про боротьбу з відмиванням грошей).[58]

- **Регламент (ЄС) 2015/847** щодо інформації про платника, яка супроводжує перекази коштів[59] — робить перекази коштів більш прозорими, тим самим допомагаючи правоохоронним органам відстежувати терористів та злочинців.

[58] Директива (ЄС) 2015/849 Європейського Парламенту та Ради від 20 травня 2015 року про запобігання використанню фінансової системи для відмивання коштів або фінансування тероризму, що вносить зміни до Регламенту (ЄС) № 648/2012 Європейського Парламенту та Ради і скасовує Директиву 2005/60/ЄС Європейського Парламенту та Ради і Директиву Комісії 2006/70/ЄС (Текст має значення для ЄЕП); OB L 141, 05.06.2015, с. 73-117.

[59] Регламент (ЄС) 2015/847 Європейського Парламенту та Ради від 20 травня 2015 року щодо інформації, яка супроводжує переказ коштів, та про скасування Регламенту (ЄС) №о 1781/2006 (Текст має значення для ЄЕП); OB L 141, 05.06.2015, с. 1-18.

Обидва законодавчі акти враховують рекомендації FATC за 2012 рік та продовжують розглядати низку питань щодо просування найвищих можливих стандартів протидії відмиванню коштів та фінансуванню тероризму.

- **Директива (ЄС) 2018/843, П'ята директива про боротьбу з відмиванням грошей[60] (Поправки до Четвертої директиви про боротьбу з відмиванням грошей).**
- **Директива 2018/822/ЄС[61]**, яка вимагає від посередників надання інформації про підзвітні транскордонні податкові утворення їх національним органам влади[62], набирає чинності з 2020 року.

П'ята директива про боротьбу з відмиванням грошей, яка вносить зміни у Четверту директиву про боротьбу з відмиванням грошей, була опублікована в Офіційному віснику Європейського Союзу 19 червня 2018 року. Держави-члени повинні транспонувати цю Директиву до 10 січня 2020 року, але певні зміни мають бути внесені до 10 березня 2020 року. До 10 березня 2021 року мають бути узгоджені реєстри про бенефіціарне право власності.

Що стосується створення юридичних суб'єктів та, зокрема, юридичних утворень, поправки, внесені цією новою законодавчою базою:

- покращують прозорість реальних власників компаній;
- покращують прозорість реальних власників довірчих фондів;
- встановлюють взаємозв'язок реєстрів бенефіціарного права власності на рівні ЄС; та
- покращують співпрацю та обмін інформацією між органами нагляду в області протидії відмиванню коштів та між ними та пруденційними органами нагляду та Європейським центральним банком.

У цій покращеній базі основними завданнями для компетентних органів/саморегулюючих органів залишаються:

- Держави-члени повинні забезпечити організацію компетентними органами/органами саморегулювання навчальних сесій та надання настанов щодо факторів ризику з акцентуванням уваги на непрямих комерційних відносинах, офшорних професійних посередниках, клієнтах або юрисдикціях та складних структурах/структурах-оболонках.

[60] Директива (ЄС) 2018/843 Європейського Парламенту та Ради від 30 травня 2018 року, яка вносить зміни у Директиву (ЄС) 2015/849 про запобігання використанню фінансової системи для відмивання коштів або фінансування тероризму та у Директиви 2009/138/ЄС та 2013/36/ЄС (Текст має значення для ЄЕП); OB L 156, 19.06.2018, с. 43–74.

[61] Директива Ради (ЄС) 2018/822 від 25 травня 2018 року, яка вносить зміни у Директиву 2011/16/ЄС стосовно обов'язкового автоматичного обміну інформацією у сфері оподаткування щодо підзвітних транскордонних утворень; OB L 139, 05.06.2018, с. 1-13.

[62] Адміністративна співпраця у (прямому) оподаткування в ЄС: https://ec.europa.eu/taxation_customs/business/tax-cooperation-control/administrative-cooperation/enhanced-administrative-cooperation-field-direct-taxation_en.

- Держави-члени повинні забезпечити, що органи саморегулювання/компетентні органи здійснюватимуть тематичні перевірки того, наскільки виконуються вимоги щодо ідентифікації бенефіціарних власників.

- Щорічні звіти про заходи, вжиті для перевірки дотримання цими суб'єктами своїх зобов'язань щодо належної перевірки клієнтів, включаючи вимоги щодо бенефіціарного права власності, звіти про підозрілі операції та внутрішні засоби контролю мають бути надані компетентними органами/органами саморегулювання державам-членам.

- Держави-члени мають забезпечити, що консультанти з питань структури капіталу та галузевої стратегії, консультанти та провайдери послуг з питань злиття і поглинання та консультанти з питань бізнес-стратегій виконуватимуть свої зобов'язання щодо бенефіціарного права власності.

2. Комерційна діяльність юридичних суб'єктів та юридичних утворень

Продукт/Послуга
Комерційна діяльність юридичних суб'єктів та юридичних утворень

Сектор
Особи, які надають послуги з управління довірчими фондами та компаніями, юристи, податкові консультанти/бухгалтери/аудитори, консультанти з питань структури капіталу та галузевої стратегії, консультанти та провайдери послуг з питань злиття і поглинання та консультанти з питань бізнес-стратегій («професійні посередники»)

Загальний опис сектора та відповідного продукту/діяльності

Особи, які надають послуги з управління довірчими фондами та компаніями, юристи, податкові консультанти/бухгалтери та консультанти з питань структури капіталу та галузевої стратегії, консультанти та провайдери послуг з питань злиття і поглинання та консультанти з питань бізнес-стратегій надають широкий спектр послуг фізичним та юридичним особам для комерційних підприємств та управління капіталом.

Четверта директива про боротьбу з відмиванням грошей вимагає, щоб суб'єкти ідентифікували бенефіціарного власника при встановленні ділових відносин та вживали відповідних заходів на основі ризиків для верифікації особи бенефіціарних власників, як визначено у частині 6 статті 3.

На додаток до законодавства про боротьбу з відмиванням грошей у вказаних нижче директивах ЄС стосовно закону про компанії передбачені загальні правила заснування товариств з обмеженою відповідальністю, особливо що стосується вимог до капіталу та розкриття інформації. Європейське законодавство про компанії частково кодифіковане у Директиві 2017/1132/ЄС стосовно деяких аспектів законодавства про компанії, і держави-члени продовжують застосовувати окремі закони про компанії, які час від часу приводяться у відповідність до директив та норм ЄС.

Директива 2017/1132/ЄС охоплює такі питання:

1. **Розкриття інформації** про документи компанії, чинність зобов'язань компанії та їх анулювання. Директива застосовується до всіх публічних та приватних компаній з обмеженою відповідальністю.
2. **Формування** публічних компаній з обмеженою відповідальністю та правил щодо **збереження та зміни їх капіталу**. Директива встановлює мінімальну вимогу до капіталу для публічних компаній з обмеженою відповідальністю ЄС у розмірі 25 000 євро.

3. Вимоги до розкриття інформації для **іноземних філій** компаній. Директива охоплює компанії ЄС, які заснували філії в іншій країні ЄС, або компанії з країн, які не є державами-членами ЄС, що засновують філії в ЄС.

Крім того, Директива **2009/102/ЄС** (Дванадцята директива стосовно законодавства про компанії) забезпечує законодавчі вимоги для заснування **компанії з єдиним учасником** (в якій всі акції належать одному акціонеру). Директива охоплює приватні товариства з обмеженою відповідальністю, але країни ЄС можуть прийняти рішення поширити Директиву на публічні товариства з обмеженою відповідальністю. Вона замінює Директиву 89/667/ЄЕС.

Правила щодо формування, вимоги до капіталу та розкриття інформації доповнюються **стандартами бухгалтерського обліку та фінансової звітності**.[63]

Включені до переліку компанії також мають відповідати певним **вимогам щодо прозорості**.[64]

Опис сценарію ризиків

Підставні компанії, які використовуються для шахрайства шляхом виставлення фальшивих рахунків-фактур: Злочинці використовують підставні компанії для виставлення фальшивих рахунків-фактур на імпортні товари, при цьому переплати використовуються для терористичних цілей.

Відмивання коштів на основі торговельної діяльності: Злочинці використовують відмивання коштів на основі торговельної діяльності (TBML) для обґрунтування перміщення злочинних доходів через банківські канали (за допомогою акредитивів, рахунків-фактур тощо) або за допомогою глобальних операцій часто з використанням підроблених документів для торгівлі товарами та послугами.[65] Це може уможливлювати швидкий переказ крупних сум, виправдовуючи стверджувану економічну мету. Схеми відмивання коштів на основі торговельної діяльності також використовуються міжнародними терористичними групами зі складними схемами фінансування.[66]

Шахрайські позики: Компанії надають одна одній фіктивні позики для того, щоб створити інформаційний слід з метою обґрунтування переказів коштів незаконного походження. Злочинці використовують фіктивні позики для обґрунтування переміщення злочинних доходів через банківські канали – без будь-якого економічного обґрунтування.

З точки зору законодавства, ЄС прийняв кілька директив щодо бухгалтерського обліку[67] та встановив вимоги до аудиту для забезпечення того, що у звітності компаній буд відображена справжня і точна інформація.

---

[63] Звітування компанії:
https://ec.europa.eu/info/business-economy-euro/company-reporting-and-auditing/company-reporting_en.
[64] Ринки цінних паперів:
https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-markets/securities- markets_en.
[65] Відмивання коштів на основі торговельної діяльності – FATF:
http://www.fatf-gafi.org/publications/methodsandtrends/documents/trade-basedmoneylaundering.html.
[66] «Управління по боротьбі з наркотиками та європейські органи влади розкривають схему масштабної торгівлі наркотиками та відмивання грошей Хезболла» (DEA and European Authorities Uncover Massive Hezbollah Drug and Money Laundering Scheme), Управління по боротьбі з наркотиками - 1 лютого 2016 року: справа ліванської групи Хезболла, яка відмиває значні суми доходів від торгівлі наркотиками в Європі в рамках схеми відмивання коштів на основі торговельної діяльності, відомої як чорний ринок обміну песо.
[67] Огляд звітування компанії:
https://ec.europa.eu/info/business-economy-euro/company-reporting-and-auditing/company-reporting_en#overview.

Загальні зауваження

Для цього сценарію ризиків оцінка охоплює таких юридичних суб'єктів, як компанії, корпоративні структури, фонди, асоціації, некомерційні організації, благодійні організації та подібні структури. Вона також охоплює довірчі фонди та інші юридичні утворення зі структурою або функціями, подібними до структури та функцій довірчих фондів (наприклад, *fiducie, treuhand, fideicomiso*…).

Оцінка ризиків стосується характеру діяльності, а не структури як такої. Цей підхід не заперечує специфіку юридичних суб'єктів порівняно з юридичними утвореннями (останні не мають правосуб'єктності та здебільшого є договірними відносинами). Однак, що стосується характеру послуги (тут створення структури), ці специфічні особливості не мають суттєвого значення: юридичні суб'єкти та юридичні утворення можна використовувати однаково для приховування справжніх бенфіціарних власників. Злочинці обирають тип структури, залежно від правового середовища певної юрисдикції, свого досвіду та як їх зручно. Організовані злочинні групи можуть легко створювати всі ці структури, і всі вони можуть стати засобами для створення непрозорих і складних схем, що ускладнюють ідентифікацію реального власника та реального походження коштів.

Загроза

Фінансування тероризму

Оцінка загрози фінансування тероризму, пов'язаної з підприємницькою діяльністю юридичних суб'єктів або юридичних утворень, вказує на те, що терористичні групи не надають перевагу такому методу фінансування терористичної діяльності. На думку правоохоронних органів, такий сценарій ризику не є досить привабливим для терористичних груп, оскільки він вимагає створення непрозорої структури (незаконного юридичного суб'єкта або юридичного утворення) або проникнення у право власності законного юридичного суб'єкта чи юридичного утворення. Він вимагає знань та здатності планувати. З огляду на різні заходи, які мають бути вжити, малоймовірно, що цей метод допоможе швидко зібрати «чисті» гроші. Однак, якщо злочинці мають досвід, вони можуть використовувати цей метод для грошових переказів замість інших класичних прийомів (послуги з переказу грошових коштів, система «хавала» тощо). Метод може бути привабливим, якщо необхідно переказати великий обсяг коштів для фінансування терористичної діяльності. Тому терористичні групи можуть мати намір використовувати його.

Висновки: На основі доказів, наданих правоохоронними органами та підрозділами фінансової розвідки, рівень загрози фінансування тероризму, пов'язаної з комерційною діяльністю юридичних суб'єктів та юридичних утворень, вважається <u>помірно значним</u> (рівень 2).

<u>Відмивання коштів</u>

Оцінка загрози відмивання коштів, пов'язаної з комерційною діяльністю юридичних суб'єктів або юридичних утворень, вказує на те, що найбільш поширеними способами, які використовуються організованими злочинними групами для відмивання доходів, одержаних злочинним шляхом, є відмивання коштів на основі торговельної діяльності та виставлення фальшивих рахунків-фактур. Такі незаконні операції дозволяють виводити законні кошти з грошових потоків компанії: (i) шляхом використання підроблених рахунків-фактур; (ii) шляхом зменшення бази для обчислення податку; (iii) шляхом зменшення податку на прибуток, виводячи законні кошти з компанії; та (iv) шляхом відмивання незаконних доходів, знімаючи готівкові кошти з рахунка іншої компанії через посередників. Дедалі більше торгових операцій насправді є законними та передбачають експорт товарів та продукції за ринковою ціною, але переважно оплачуються готівкою та експортуються перед реекспортом між різними країнами. Це стосується переважно товарів високої вартості (автомобілі, товари електроніки, предмети розкоші), але все частіше включаються товари низької вартості/великого обсягу, такі як

агропродовольча продукція.

Майже у всіх випадках для відмивання своїх злочинних доходів організовані злочинні групи використовують законні бізнес-структури. Цей метод широко відомий як «бізнес-ресайклінг» (відмивання злочинних доходів через законний бізнес). Підприємства з високим оборотом готівки, такі як об'єкти громадського харчування чи роздрібної торгівлі, забезпечують належне покриття джерела інакше незрозумілих обсягів готівки. Ці підприємства можуть використовуватися організованими злочинними групами різними способами, але в більшості випадків вони використовуються як законне джерело доходу від клієнтів для полегшення суміщення незаконних коштів із законними коштами. У цих випадках послуги бухгалтера-співучасника використовуються для легітимізації злочинних грошових потоків за допомогою фальшивих рахунків-фактур, квитанцій та рахунків. У деяких інших випадках підприємство не має жодної законної діяльності, а отже не має законного джерела грошових коштів. Тому фіктивні рахунки та операції створюються з метою маскування злочинних доходів під виглядом законних надходжень від торгівлі товарами та послугами. Фінансова звітність також може підроблятися для відображення грошових потоків.

Незважаючи на те, що необхідні знання та здатність планувати не ігноруються, правоохоронні органи та підрозділи фінансової розвідки вважають, що організовані злочинні групи часто застосовують цей метод, оскільки він є досить доступним, низькозатратним і його досить легко використовувати. Однак цей метод також включає кілька секторів. Наприклад, грошові перекази через структури компаній зазвичай обробляються через банківський сектор.

Висновки: Незважаючи на те, що формування схеми відмивання коштів на основі торговельної діяльності може вимагати помірного рівня технічних знань та досвіду, підрозділи фінансової розвідки та правоохоронні органи виявили багато таких випадків, які свідчать про те, що цей метод є досить доступним і легким у використанні. Виходячи з цього, рівень загрози відмивання коштів, пов'язаної з комерційною діяльністю юридичних суб'єктів та юридичних утворень, та рівень загрози відмивання коштів на основі торговельної діяльності вважаються <u>дуже значними</u> (рівень 4).

Вразливість

Фінансування тероризму

Оцінка вразливості до фінансування тероризму, пов'язаної з комерційною діяльністю юридичних суб'єктів або юридичних утворень, свідчить про таке:

a) схильність до ризику

Значні суми можуть збиратися за рахунок комерційної діяльності для фінансування терористичних організацій та їх діяльності. Така комерційна діяльність здебільшого залежить від грошових коштів і може включати транскордонні операції з третіми країнами високого ризику.

b) обізнаність про ризики

Складається враження, що як особи, які надають послуги з управління довірчими фондами та компаніями, так і юристи/податкові консультанти усвідомлюють ризик зловживання їх послугами для створення юридичних суб'єктів та юридичних утворень. Ризик можливого використання таких структур для приховування бенефіціарного власника є добре відомим. Однак все ще мають місце значні недоліки у розумінні ними своїх зобов'язань щодо ПВК/ФТ, або навіть їх знаннях про такі зобов'язання. Зокрема, враховуючи те, що у контексті фінансування тероризму комерційна діяльність все ще може покладатися на законні гроші, це необов'язково ініціює тривожні сигнали. Здійснювані перевірки є досить слабкими, тому

підрозділи фінансової розвідки можуть виявляти та аналізувати ризики фінансування тероризму, пов'язані з комерційною діяльністю через юридичних суб'єктів або юридичні утворення, за обмежених обставин. До створення правових структур можуть залучатися багато професійних секторів, і компетентні органи не завжди в змозі надати належні настанови таким професійним секторам.

c) законодавча база і перевірки

Законодавча база: Бухгалтери, аудитори, податкові радники та юристи (з 2001 року), особи, які надають послуги з управління довірчими фондами та компаніями, (з 2005 року) та консультанти з питань структури капіталу та галузевої стратегії, консультанти і провайдери послуг з питань злиття і поглинання та консультанти з питань бізнес-стратегій (з 2005 року) підлягають вимогам ЄС щодо протидії відмиванню коштів. Ці вимоги ЄС передбачають, що ідентифікація бенефіціарного власника правової структури або юридичного утворення, включаючи некомерційні організації або фонди, здійснюється перед початком ділових відносин.

Перевірки:
На думку компетентних органів, кількість здійснюваних перевірок є недостатньою і елементи, зібрані на початку ділових відносин, є недостатніми для виявлення та аналізу ризиків фінансування тероризму, пов'язаних із створенням та діяльністю юридичних суб'єктів та юридичних утворень.

Що стосується консультантів в області структури капіталу та галузевої стратегії, консультантів та провайдерів послуг в області злиття і поглинання та консультантів в області бізнес-стратегій, немає інформації про те, як компетентні органи контролюють їх та чи відповідають вони вимогам щодо ПВК/ФТ.

Висновки: На основі зібраних елементів і незважаючи на те, що цей метод необов'язково є найбільш очевидним способом фінансування тероризму, рівень вразливості до фінансування тероризму, пов'язаної з комерційною діяльністю юридичних суб'єктів та юридичних утворень, вважається значним (рівень 3).

Відмивання коштів

Оцінка вразливості до відмивання коштів, пов'язаної із створенням юридичних суб'єктів або юридичних утворень, свідчить про таке:

a) схильність до ризику

Шахрайські позики широко використовуються організованими злочинними групами. У деяких випадках відмивання коштів на основі торговельної діяльності може передбачати здійснення великої кількості міжнародних торговельних операцій, які нелегко відстежувати банкам. Це може ускладнюватися постійним використанням підставних осіб, що може впливати на рівень вразливості.

b) обізнаність про ризики

Складається враження, що як особи, які надають послуги з управління довірчими фондами та компаніями, так і юристи/податкові консультанти усвідомлюють ризик зловживання їх послугами для створення юридичних суб'єктів та юридичних утворень для незаконних цілей, пов'язаних з відмиванням коштів та фінансуванням тероризму. Ризик використання таких структур для приховування бенефіціарного власника є добре відомим. Загалом, особи, які надають послуги з управління довірчими фондами та компаніями, усвідомлюють, що вони не повинні мати справу з третіми особами без забезпечення належного нормативно-правового

дотримання. Однак операції, які перебувають під загрозою, є досить складними (зокрема, транскордонні), що ускладнює слідчу роботу правоохоронних органів. Незаконне походження коштів, як правило, важко довести з огляду на кількість людей/органів та географічних зон і використовуваних каналів. Тому підозрілі операції досить важко виявити (відмивання коштів на основі торговельної діяльності та виставлення шахрайських рахунків-фактур).

c) законодавча база і перевірки

Законодавча база: Бухгалтери, аудитори, податкові радники та юристи (з 2001 року), особи, які надають послуги з управління довірчими фондами та компаніями, (з 2005 року) та консультанти з питань структури капіталу та галузевої стратегії, консультанти і провайдери послуг з питань злиття і поглинання та консультанти з питань бізнес-стратегій (з 2005 року) підлягають вимогам ЄС щодо протидії відмиванню коштів. Ці вимоги ЄС передбачають, що ідентифікація бенефіціарного власника правової структури або юридичного утворення, включаючи некомерційні організації або фонди, здійснюється перед початком ділових відносин.

Перевірки: У деяких ситуаціях, компетентні органи влади та підрозділи фінансової розвідки звернули уваги на причетність офшорних юрисдикцій, де здатність правоохоронних органів здійснювати розслідування залежить від наявності угод про взаємну правову допомогу з такими юрисдикціями. Наслідком цього є те, що за відсутності угоди про взаємну правову угоду, процес ідентифікації бенефіціарного права власності припиняється.

Що стосується консультантів в області структури капіталу та галузевої стратегії, консультантів та провайдерів послуг в області злиття і поглинання та консультантів в області бізнес-стратегій, немає інформації про те, як компетентні органи контролюють їх та чи відповідають вони вимогам щодо ПВК/ФТ.

Висновки: Схильність до ризику у секторі вважається дуже значною з огляду на відсутність надійної бази щодо відмивання коштів у багатьох юрисдикціях країн, які не є членами ЄС, особливо з огляду на відсутність правил щодо ідентифікації бенефіціарних власників. Це означає, що перевірки не здійснюються у непрозорих структурах, які включають багато юрисдикцій. Крім того, немає інформації про те, чи відповідає цей сектор вимогам щодо ПВК/ФТ. Виходячи з цього, рівень загрози відмивання коштів, пов'язаної з комерційною діяльністю через правові структури та на основі торговельної діяльності, вважається значним/дуже значним (рівень 3/4).

Пом'якшувальні заходи:

Відповідно до вдосконаленої законодавчої бази, запровадженої Четвертою директивою про боротьбу з відмиванням грошей, та згідно із змінами, передбаченими вимогами щодо прозорості у П'ятій директиві про боротьбу з відмиванням грошей, інформація про бенефіціарне право власності для юридичних суб'єктів та юридичних утворень була зміцнена:

- З'ясовано фактор, що визначає, яка держава-член несе відповідальність за моніторинг та реєстрацію інформації про бенефіціарне право власності для довірчих фондів та подібних юридичних утворень.

- Доступ громадськості до інформації про бенефіціарне право власності дозволяє громадянському суспільству більш ретельно перевіряти інформацію, в тому числі пресі або організаціям громадянського суспільства, і сприяє збереженню довіри до доброчесності комерційних операцій та фінансової системи.

- Посилений громадський контроль допомагає запобігти зловживанню юридичними суб'єктами та юридичними утвореннями, включаючи ухилення від сплати податків.

- Центральні реєстри держав-членів, що містять інформацію про бенефіціарне право власності, мають бути узгоджені через Європейську центральну платформу, передбачену Директивою (ЄС) 2017/1132.

- Директива 2018/822/ЄС набирає чинності з 2020 року, коли посередники стануть зобов'язаними звітувати перед національними органами про автоматичний обмін інформацією щодо транскордонних механізмів оподаткування.[68]

<u>У цій покращеній базі основними завданнями компетентних органів/ органів саморегулювання залишаються:</u>

- Компетентні органи/органи саморегулювання повинні забезпечити проведення підготовки та надання настанов щодо факторів ризику, акцентуючи увагу на непрямих ділових відносинах, офшорних професійних посередниках, клієнтах чи юрисдикціях, а також на складних структурах/структурах-оболонках.

- Органи саморегулювання/компетентні органи повинні здійснювати тематичні перевірки того, наскільки виконуються вимоги щодо ідентифікації бенефіціарних власників.

- Щорічні звіти про заходи, вжиті для перевірки дотримання цими суб'єктами своїх зобов'язань щодо належної перевірки клієнтів, включаючи вимоги щодо бенефіціарного права власності, звіти про підозрілі операції та внутрішні засоби контролю мають бути надані компетентними органами/органами саморегулювання державам-членам.

[68] Адміністративна співпраця в (прямому) оподаткуванні в ЄС: https://ec.europa.eu/taxation_customs/business/tax-cooperation-control/administrative- cooperation/enhanced-administrative-cooperation-field-direct-taxation_en.

3. Припинення діяльності юридичних суб'єктів та юридичних утворень

Продукт
Припинення комерційної діяльності юридичних суб'єктів та юридичних утворень

Сектор
Особи, які надають послуги з управління довірчими фондами та компаніями, юристи, податкові консультанти/бухгалтери/аудитори, консультанти з питань структури капіталу та галузевої стратегії, консультанти та провайдери послуг з питань злиття і поглинання та консультанти з питань бізнес-стратегій («професійні посередники»)

Загальний опис сектора та відповідного продукту/діяльності

Особи, які надають послуги з управління довірчими фондами та компаніями, юристи, податкові консультанти/бухгалтери та консультанти з питань структури капіталу та галузевої стратегії, консультанти та провайдери послуг з питань злиття і поглинання та консультанти з питань бізнес-стратегій надають широкий спектр послуг фізичним та юридичним особам для комерційних підприємств та управління капіталом.

Четверта директива про боротьбу з відмиванням грошей вимагає, щоб суб'єкти ідентифікували бенефіціарного власника при встановленні ділових відносин та вживали відповідних заходів на основі ризиків для верифікації особи бенефіціарних власників, як визначено у частині 6 статті 3.

На додаток до законодавства про боротьбу з відмиванням грошей у вказаних нижче директивах ЄС стосовно закону про компанії передбачені загальні правила заснування товариств з обмеженою відповідальністю, особливо що стосується вимог до капіталу та розкриття інформації. Європейське законодавство про компанії частково кодифіковане у Директиві 2017/1132/ЄС[69] стосовно деяких аспектів законодавства про компанії, і держави-члени продовжують застосовувати окремі закони про компанії, які час від часу приводяться у відповідність до директив та норм ЄС.

Директива 2017/1132/ЄС охоплює такі питання:

[69] Директива (ЄС) 2017/1132 Європейського Парламенту та Ради від 14 червня 2017 року щодо певних аспектів законодавства про компанії (Текст має значення для ЄЕП); OB L 169, 30.06.2017, с. 46-127.

1. **Розкриття інформації** про документи компанії, чинність зобов'язань компанії та їх анулювання. Директива застосовується до всіх публічних та приватних компаній з обмеженою відповідальністю.
2. **Формування** публічних компаній з обмеженою відповідальністю та правил щодо **збереження та зміни їх капіталу**. Директива встановлює мінімальну вимогу до капіталу для публічних компаній з обмеженою відповідальністю ЄС у розмірі 25 000 євро.
3. Вимоги до розкриття інформації для **іноземних філій** компаній. Директива охоплює компанії ЄС, які заснували філії в іншій країні ЄС, або компанії з країн, які не є державами-членами ЄС, що засновують філії в ЄС.

Крім того, Директива **2009/102/ЄС**[70] (Дванадцята директива стосовно законодавства про компанії) забезпечує законодавчі вимоги для заснування **компанії з єдиним учасником** (в якій всі акції належать одному акціонеру). Директива охоплює приватні товариства з обмеженою відповідальністю, але країни ЄС можуть прийняти рішення поширити Директиву на публічні товариства з обмеженою відповідальністю. Вона замінює Директиву 89/667/ЄЕС.

Правила щодо формування, вимоги до капіталу та розкриття інформації доповнюються **стандартами бухгалтерського обліку та фінансової звітності**.[71]

Включені до переліку компанії також мають відповідати певним **вимогам щодо прозорості**.[72]

Опис сценарію ризиків

Шахрайство з використанням банкрутства/юридичної ліквідації компанії: після банкрутства компанії ту саму компанію купує колишній акціонер, який створює нову структуру для здійснення тієї самої комерційної діяльності, але тепер без фінансових труднощів. Зловмисники вилучають кошти з підставної компанії до виявлення незаконної діяльності або до вилучення активів компетентними органами, маскуючи аудиторський слід грошей, відмитих через ліквідовану компанію.

Загальні зауваження

Для цього сценарію ризиків оцінка охоплює таких юридичних суб'єктів, як компанії, корпоративні структури, фонди, асоціації, некомерційні організації, благодійні організації та подібні структури. Вона також охоплює довірчі фонди та інші юридичні утворення зі структурою або функціями, подібними до структури та функцій довірчих фондів (наприклад, *fiducie, treuhand, fideicomiso*…).

Оцінка ризиків стосується характеру діяльності, а не структури як такої. Цей підхід не заперечує специфіку юридичних суб'єктів порівняно з юридичними утвореннями (останні не мають правосуб'єктності та здебільшого є договірними відносинами). Однак, що стосується характеру послуги (тут створення структури), ці специфічні особливості не мають суттєвого значення: юридичні суб'єкти та юридичні утворення можна використовувати однаково для приховування справжніх бенфіціарних власників. Злочинці обирають тип структури, залежно від правового

[70] Директива 2009/102/ЄС Європейського Парламенту та Ради від 16 вересня 2009 року щодо законодавства про компанії стосовно приватних товариств з обмеженою відповідальністю з єдиним учасником (Текст має значення для ЄЕП); OB L 258, 01.10.2009, с. 20-25.
[71] Звітування компанії:
https://ec.europa.eu/info/business-economy-euro/company-reporting-and-auditing/company-reporting_en.
[72] Ринки цінних паперів:
https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-markets/securities-markets_en.

середовища певної юрисдикції, свого досвіду та як їх зручно. Організовані злочинні групи можуть легко створювати всі ці структури, і всі вони можуть стати засобами для створення непрозорих і складних схем, що ускладнюють ідентифікацію реального власника та реального походження коштів.

Загроза

Фінансування тероризму

Оцінка загрози фінансування тероризму, пов'язаної з припиненням комерційної діяльності, розглядається разом із схемами відмивання коштів, пов'язаними з припиненням комерційної діяльності, з метою приховування незаконного походження коштів. У таких ситуаціях, загроза фінансування тероризму не нівелюється окремою оцінкою.

Висновок: Оцінка загрози фінансування тероризму, пов'язаної з припиненням діяльності, вважається значним/помірно значною (рівень 1/2).

Відмивання коштів

Оцінка загрози відмивання коштів, пов'язаної з припиненням комерційної діяльності через юридичні структури, свідчить про те, що банкрутство є частиною більш глобального процесу, а деякі судові адміністратори повідомляють про випадки, коли фіктивне банкрутство було використано для відмивання доходів, одержаних злочинним шляхом. Однак правоохоронні органи виявили кілька випадків. Це свідчить про те, що злочинні організації сприймають цей метод як неприваблений або важкодоступний, оскільки він вимагає певних здібностей матеріально-технічного забезпечення та планування.

Висновки: На основі елементів, зібраних на етапі оцінювання, рівень загрози відмивання коштів, пов'язаної з припиненням комерційної діяльності, вважається значним/помірно значним (рівень 1/2).

Вразливість

Фінансування тероризму

Оцінка вразливості до фінансування тероризму, пов'язаної з припиненням комерційної діяльності, розглядається разом із схемами відмивання коштів, пов'язаними з припиненням комерційної діяльності, з метою приховування незаконного походження коштів. У таких ситуаціях, загроза фінансування тероризму не нівелюється окремою оцінкою.

Висновки: У таких ситуаціях, рівень вразливості є помірно значним (рівень 2)

Відмивання коштів

Оцінка вразливості до відмивання коштів, пов'язаної з припиненням комерційної діяльності через юридичні структури, свідчить про таке:

a) схильність до ризику

Ситуації, коли припинення комерційної діяльності під загрозою, починаються зазвичай з випадків шахрайства.

b) обізнаність про ризики

Виявлення використання цього методу правоохоронними органами та підрозділами фінансової розвідки є легким, враховуючи, що він здебільшого починається з інциденту шахрайства. Таке предикатне правопорушення ініціює тривожні сигнали для сектора або для компетентних органів. Загалом банкрутство складно реалізувати, і зобов'язані суб'єкти (зокрема, банки) приділяють особливу увагу таким сценаріям, більшість з яких вважаються підозрілими.

c) законодавча база і засоби контролю

Бухгалтери, аудитори, податкові радники та юристи (з 2001 року), особи, які надають послуги з управління довірчими фондами та компаніями, (з 2005 року) та консультанти з питань структури капіталу та галузевої стратегії, консультанти і провайдери послуг з питань злиття і поглинання та консультанти з питань бізнес-стратегій (з 2005 року) підлягають вимогам ЄС щодо протидії відмиванню коштів.

Не існує жодного спеціального положення, яке б охоплювало цю ситуацію в рамках законодавчої бази ЄС про протидію відмиванню коштів, окрім необхідності ідентифікувати та звітувати про підозрілі зобов'язання зобов'язаними суб'єктами. Але кількість отриманих звітів про підозрілі операції свідчить про те, що здійснювані перевірки є ефективними та дозволяють виявляти підозрілі ситуації. Додатковим елементом контролю є також директори з питань неплатоспроможності, що керують процедурою неплатоспроможності.

Що стосується консультантів в області структури капіталу та галузевої стратегії, консультантів та провайдерів послуг в області злиття і поглинання та консультантів в області бізнес-стратегій, немає інформації про те, як компетентні органи контролюють їх та чи відповідають вони вимогам щодо ПВК/ФТ.

Висновки: Хоча банкрутство є проблемним питанням для деяких держав-членів, виявлення таких випадків та рівня обізнаності сектора та інших зобов'язаних суб'єктів призводить до оцінки того, що рівень вразливості є <u>помірно значним</u> (рівень 2).

Пом'якшувальні заходи:

Чинна законодавча база ЄС посилила вимоги прозорості до інформації про бенефіціарне право власності для юридичних суб'єктів та юридичних утворень. Вона також передбачає та уточнює роль певних сторін, які діють як зобов'язані суб'єкти.

У цій покращеній базі основними завданнями для компетентних органів/саморегулюючих органів залишаються:

А/ якщо припинення пов'язане із створенням іншого юридичного суб'єкта або юридичного утворення

Для компетентних органів/органів саморегулювання:

- Держави-члени повинні забезпечити, що компетентні органи/органи саморегулювання проводитимуть навчальні сесії та надаватимуть настанови щодо факторів ризику, акцентуючи увагу на непрямих ділових відносинах, офшорних професійних посередниках/клієнтах чи юрисдикціях, а також складних структурах/структурах-оболонках.

- Держави-члени повинні забезпечити, що органи саморегулювання/компетентні органи здійснюватимуть тематичні перевірки того, наскільки виконуються вимоги щодо ідентифікації бенефіціарних власників.

- Щорічні звіти про заходи, вжиті для верифікації дотримання цими зобов'язаними суб'єктами своїх зобов'язань щодо належної перевірки клієнтів, включаючи вимоги щодо бенефіціарного права власності, звіти про підозрілі операції та внутрішні засоби контролю мають надаватися компетентними органами/органами саморегулювання державам-членам.

- Держави-члени повинні запровадити деякі механізми для забезпечення того, що створення структур здійснюватимуться під наглядом професіонала (зобов'язаного суб'єкта), який повинен здійснювати їх належну перевірку.

- Держави-члени повинні запровадити механізми, щоб забезпечити регулярну перевірку інформації, яка зберігається у центральному реєстрі бенефіціарних прав власності.

- Держави-члени мають забезпечити, що консультанти з питань структури капіталу та галузевої стратегії, консультанти та провайдери послуг з питань злиття і поглинання та консультанти з питань бізнес-стратегій виконуватимуть свої зобов'язання щодо бенефіціарного права власності.

В/ якщо припинення пов'язане з придбанням іншого юридичного суб'єкта або юридичного утворення

Для компетентних органів/органів саморегулювання:

- Компетентні органи/органи саморегулювання повинні забезпечити проведення навчальних сесій та надання настанов щодо факторів ризику, акцентуючи увагу на непрямих ділових відносинах, офшорних професійних посередниках, клієнтах чи юрисдикціях, а також на складних структурах/структурах-оболонках.

- Органи саморегулювання/компетентні органи повинні здійснювати тематичні перевірки того, наскільки виконуються вимоги щодо ідентифікації бенефіціарних власників.

- Щорічні звіти про заходи, вжиті для перевірки дотримання цими зобов'язаними суб'єктами своїх зобов'язань щодо належної перевірки клієнтів, включаючи вимоги щодо бенефіціарного права власності, звіти про підозрілі операції та внутрішні засоби контролю.

- Держави-члени повинні запровадити механізми, щоб забезпечити регулярну перевірку інформації, яка зберігається у центральному реєстрі бенефіціарних прав власності.

Держави-члени мають забезпечити, що консультанти з питань структури капіталу та галузевої стратегії, консультанти та провайдери послуг з питань злиття і поглинання та консультанти з питань бізнес-стратегій належним чином регулюватимуться та контролюватимуться на національному рівні та виконуватимуть свої зобов'язання щодо бенефіціарного права власності.

4. Товари високої вартості – артефакти і антикваріат

Продукт
Товари високої вартості – артефакти і антикваріат

Сектор
Торговці товарами високої вартості

Опис сценарію ризиків

Фінансування тероризму – Злочинці отримують прибуток від продажу вкрадених артефактів і антикваріату. Торгівля культурними товарами є однією з найбільших категорій злочинної торгівлі, яка, можливо, є третьою або четвертою найбільшою категорією. Однак навряд чи існують інструменти для оцінки законної торгівлі чи будь-які дані про масштаби незаконної торгівлі (особливістю цієї незаконної торгівлі є те, що законна та незаконна торгівля іноді перетинаються).

Навряд чи є дані або інструменти для оцінки незаконної комерційної діяльності. Тим не менш, за даними Інтерполу, чорний ринок творів мистецтва стає таким же привабливим, як і продаж наркотиків, зброї та підроблених товарів.

В інформаційному досьє, яке ЮНЕСКО підготувало до 40-ї річниці Конвенції 1970 року, зазначається, що разом із торгівлею наркотиками та зброєю, чорний ринок антикваріату та культурних цінностей є однією з найбільш міцно вкорінених незаконних сфер торгівлі у світі[73].

Обсяги незаконної торгівлі антикваріатом також важко оцінити[74] з огляду на його невидимий та безперешкодний характер.[75] За оцінками, лише 30-40 % антикварних угод укладаються в

[73] ЮНЕСКО. Боротьба з незаконною торгівлею культурними цінностями: Конвенція 1970 року: Минуле та майбутнє. 15 та 16 березня 2011 року. .http://unesdoc.unesco.org/images/0019/001916/191606E.pdf
[74]Алеся Куш «Боротьба з незаконною торгівлею антикваріатом в ЄС: Заповнення законодавчих прогалин» (Fight against the Illegal Antiquities' Traffic in the EU: Bridging the Legislative Gaps), Брюгес, Коледж Європи 2011; Харді «Незаконна торгівля, дослідження та належна перевірка: сучасний стан справ» (Illicit trafficking, provenance research and due diligence). Наукове дослідження, 30 березня 2016 року.
[75] Дункан Чаппелл і Кеннет Полк, «Розгадка Кордети: Як організована міжнародна торгівля культурними цінностями?» (Unravelling the Cordata: Just How Organised Is the International Traffic in Cultural Objects?), Стефано Манакорда і Дункан Чаппелл (під ред.), *«Злочин у секторі мистецтва і антикваріату. Незаконна торгівля культурними цінностями» (Crime in the Art and Antiquities' World. Illegal Trafficking in Cultural Property).*

аукціонних будинках, де товари розміщуються в каталогах.[76] Решта угод укладається шляхом приватних (часто неконтрольованих і незареєстрованих) операцій.[77]

Згідно з дослідженнями, загальна фінансова вартість незаконної торгівлі антикваріатом і предметами мистецтва є більшою за будь-яку іншу сферу міжнародної злочинності, крім торгівлі зброєю і наркотиками[78], і оцінюється у розмірі 3-6 млрд доларів США на рік.[79]

Широко повідомлялося про зв'язки між торгівлею антикваріатом і торгівлею наркотиками, дикими тваринами та зброєю, відмиванням грошей і ухиленням від сплати податків та фінансуванням військових машин і терористичних організацій, що ставить торгівлю антикваріатом на рівень серйозної транснаціональної організованої злочинності.

Відмивання коштів — Злочинці конвертують надходження від злочинної діяльності на антикваріат та предмети мистецтва, щоб легше зберігати або переміщувати ці активи.

Загроза

Фінансування тероризму

Оцінка загрози фінансування тероризму, пов'язаної з торгівлею краденими артефактами і антикваріатом, вказує на те, що правоохоронні органи виявили випадки торгівлі антикваріатом на території ЄС. Правоохоронними органами держав-членів було проведено декілька розслідувань, в яких торгівля товарами, вивезеними із зон конфлікту[80] за участі країн Далекого Сходу, використовувалася для приховування походження товарів. Безумовно, необхідно брати до уваги частку нелегального ринку, але її дуже важко виявити. Відповідно до національних досліджень, проведених до цього часу, основна загроза пов'язана з крадіжкою такої продукції у третіх країнах, особливо у зонах конфлікту, таких як Сирія, терористичними організаціями, що контролюють територію, і накладенням податків на таку діяльність. Наприклад, «замість торгівлі артефактами, Ісламська держава заробляє гроші на продажі дозволів на копальні роботи та стягуванні транзитних зборів».[81] Однак терористи можуть також продавати продукцію самостійно, щоб отримати дохід, що доведено первинними доказами, зібраними США[82] та визнано Радою Безпеки ООН.[83]

---

[76] Пітер Уотсон, «Сотбі: Історія зсередини» (Sotheby's: The Inside Story), Random House, 1997, цит. у Шонсі Д. Стіл.

[77] Алеся Куш, там же, с. 4.

[78] Ліза Дж. Бородкін, «Економіка розкрадання антикваріату та запропонована юридична альтернатива» (The Economics of Antiquities looting and a Proposed Legal Alternative), *Columbia Law Review*, № 2, 1995, с. 377-418.

[79] *Там же*, с. 377. Оцінка автора.

[80] https://blogs.state.gov/stories/2018/06/20/en/tackling-illicit-trafficking-antiquities-and-its-ties-terrorist-financing

[81] «Халіфат у занепаді: Оцінка фінансових статків Ісламської держави» (Caliphate in Decline: An Estimate of Islamic State's Financial Fortunes), ICSR, 2017.

[82] https://www.justice.gov/usao-dc/pr/united-states-files-complaint-seeking-forfeiture-antiquities-associated-islamic-state

[83] Постанова РБ ООН 2347 (2017) визнає (подібно до Р 2199, прийнятої відповідно до обов'язкової до виконання Глави VII), що Ісламська держава та групи, пов'язані з Аль-Каїдою, «отримують прибуток від прямої або опосередкованої участі у розкраданні та контрабанді культурної спадщини», використовуючи її для фінансування *«наймання та зміцнення їхніх операційної здатності організовувати і здійснювати теракти»*.

Більшість предметів, викрадених терористами у деяких зонах конфлікту, є предметами невеликого/середнього розміру, які є результатом незаконних розкопок, що ще більше ускладнює встановлення правоохоронними органами походження та доведення того, що сертифікат є підробленим, особливо для невеликих предметів.

Оскільки продукція може продаватися в ЄС посередниками, існує непрямий, хоча й конкретний ризик фінансування тероризму.

З точки зору наміру та здатності, цей сценарій ризику є фінансово вигідним, враховуючи той факт, що розкрадання артефактів може принести значну суму доходу. Однак це непростий метод. Він вимагає (у країнах-джерелах): доступу до нелегальної/темної економіки (предмети, які потім часто відмиваються та змішуються з легальними ланцюгами у країнах призначення); технічних знань; та знань ринку предметів мистецтва, на що не здатні всі терористичні групи. Більше того, транспортування таких товарів не є достатньо безпечним або дискретним, і їх включення у справу вимагає часу та планування, що не відповідає потребі терористичних груп у швидкому отриманні готівки.

Міжнародний вимір цієї загрози не може бути виключений з аналізу загрози. Правоохоронні органи та ООН надали докази того, що у зонах конфлікту мають місце розкрадання і торгівля артефактами. Така діяльність приносить фінансові доходи, які можуть бути використані шляхом повернення іноземних бойовиків-терористів для здійснення терористичних актів на території ЄС. Також є дані про ідентифікацію деяких радикалізованих особи на території ЄС, які володіють неідентифікованими артефактами.

Висновок: На цьому етапі дуже мало доказів того, що торгівля вкраденими артефактами і антикваріатом може використовуватися для фінансування терористичної діяльності на території ЄС. Однак це привабливе джерело доходу для організацій, які контролюють територію у зонах конфлікту, що мають намір фінансувати терористичну діяльність в ЄС. Тим не менш, необхідний рівень знань, досвіду та здатності планувати знижує рівень загрози. Тому рівень загрози фінансування тероризму, пов'язаної з торгівлею артефактами і антикваріатом, вважається <u>помірно значним</u> (хоча і підвищеним з огляду на ситуацію на Близькому Сході та у Північній Африці і з огляду на те, що зникнення територіального «Халіфату», яким було інституалізовано розкрадання, не поклало кінець поодиноким випадкам розкрадання) (рівень 2).

Відмивання коштів

Оцінка загрози відмивання коштів, пов'язаної з торгівлею вкраденими артефактами і антикваріатом, вказує на те, що цей сценарій ризику може бути цікавим для організованих злочинних груп, оскільки ці «продукти» можуть бути конвертовані у готівку для відмивання доходів, одержаних злочинним шляхом, або для ухилення від сплати податків. Правоохоронні органи вважають, що подібна торгівля має місце здебільшого у зонах вільних портів і це ускладнює оцінку масштабів цього явища. Є дані, що цей метод використовуються організованими злочинними групами (щоб продати товар за найкращою ціною, потрібні досвід та знання). Нелегальна економіка також відіграє роль у цьому сценарії ризиків, але її важко оцінити. Деякі злочинні мережі намагаються продавати підроблені товари у вигляді вкраденого антикваріату і забезпечують шахрайське походження предметам.

Висновки: Цей сценарій ризику може бути привабливим інструментом для організованих злочинних груп для конвертації доходів, одержаних злочинним шляхом, у чисті готівкові кошти. Однак це вимагає високого рівня знань і не є безпечною діяльністю для них. Тому рівень загрози відмивання коштів, пов'язаної з незаконною торгівлею артефактами і антикваріатом, вважається <u>помірно значним</u> (рівень 2).

Вразливість

Фінансування тероризму

Оцінка вразливості до фінансування тероризму, пов'язаної з незаконною торгівлею вкраденими артефактами і антикваріатом, вказує на те, що цей ризик є новим, але він може зрости у короткостроковій перспективі. Вкрадені товари можуть бути репатрійовані до ЄС. Наприклад, деякі невеликі вкрадені артефакти/монети можуть продаватися місцевими радикалізованими особами, які повертаються до ЄС, у кількостях, що є надто малими, аби їх можна було виявити або навіть переслідувати.

a) схильність до ризику

За даними розслідувань, антикваріат пропонується колекціонерам ЄС з різних країн, які не є членами ЄС, як правило, на інтернет-аукціонах або у спеціалізованих інтернет-магазинах. Терористичні організації можуть застосовувати заходи приховування, такі як підробка IP-адрес, що ускладнює ідентифікацію та визначення фактичного місцезнаходження продавця. Також дедалі частіше використовуються соціальні мережі для уникнення звернення до послуг посередників та безпосереднього продажу артефактів покупцям.

Перевага надається готівковим операціям (іноді на крупні грошові суми), але операції у режимі онлайн також є популярними, оскільки фінансова установа не може ідентифікувати реального власника/покупця антикваріату. Спеціальний моніторинг операцій відсутній.

b) обізнаність про ризики

За даними правоохоронних органів, культурні артефакти або не надходять на територію ЄС, або залишаються невиявленими. Це свідчить про те, що обізнаність компетентних органів та підрозділів фінансової розвідки у цьому питанні є дуже низькою. Зобов'язані суб'єкти не ведуть документацію (наприклад, про походження артефактів або кому вони продаються), будь-яка звітність відсутня. Митні органи мають труднощі з виявленням незаконного походження культурних артефактів.

c) законодавча база і засоби контролю

Законодавча база щодо ПВК: згідно з чинною законодавчою базою ЄС щодо протидії відмиванню коштів, до фізичних осіб, які торгують товарами, застосовуються відповідні вимоги ЄС, якщо вони отримують готівкові виплати у розмірі понад 10 000 євро. Такі вимоги застосовуються у разі готівкових платежів, але не враховують ризиків від інших видів платіжних операцій.

Чинна законодавча база ЄС щодо протидії відмиванню коштів (Четверта директива про боротьбу з відмиванням грошей, із змінами, внесеними П'ятою директивою про боротьбу з відмиванням грошей) наразі спрямована на осіб, які торгують предметами мистецтва, і розглядає їх як зобов'язаних суб'єктів, коли вони торгують або діють в якості посередників у торгівлі предметами мистецтва. Сюди відносяться люди, які займаються зберіганням, торгівлею або виступають в якості посередників у торгівлі предметами мистецтва, якщо така торгівля здійснюється через порти вільної торгівлі.

Спеціальні торговельні заборон ЄС: ЄС ухвалив спеціальні положення щодо імпорту культурних цінностей на свою митну територію з Сирії та Іраку. Регламент Ради (ЄС) № 1210/2003 від 7 липня 2003 року щодо спеціальних обмежень для економічних та фінансових відносин з Іраком та Регламент Ради (ЄС) № 36/2012 щодо обмежувальних положень з огляду на ситуацію в Сирії забороняють торгівлю культурними цінностями з цими країнами, якщо є обґрунтовані підстави підозрювати, що товари були вивезені без згоди їх законного власника або були вивезені з порушенням положень національного чи міжнародного права. Однак у компетентних органів все ще виникають труднощі з відстеженням будь-яких товарів, що походять з цих країн, і застосування таких положень іноді може бути складним з огляду на характер продукції (наприклад, предмет, який не є незаконним як такий, але справжнє походження якого складно встановити). Цікавим є те, що у державах-членах, яким вдалося конфіскувати культурні цінності, що походять з Іраку чи Сирії, цей захід є частиною щоденної роботи тих самих установ, які контролюють загальний імпорт культурних цінностей, і виконання відповідних норм не накладає на них жодного додаткового тягаря.

У будь-якому разі, незважаючи на існування певних норм ЄС, вони обмежуються конкретними регіонами і не охоплюють усіх випадків імпорту культурних цінностей. Це призводить до недостатності перевірок для подолання ризиків.

Висновки: Незважаючи на недостатність доказів того, що такі методи використовуються в ЄС, складається враження, що схильність до ризику тільки-но з'являється, але може зрости з огляду на геополітичний контекст. Законодавча база не дозволяє ефективно контролювати такі операції через те, що зобов'язані суб'єкти не усвідомлюють таку вразливість до фінансування тероризму (відсутність звітності, відсутність ведення обліку). Тому рівень вразливості до відмивання коштів, пов'язаної з купівлею артефактів і антикваріату, вважається значним/дуже значним (рівень 3/4).

Відмивання коштів

Оцінка вразливості до відмивання коштів, пов'язаної з незаконною торгівлею вкраденими артефактами і антикваріатом, свідчить про таке:

a) схильність до ризику

З огляду на свою чутливу природу, ринок артефактів і антикваріату зазвичай надає перевагу використанню неформальних каналів, де відсутні спеціальні заходи безпеки або моніторинг операцій. Він передбачає використання готівкових платежів (іноді на крупні грошові суми), коли ідентифікувати покупця майже неможливо.

b) обізнаність про ризики

Складається враження, що сектор є більш обізнаним про ризик відмивання коштів, ніж про ризик фінансування тероризму. У кількох державах-членах торговці товарами високої вартості проходять відповідне навчання і одержують настанови. Однак рівень звітування про підозрілі операції є дуже низьким, що викликає сумніви стосовно належного розуміння переліку.

c) законодавча база і засоби контролю

Фізичні особи, які торгують товарами, підпадають під вимоги ЄС щодо протидії відмиванню коштів, якщо вони отримують готівкові виплати у розмірі понад 10 000 євро. Чинна законодавча база ЄС щодо протидії відмиванню коштів також розглядає людей, які торгують предметами мистецтва, як зобов'язаних суб'єктів. Крім того, у багатьох державах-членах ухвалено норми, спрямовані на обмеження готівкових виплат. Однак, як і у випадку фінансування тероризму, здійснювані перевірки є недостатніми для усунення ризиків, що можуть створювати вкрадені товари.

Крім того, члени Великої сімки вважають, що незаконна торгівля артефактами представляє високий ризик і що ця сфера потребує подальших досліджень.

Висновки: Незважаючи на те, що рівень обізнаності щодо ризиків є вищим, ніж для фінансування тероризму, інші елементи оцінки мають спільні риси. Вони включають низький рівень звітування та відсутність доказів того, що обмеження на готівкові виплати зменшують ризики. Тому рівень вразливості до відмивання коштів, пов'язаної з придбанням артефактів і антикваріату, вважається <u>значним/дуже значним</u> (рівень 3/4).

Пом'якшувальні заходи:

1) <u>Для Комісії:</u>

- 13 липня 2017 року Європейська Комісія внесла пропозицію щодо регламенту стосовно імпорту культурних цінностей[84] для встановлення умов та порядку ввезення культурних цінностей на митну територію ЄС. Комісія також проводить дослідження на тему «Покращення знань про незаконну торгівлю культурними цінностями в ЄС та нові технології, доступні для боротьби з нею».[85]

- Комісія також прийняла пропозицію[86] щодо швидкого посилення законодавчої бази ЄС стосовно запобігання фінансуванню тероризму шляхом підвищення прозорості готівкових виплат. Це буде здійснено шляхом встановлення обмеження на готівкові платежі або будь-яким іншим відповідним способом. Обмежуючи можливості використання готівкових коштів, пропозиція допоможе запобігти фінансуванню тероризму, оскільки потреба у використанні неанонімних платіжних засобів може стримувати діяльність або сприяти її легшому виявленню та розслідуванню. Будь-яка така пропозиція також має на меті гармонізувати обмеження на всій території ЄС, щоб створити рівні умови для підприємств та усунути порушення конкуренції на внутрішньому ринку. Це також допоможе у боротьбі з відмиванням коштів, шахрайством та організованою злочинністю.

- Держави-члени повинні повідомляти про заходи, які вживають торговці товарами для дотримання своїх зобов'язань щодо ПВК/ФТ. Це дозволить Комісії додатково оцінити ризики, що створюють провайдери послуг, які приймають готівкові платежі. Комісія також має оцінити вигоди від застосування положень щодо ПВК/ФТ до інших секторів.

[84] Регламент (ЄС) 2019/880 Європейського Парламенту та Ради від 17 квітня 2019 року щодо запровадження та імпорту культурних цінностей; PE/82/2018/REV/1; OB L 151, 07.06.2019, с. 1-14.
[85] Публікація цього дослідження спочатку була запланована на 2018/2019 роки.
[86] Регламент (ЄС) 2018/1672 Європейського Парламенту та Ради від 23 жовтня 2018 року про контроль ввезення в ЄС та вивезення з ЄС готівкових коштів і про скасування Регламенту (ЄС) № 1889/2005, OB L 284, 12.11.2018, с. 6-2.

- Має бути вирішено питання тягаря доведення та приватних продажів.

2) Для держав-членів:

- Держави-члени повинні належним чином враховувати ризики, які створюють готівкові виплати, у своїх національних оцінках ризиків та визначити відповідні пом'якшувальні заходи. Держави-члени повинні розглянути можливість застосування до таких секторів, які є особливо схильними до ризиків відмивання коштів та фінансування тероризму, режиму ПВК/ФТ на основі результатів їх національних оцінок ризиків.

- Держави-члени повинні заохочувати до співпраці між правоохоронними органами та археологами, які є їхніми «очима та вухами» у цій галузі.

- Держави-члени повинні забезпечити навчання працівників правоохоронних органів (митниця та поліція) та забезпечити співпрацю та обмін інформацією між працівниками митниць, прикордонних служб та інших органів.

- Просування ухвалення вимог щодо надання дозволів у країні експорту та/або в ЄС або вимог щодо самостійного декларування, тобто декларування імпортером ЄС про те, що товар залишив країну експорту відповідно до її законів та підзаконних актів.

- Кампанія з підвищення обізнаності та просування заходів на ринку предметів мистецтва та у музеях, таких як належна перевірка, зобов'язання щодо комп'ютеризованої інвентаризації та офіційне визнання ЄС існуючих етичних кодексів чи кодексів поведінки для музеїв та ринку предметів мистецтва.

- Розгляд можливості стати стороною конвенцій Ради Європи UNIDROIT та NICOSIA – або ухвалення деяких положень, передбачених у цих конвенціях.

- Зобов'язання компаній, які займаються торгівлею предметами мистецтва та зберіганням антикваріату (відомі як «порти вільної торгівлі»), звітувати про всі підозрілі операції, а також застосування до власників компаній, що займаються торгівлею та зберіганням предметів мистецтва та антикваріату, які причетні до незаконної торгівлі такими предметами, ефективних, відповідних та запобіжних санкцій, включаючи кримінальні покарання, за необхідності.

3) Для зобов'язаних суб'єктів

- Сприяння використанню письмових угод для отримання дуже докладного рахунка-фактури з чітким описом товару (наприклад, вартість, опис продукту і картинка високої якості), що також дозволить ідентифікувати реального бенефіціара операції.

- Заохочування до припинення практики приватних операцій готівкою для анонімних покупців.

- Пропагування ідеї надійної системи відстеження як для онлайн-торгівлі, так і для фізичної торгівлі, що відповідає всій філософії протидії відмиванню коштів.

5. Активи високої вартості – Дорогоцінні метали і дорогоцінні камені

Продукт
Активи високої вартості – золото і алмази

Сектор
Торговці товарів високої вартості

Загальний опис сектора та відповідного продукту/діяльності

В ЄС ринок алмазів здебільшого обмежується однією країною – Бельгією, і бельгійські торговці алмазами займають переважну частку на європейському ринку алмазів. 1 700 компаній офіційно зареєстровані як торговці алмазами у Федеральній державній службі економіки. Загальний обсяг імпорту та експорту Бельгії лише у 2015 році склав 48 млрд доларів США. Найбільші світові видобувні компанії мають офіс в Антверпені і продають значну частину своїх товарів безпосередньо бельгійським компаніям. У Бельгії є чотири алмазні біржі, які є членами Світової федерації алмазних бірж. За даними 2015 року, опублікованими алмазним офісом в Антверпені[87], 84 % усіх необроблених алмазів і 50 % усіх відшліфованих алмазів на планеті походять з Антверпена.

Спеціалізовані фінансові установи забезпечують ліквідність торгівлі алмазами. Компанії, що торгують алмазами, потребують такого фінансування для придбання великої кількості необроблених алмазів і для фінансування їх перетворення на відшліфовані алмази.

Опис сценарію ризиків

Доходи від злочинної діяльності (наприклад, торгівля наркотиками) переміщуються в іншу країну для придбання золота та ювелірних виробів, які потім продаються в іншій країні за допомогою фальшивих рахунків-фактур та сертифікатів, або безпосередньо використовуються для придбання золота на національній території і продаються брокеру дорогоцінних металів, який потім продає його іншим підприємствам. Після цього доходи від продажу можуть бути передані третій стороні для фінансування нових злочинних операцій. Злочинці надають перевагу дорогоцінним металам, таким як золото та дорогоцінне каміння, таке як алмази, оскільки їх зберігання є не затратним і їх легко перетворити на готівку.

[87] Світовий алмазний центр в Антверпені, https://www.awdc.be/.

Загроза

Фінансування тероризму

Оцінка загрози фінансування тероризму, пов'язаної з придбанням золота та алмазів, вказує на те, що терористи використовують цей метод з огляду на його легкодоступність та фінансову доцільність. Він вимагає помірного рівня планування та знань. Золото зазвичай використовується у зонах війни та є дуже привабливим для терористичних груп.

Висновки: Рівень вразливості до фінансування тероризму, пов'язаної з купівлею золота та алмазів, вважається помірно значним/значним (рівень 2-3).

Відмивання коштів

Оцінка загрози відмивання коштів, пов'язаної з купівлею золота та алмазів, вказує на те, що злочинці розробили схеми відмивання крупних грошових сум за допомогою такого методу. Відповідно до аналізу FATF, це сценарій високого ризику, оскільки золото та алмази легко переміщувати через кордон (наприклад, схованими в автомобілі). Міжнародна торгівля золотом також розглядається як спосіб відмивання доходів, одержаних злочинним шляхом. Справа, що розглядається, стосувалася заявленого імпорту золота з Об'єднаних Арабських Еміратів на територію держави-члена ЄС, перепродажу золота в іншу державу-члена ЄС та його вивезення звідти назад до Об'єднаних Арабських Еміратів. Карусельний характер діяльності та низька якість транспортованого підробленого золота у цій справі дає підстави вважати, що торгівля товарами здійснювалася лише для виправдання злочинних грошових переказів. Цей метод тісно пов'язаний з оцінкою ризику, який створюють кур'єри золота/алмазів (див. спеціальний розділ).

Висновки: Рівень вразливості до відмивання коштів, пов'язаної з купівлею золота та алмазів, вважається дуже значним (рівень 4).

Вразливість

Фінансування тероризму

Рівень вразливості до фінансування тероризму, пов'язаної з придбанням золота та алмазів, свідчить про таке:

a) схильність до ризику

Деякі представники приватного сектора зазначають, що використання готівкових коштів у торгівлі алмазами зменшилось завдяки обмеженням, встановленим деякими національними положеннями щодо протидії відмиванню коштів (у деяких країнах готівкові платежі обмежуються до 10 % від загальної суми операції, максимум 3 000 євро). Однак немає конкретної інформації про торгівлю золотом, коли готівкові виплати все ще періодично використовуються, без можливості ідентифікації сторін, що беруть участь в операціях.

b) обізнаність про ризики

Що стосується ризику фінансування тероризму, він є дуже низьким. Не існує спеціальної законодавчої бази для обмеження транспортування та закупівлі золота і алмазів. З огляду на транскордонний характер таких переміщень, складно або навіть неможливо здійснювати перевірки.

Що стосується торгівлі алмазами, деякі національні організації торговців алмазами розробили організаційну базу для надання настанов, проведення навчальних курсів та надання допомоги із звітами про підозрілі операції, а також допомоги з аналізом ризиків. Ці організації також можуть надавати бази даних «знай свого клієнта», що включають санкційні переліки, інформацію про впливових політичних осіб та/або переліки третіх країн високого ризику. Деякі торговці алмазами забезпечують, що процеси ідентифікації та верифікації здійснюватимуться перед операцією, що передбачає платіж шляхом банківського переказу.

Тим не менш, така практика є досить обмеженою і недостатньо поширеною, аби вважати, що сектор є належним чином обізнаним про ризики.

Що стосується торгівлі золотом, від приватного сектора не було отримано конкретної зворотної інформації, оскільки неможливо було ідентифікувати контактну особу для обговорення заходів протидії відмиванню коштів.

c) законодавча база і засоби контролю

Фізичні особи, які торгують товарами, підпадають під вимоги ЄС щодо протидії відмиванню коштів, якщо вони отримують готівкові виплати у розмірі понад 10 000 євро. Такі вимоги щодо протидії відмиванню коштів також обмежуються готівковими виплатами і не беруть до уваги ризики, пов'язані з операціями з використанням інших способів платежу.

Що стосується торгівлі алмазами, одна з найбільших груп алмазів у Європі підпадає під дію положень щодо ПВК/ФТ. Тому більшість торговців алмазами в ЄС підпорядковуються вимогам щодо реєстрації (після здійснення належних перевірок, зокрема, з точки зору бенефіціарного власника) та перевіркам, які здійснюються їх відповідальними органами, уповноваженими перевіряти не тільки дотримання зобов'язань щодо протидії відмиванню коштів, але і готівкові платежі.

ЄС має Кімберлійські органи[88] у шести країнах, які перевіряють імпортні та експортні поставки необроблених алмазів, особливо на предмет наявності Кімберлійського сертифіката (Бельгія, Сполучене Королівство, Німеччина, Чехія, Румунія та Португалія). Це означає, що необроблені алмази не можуть бути завезені або вивезені з ЄС без Кімберлійського сертифіката та без проходження через один з шести призначених органів Кімберлійського процесу. Ці шість органів Кімберлійського процесу призначаються Європейською Комісією та працюють під її наглядом. Тому транспортування необроблених алмазів завжди підлягає перевіркам під час ввезення та вивезення з ЄС. Оскільки торгівля необробленими алмазами без Кімберлійського сертифіката рівнозначна «незаконній торгівлі», Кімберлійський процес є сильним превентивним заходом проти відмивання грошей.

[88] Кімберлійський процес – це зобов'язання вилучити конфліктні алмази зі світового ланцюга поставок. Сьогодні учасники активно запобігають 99,8 % світової торгівлі. З моменту впровадження Кімберлійського процесу у 2003 році торгівля конфліктними алмазами, яка підлягає ідентифікації, знизилася з 15 % до менш ніж 1 %. https://www.kimberleyprocess.com/en/european-union-0.

Законодавча база ЄС відрізняється для відшліфованих алмазів, оскільки їх можна імпортувати у будь-яку країну ЄС. Що стосується держав-членів, які мають дуже сувору систему контролю за імпортом та експортом алмазів, які імпортуються з країн за межами ЄС або експортуються за межі ЄС, цей механізм контролю можна обійти шляхом імпорту/експорту через іншу країну ЄС.

Однак національні закони наразі не узгоджені ані для алмазів, ані для золота, і це створює ризик виникнення розбіжностей у зобов'язаннях, що накладаються (таких як реєстрація), та здійснюваних перевірках.

Що стосується золота, відсутність узгодженої законодавчої бази також становить проблему для перевірок та їх приведення у виконання.

Кількість звітів про підозрілі операції є досить низькою для цієї категорії зобов'язаних суб'єктів. Операції часто є прямими, що створює певну проблему для захисту працівників.

Висновки: З огляду на вищезазначені елементи, рівень вразливості до фінансування тероризму, пов'язаної з купівлею золота та алмазів, вважається значним (рівень 3).

Відмивання коштів

Рівень уразливості до відмивання коштів, пов'язаної з придбанням золота та алмазів, свідчить про таке:

a) схильність до ризику

Деякі представники приватного сектора зазначають, що використання готівкових коштів у торгівлі алмазами зменшилось завдяки обмеженням, встановленим деякими національними положеннями щодо протидії відмиванню коштів (у деяких країнах готівкові платежі обмежуються до 10 % від загальної суми операції, максимум 3 000 євро). Однак немає конкретної інформації про торгівлю золотом, коли готівкові виплати все ще періодично використовуються, без можливості ідентифікації сторін, що беруть участь в операціях.

b) обізнаність про ризики

Що стосується ризику відмивання коштів, він є дуже низьким. Не існує спеціальної законодавчої бази для обмеження транспортування та закупівлі золота і алмазів. З огляду на транскордонний характер таких переміщень, складно або навіть неможливо здійснювати перевірки.

Що стосується торгівлі алмазами, деякі національні організації торговців алмазами розробили організаційну базу для надання настанов, проведення навчальних курсів та надання допомоги із звітами про підозрілі операції, а також допомоги з аналізом ризиків. Ці організації також можуть надавати бази даних «знай свого клієнта», що включають санкційні переліки, інформацію про впливових політичних осіб та/або переліки третіх країн високого ризику. Деякі торговці алмазами забезпечують, що процеси ідентифікації та верифікації здійснюватимуться перед операцією, що передбачає платіж шляхом банківського переказу.

Тим не менш, така практика є досить обмеженою і недостатньо поширеною, аби вважати, що сектор є належним чином обізнаним про ризики. Сектори алмазів та золота складаються здебільшого з невеликих компаній (найчастіше компаній з одним учасником), де відповідальна особа не має юридичних знань, і їй вірогідно буде складно застосувати законодавство щодо протидії відмиванню коштів на практиці та здійснювати процедури належної перевірки клієнтів.

Що стосується торгівлі золотом, від приватного сектора не було отримано конкретної зворотної інформації, оскільки неможливо було ідентифікувати контактну особу для обговорення заходів протидії відмиванню коштів.

c) законодавча база і засоби контролю

Фізичні особи, які торгують товарами, підпадають під вимоги ЄС щодо протидії відмиванню коштів, якщо вони отримують готівкові виплати у розмірі понад 10 000 євро. Такі вимоги щодо протидії відмиванню коштів також обмежуються готівковими виплатами і не беруть до уваги ризики, пов'язані з операціями з використанням інших способів платежу.

Що стосується торгівлі алмазами, одна з найбільших груп алмазів у Європі підпадає під дію положень щодо ПВК/ФТ. Тому більшість торговців алмазами в ЄС підпорядковуються вимогам щодо реєстрації (після здійснення належних перевірок, зокрема, з точки зору бенефіціарного власника) та перевіркам, які здійснюються їх відповідальними органами, уповноваженими перевіряти не тільки дотримання зобов'язань щодо протидії відмиванню коштів, але і готівкові платежі.

ЄС має Кімберлійські органи у шести країнах, які перевіряють імпортні та експортні поставки необроблених алмазів, особливо на предмет наявності Кімберлійського сертифіката (Бельгія, Сполучене Королівство, Німеччина, Чехія, Румунія та Португалія). Це означає, що необроблені алмази не можуть бути завезені або вивезені з ЄС без Кімберлійського сертифіката та без проходження через один з шести призначених органів Кімберлійського процесу. Ці шість органів Кімберлійського процесу призначаються Європейською Комісією та працюють під її наглядом. Тому транспортування необроблених алмазів завжди підлягає перевіркам під час ввезення та вивезення з ЄС. Оскільки торгівля необробленими алмазами без Кімберлійського сертифіката рівнозначна «незаконній торгівлі», Кімберлійський процес є сильним превентивним заходом проти відмивання грошей.

Законодавча база ЄС відрізняється для відшліфованих алмазів, оскільки їх можна імпортувати у будь-яку країну ЄС. Що стосується держав-членів, які мають дуже сувору систему контролю за імпортом та експортом алмазів, які імпортуються з країн за межами ЄС або експортуються за межі ЄС, цей механізм контролю можна обійти шляхом імпорту/експорту через іншу країну ЄС.

Однак національні закони наразі не узгоджені ані для алмазів, ані для золота, і це створює ризик виникнення розбіжностей у зобов'язаннях, що накладаються (таких як реєстрація), та здійснюваних перевірках.

Що стосується золота, відсутність узгодженої законодавчої бази також становить проблему для перевірок та їх приведення у виконання.

Кількість звітів про підозрілі операції є досить низькою для цієї категорії зобов'язаних суб'єктів. Операції часто є прямими, що створює певну проблему для захисту працівників.

Висновки: Незважаючи на те, що в деяких державах-членах чинні нормативно-правові положення підвищують рівень обізнаності щодо ризиків, сектор все ще недостатньо організований для здійснення ефективного моніторингу та управління. Тому рівень вразливості до відмивання коштів, пов'язаної з купівлею золота та алмазів, вважається значним (рівень 3).

Пом'якшувальні заходи:

1) Для держав-членів:

- Держави-члени повинні належним чином враховувати ризики, які створюють готівкові платежі, у своїх національних оцінках ризиків та визначити відповідні пом'якшувальні заходи. Держави-члени повинні розглянути можливість застосування до таких секторів, які є особливо схильними до ризиків відмивання коштів та фінансування тероризму, режим ПВК/ФТ на основі результатів їх національних оцінок ризиків.

- Держави-члени повинні гарантувати, що компетентні органи проводитимуть достатні неоголошені перевірки в алмазних компаніях та приміщеннях торговців золотом, щоб виявити можливі лазівки у відповідності до вимог належної перевірки клієнтів, та залучати фахівців по алмазам для перевірки потоків товарів.

2) Для зобов'язаних суб'єктів:

- Навчання щодо належної перевірки клієнтів, особливо для малого бізнесу. Цю роль може виконувати галузева федерація або алмазна біржа у випадку з алмазними торговцями. Навчання може стосуватися основних вимог щодо ПВК/ФТ, наприклад, як ідентифікувати клієнтів, як здійснити аналіз ризиків, хто є кінцевими бенефіціарними власниками, що таке підрозділ фінансової розвідки та як звітувати йому тощо.

- Заохочення до використання письмових угод для отримання дуже детального рахунка-фактури з чітким описом товару (наприклад, вартість, вага, якість).

3) Для Комісії:

- Відповідно до нового Регламенту про контроль готівкових коштів, визначення готівкових коштів було розширено до охоплення не лише банкнот, але й інших інструментів або високоліквідних товарів, таких як чеки, дорожні чеки, передплачені картки та золото.

- Можуть здійснюватися додаткові дослідження для поглиблення аналізу тих економічних секторів/ситуацій, які більше схильні до ризиків ПВК/ФТ.

Подальша типологічна робота може бути виконана для ідентифікації економічних секторів, які є особливо вразливими до ризиків відмивання коштів та фінансування тероризму, перш ніж визначити спеціально розроблені пом'якшувальні заходи. Цей аналіз також може відображати практику держав-членів, оскільки багато з них вирішили застосовувати до відповідних професій режим ПВК/ФТ з огляду на їх аналізу ризиків.

6. Активи високої вартості – інші активи, відмінні від дорогоцінних металів та дорогоцінних каменів

Продукт

Активи високої вартості – інші активи, відмінні від дорогоцінних металів та дорогоцінних каменів

Сектор

Торговці товарами високої вартості

Опис сценарію ризиків

Злочинці використовують товари високої вартості як простий спосіб інтегрувати кошти в правову економіку, перетворюючи злочинні грошові кошти в інший клас активів, який зберігає свою цінність і навіть може забезпечувати зростання капіталу. Деякі продукти, такі як автомобілі, а також ювелірні вироби, годинники, дорогі судна є особливо привабливими як товари для життя та як економічні активи.

Загроза

Фінансування тероризму

Оцінка загрози фінансування тероризму, пов'язаної з придбанням інших видів товарів високої вартості (крім золота, алмазів, артефактів і антикваріату), не вважається доцільною, з точки зору фінансування тероризму. Тому загроза фінансування тероризму не є частиною оцінки.

Висновки: не застосовується

Відмивання коштів

Оцінка загрози відмивання коштів, пов'язаної з придбанням інших видів товарів високої вартості (крім золота, алмазів, артефактів і антикваріату), свідчить про те, що організації періодично використовують цей метод, який є легкодоступним та не вимагає спеціальних знань (сюди відноситься торгівля ювелірними виробами, автомобілями, суднами та годинниками).

Отриману злочинним шляхом готівку часто конвертують у товари, які користуються великим попитом на іноземних ринках. Одними з найпоширеніших товарів, що купуються та експортуються, є автомобілі та інші транспортні засоби. Основними ринками є Північна Африка та Близький Схід. Машинне обладнання експортується в Ірак і Кувейт; дорогі годинники, золото та ювелірні вироби експортуються до країн Близького Сходу та Північної Африки; а продукти харчування – до Африки.

У деяких юрисдикціях ЄС відсутність обмежень на готівкові платежі робить їх більш привабливими для відмивання коштів на основі торговельної діяльності з використанням готівки. В інших юрисдикціях – навіть у країнах з обмеженнями та зобов'язаннями щодо звітування – рівні звітування є дуже низькими. Торговцями товарами високої вартості є ті, для кого встановлено найменші вимоги щодо звітування. У деяких випадках клієнти-злочинці приносять торговцю підприємство, що коштує мільйони, що становить ще одну перешкоду для звітування.

Було встановлено, що китайські організовані злочинні групи використовують предмети розкоші (дорогий модний одяг) та популярні європейські бренди високого статусу на китайському ринку. Незаконна готівка постачається китайським громадянам, які використовують її для придбання предметів розкоші. Такі предмети розкоші переважно продаються у мережі Інтернет в Китаї, а виручка використовується для здійснення розрахунків у Китаї. Незаконна діяльність китайських організованих злочинних груп в Європі є основним джерелом злочинних доходів, які використовуються для придбання таких предметів розкоші. Така незаконна діяльність включає податкове та митне шахрайство з китайськими вантажами, підробку товарів, торгівлю наркотиками, експлуатацію робочої сили та сексуальну експлуатацію.

Згідно з висновками правоохоронних органів, до 2015–2016 років громадяни Китаю, які проживають в ЄС, використовувались в якості грошових мулів. Вони відкривали банківські рахунки, здійснювали готівкові депозити та переказували гроші в Китай. Ще одним методом було використання китайських туристів, які приїжджають в ЄС, для переказу готівки після їх повернення до Китаю. З часом і завдяки втручанню правоохоронних органів китайські злочинні угруповання перейшли на інші методи, такі як використання покупців для придбання предметів розкоші. Після придбання в Європі ці товари перевозяться до Китаю, де вони продаються з метою отримання прибутку, а отримані надходження передаються у межах Китаю між покупцями товарів та кримінальними структурами. Цей метод дозволяє злочинцям здійснювати повний цикл відмивання коштів до того моменту, коли вони можуть вільно використовувати виручку в Китаї, наприклад, для оплати нових партій китайських вантажів. У разі імпорту в Європу, такі товари будуть недооцінюватися та продаватися без документації. Отримані готівкові кошти знову будуть відмиті та вивезені з Європи до Китаю, що створює кримінальний цикл, який обходить втручання як правоохоронних органів, так і податкових органів.

Висновки: Рівень вразливості до відмивання коштів, пов’язаної з купівлею інших типів товарів високої вартості, вважається <u>дуже значним</u> (рівень 4).

Вразливість

Фінансування тероризму

Оцінка вразливості до фінансування тероризму, пов’язаної з придбанням інших типів товарів високої вартості (крім золота, алмазів, артефактів і антикваріату), не вважалася доцільною з точки зору фінансування тероризму. Тому вразливість до фінансування тероризму не є частиною цієї оцінки.

Висновки: Не застосовується

Відмивання коштів

Оцінка вразливості до відмивання коштів, пов'язаної з придбанням інших типів товарів високої вартості (крім золота, алмазів, артефактів і антикваріату), вказує на те, що цей сценарій ризиків має ті самі вразливості, що і у разі придбання золота/алмазів.

a) схильність до ризику

Важко визначити інші типи товарів, які можуть використовуватися для відмивання коштів. Однак торгівля товарами високої вартості, крім золота та алмазів, може передбачати готівкові операції з низьким рівнем заходів безпеки та моніторингу у каналах доставки. Вона може передбачати транскордонні операції, які важко контролювати.

b) обізнаність про ризики

Що стосується ризику відмивання коштів, він є дуже низьким. Сектор є реально широким, і немає жодної організаційної бази, яка могла би забезпечити надання настанов або навчання. Заходи щодо належної перевірки клієнтів не застосовуються, і рівень звітування про підозрілі операції вказує на те, що розуміння ризиків є дійсно низьким.

c) законодавча база і засоби контролю:

Фізичні особи, які торгують товарами, підпадають під вимоги ЄС щодо протидії відмиванню коштів, якщо вони отримують готівкові виплати у розмірі понад 10 000 євро. Однак це визначення є досить загальним і не вказує, які категорії товарів, що продаються, підпадають під сферу дії Директиви про боротьбу з відмиванням грошей. Крім того, ці вимоги щодо протидії відмиванню коштів обмежуються готівковими платежами та не беруть до уваги ризики, пов'язані з операціями з використанням інших способів платежу. Тим не менш, деякі держави-члени запровадили обмеження щодо готівкових платежів.

Однак не існує гармонізованого національного законодавства для усунення ризиків торгівлі товарами високої вартості. Складається враження, що рівень обліку є дуже низьким і перевірки відсутні.

Висновки: Незважаючи на те, що в деяких державах-членах нормативно-правові акти підвищують рівень обізнаності щодо ризиків, сектор все ще недостатньо організований, аби забезпечувати ефективний моніторинг та надавати настанови. Рівень вразливості до відмивання коштів, пов'язаної з купівлею інших типів товарів високої вартості, вважається <u>значним</u> (рівень 3).

Пом'якшувальні заходи:

1) Для Комісії:

Комісія вивчила потенційний вплив обмежень на готівкові платежі та опублікувала звіт з цього приводу.[89] У звіті робиться висновок, що на цьому етапі Комісія не повинна розглядати жодну законодавчу ініціативу з цього питання. Обмеження щодо готівкових платежів є чутливим питанням для громадян ЄС, багато з яких розглядають можливість готівкових платежів як основну свободу, яка не має бути обмежена.

- Держави-члени повинні повідомляти про заходи, які вживають торговці товарами, охопленими Директивою про боротьбу з відмиванням грошей, з метою дотримання своїх зобов'язань щодо ПВК/ФТ. З огляду на це, Комісія може додатково оцінити ризики, зумовлені провайдерами послуг, які приймають готівкові платежі. Комісія також має оцінити вигоди застосування до відповідних секторів положень щодо ПВК/ФТ.

2) Для держав-членів:

Держави-члени повинні належним чином враховувати ризики, які створюють готівкові платежі, у своїх національних оцінках ризиків та визначити відповідні пом'якшувальні заходи. Держави-члени повинні розглянути можливість застосування до секторів, які є особливо схильними до ризиків відмивання коштів та фінансування тероризму, режиму ПВК/ФТ на основі результатів їх національних оцінок ризиків.

[89] Звіт Комісії до Європейського Парламенту і Ради щодо обмежень на готівкові платежі – COM(2018) 483 final: https://ec.europa.eu/info/sites/info/files/economyfinance/com_2018_483_f1_report_from_commission_en_v4_p1_981536.pdf.

7. Кур’єри дорогоцінних металів і дорогоцінних каменів

Продукт
Золото та інші дорогоцінні метали

Сектор
/

Опис сценарію ризиків

Це передбачає транскордонне переміщення золота та інших дорогоцінних металів, а також дорогоцінного каміння. Злочинці, які одержали готівкові кошти від своєї незаконної діяльності, прагнуть конвертувати їх у золото та інші дорогоцінні метали чи каміння, щоб вони могли репатріювати кошти або перемістити такі товари у місце, де їх можна легше інтегрувати у правову економіку.

Кур’єри можуть використовувати повітряний, морський або залізничний транспорт для перетину міжнародної кордону, наприклад:
- контейнеризовані або інші форми вантажу, схованого у поштових відправленнях або бандеролях – якщо злочинці бажають перемістити дуже великі кількості золота та інших дорогоцінних металів, часто їх єдиним варіантом є приховування їх у вантажі, що може бути контейнеризованим або інакше транспортуватися через кордон; або
- складні приховування золота у товарах, що надсилаються звичайними поштовими відправленнями або бандеролями.

Загроза

Фінансування тероризму

Оцінка загрози фінансування тероризму, пов'язаної із золотом та іншими дорогоцінними металами, виявила лише декілька показників того, що терористичні групи використовують або мають намір використовувати цей канал для фінансування терористичної діяльності.

Кур'єри золота або алмазів не є найбільш привабливим і безпечним варіантом для терористичних груп, хоча ці активи часто використовуються у зонах військових дій, оскільки ними легко торгувати. Було виявлено/повідомлено про декілька випадків іноземних терористів-бойовиків, які обміняли своє майно на золото, але ситуація не повторюється і у будь-якому разі вимагає планування та знань.

Висновки: Кур'єри золота та дорогоцінних металів не є бажаним методом для терористичних груп, які надають перевагу використанню готівкових коштів. Тому рівень вразливості до фінансування тероризму вважається досить значним/значним (рівень 2).

Відмивання коштів

Оцінка загрози відмивання коштів, пов'язаної з кур'єрами золота та інших дорогоцінних металів, вказує на те, що організовані злочинні групи використовували цей метод для відмивання доходів, одержаних злочинним шляхом. На відміну від терористичних організацій, організовані злочинні групи вважають це привабливим способом відмивання доходів, одержаних злочинним шляхом. Це вимагає більше планування, аніж переміщення готівки, але не потребує значних знань, якщо йдеться про активи, які легко продаються (тобто перевага надається золоту порівняно з іншими дорогоцінними металами – алмазам порівняно з іншим камінням). Операції є малозатратними. Тому злочинці мають необхідну здатність і намір використовувати цей метод. Правоохоронні органи повідомляють, що використовувались інші види дорогоцінних металів (срібло, платина), але це мало місце не так часто, оскільки вони не так легко продаються та мають більш високі обмінні затрати, ніж золото/алмази.

Дослідження, проведені в ЄС, вказують на те, що одним з найбільш відповідних методів, пов'язаних з готівкою, є конвертація готівки на золото або ювелірні вироби. Деякі країни ЄС, такі як Італія та Бельгія, мають активні ринки золота. Поряд з легальним ринком, інформація вказує на те, що золото може бути вкрадено та переплавлено. Після обміну отриманих злочинним шляхом готівкових коштів на золото, воно експортується у країни Близького Сходу та Північної Африки, де спостерігається високий попит на ринку.

Висновки: Рівень загрози відмивання коштів, пов'язаної з кур'єрами золота та інших дорогоцінних металів, вважається значним (рівень 3).

Вразливість

Фінансування тероризму

Оцінка вразливості до фінансування тероризму, пов'язаної з кур'єрами золота та інших дорогоцінних металів, свідчить про таке:

а) схильність до ризику

Оцінка вразливості до фінансування тероризму, пов'язаної із схильністю до ризику, по суті пов'язана з діяльністю на основі готівкових коштів (анонімність, швидкість). Тому схильність до ризику є особливо важливою для цього методу.

b) обізнаність про ризики

Сектор демонструє обмежену обізнаність про ризики, а здійснювані перевірки є дуже слабкими.

c) законодавча база і засоби контролю

До набрання чинності новим Регламентом про контроль готівкових коштів не здійснюється жодних перевірок правильності обов'язкового декларування транспортування дорогоцінних металів/каміння на зовнішніх кордонах ЄС. Ці активи виявити непросто. Перевірки у країнах призначення за межами ЄС не допомагають зменшити ризики (конвертацію золота/алмазів у готівку у країні призначення без належної перевірки клієнтів).

Висновки: Кур'єри золота та інших дорогоцінних металів не контролюються належним чином з огляду на обмежену обізнаність сектора. Перевірки є слабкими, а залежність від готівкових коштів збільшує вразливість. Не здійснюються перевірки декларацій про переміщення дорогоцінних металів/каміння на зовнішніх кордонах ЄС. Тому рівень загрози фінансування тероризму, пов'язаної з кур'єрами золота та інших дорогоцінних металів, вважається дуже значним (рівень 4).

Відмивання коштів

Оцінка вразливості до відмивання коштів, пов'язаної з кур'єрами золота та інших дорогоцінних металів, свідчить про таке:

a) схильність до ризику

Схильність до ризику суттєво пов'язана з діяльністю на основі готівкових коштів (анонімність, швидкість). Тому схильність до ризику є особливо важливою для цього методу.

b) обізнаність про ризики

Сектор демонструє обмежену обізнаність про ризики, а здійснювані перевірки є дуже слабкими. Правоохоронні органи також зауважили, що злочинні організації користуються невизначеністю законодавчої бази ЄС, зокрема щодо розкриття інформації про готівкові платежі.

c) законодавча база і перевірки

Не здійснюються жодні перевірки шляхом обов'язкового декларування транспортування дорогоцінних металів/каміння на зовнішніх кордонах ЄС (тобто це не підпадає під дію Регламенту про контроль готівкових коштів). Ці активи виявити непросто. Перевірки у країнах призначення за межами ЄС не допомагають зменшити ризики (конвертацію золота/алмазів у готівку у країні призначення без належної перевірки клієнтів).

Висновки: Кур'єри золота та інших дорогоцінних металів не контролюються належним чином з огляду на обмежену обізнаність сектора. Перевірки є слабкими, а залежність від готівкових коштів збільшує вразливість. Не здійснюються перевірки декларацій про переміщення дорогоцінних металів/каміння на зовнішніх кордонах ЄС. Тому рівень загрози відмивання коштів, пов'язаної з кур'єрами золота та інших дорогоцінних металів, вважається дуже значним (рівень 4).

Пом'якшувальні заходи:

Як рекомендовано наднаціональною оцінкою ризиків 2017 року, Комісія ухвалила новий Регламент про контроль готівкових коштів для подальшого пом'якшення описаних ризиків.

8. Інвестиційна нерухомість

Продукт
Купівля та продаж нерухомості

Сектор
Сектор нерухомості, незалежні юристи, нотаріуси, кредитні установи

Опис сценарію ризиків

Відмивання коштів через нерухомість є зростаючою світовою проблемою, яка, за оцінками, сягає 1,6 трлн доларів США на рік. Хоча точний масштаб незаконної діяльності у секторі важко оцінити, у 2017 році фізичні особи або компанії з високим ризиком відмивання коштів в одному тільки Лондоні, за оцінками, володіли нерухомим майном на суму понад 4,2 млрд фунтів стерлінгів.[90] У Франції відділ фінансової розвідки TRACFIN визначив сектор нерухомості як основний канал відмивання коштів у країні. Із загальної кількості 62 000 звітів про підозрілі операції, надісланих до TRACFIN у 2016 році, лише 84 надійшли від агентів нерухомості, незважаючи на майже один мільйон угод, що були укладені в тому році[91].

---

[90] Шахрайські вежі: Розуміння впливу закордонної корупції на лондонський ринок нерухомості, Transparency International UK, березень 2017 року: https://www.transparency.org.uk/publications/faulty-towers-understanding-the-impact-of-overseas-corruption-on-the-london-property-market/#.W9LY-LpuaUk.

[91] Le Monde, 'Blanchiment d'Argent: les agents immobiliers font-ils preuve de complaisance?', 29 грудня 2017 року: http://www.lemonde.fr/societe/article/2017/12/29/blanchiment-d-argent-les-agents-immobiliers-en-

Злочинці можуть здійснювати інвестиції в якості нерезидентів у країні (використовуючи візові системи) та розвивати мережі ВК/ФТ.

Загроза

Фінансування тероризму

Оцінка загрози фінансування тероризму, пов'язаної з інвестиціями в нерухомість, розглядається разом із схемами відмивання коштів, пов'язаними з інвестиціями в нерухомість, для приховування незаконного походження коштів. Тому загроза фінансування тероризму не потребує окремої оцінки.

Висновок: Рівень загрози фінансування тероризму, пов'язаної з інвестиціями у нерухомість, вважається дуже значним (рівень 4).

Відмивання коштів

Оцінка загрози відмивання коштів, пов'язаної з інвестиціями у нерухомість, продемонструвала періодичне використання сектора нерухомості організованими злочинними групами для відмивання доходів, одержаних злочинним шляхом. Сектор нерухомості переважно використовується у поєднанні з іншими секторами, такими як особи, які надають послуги з управління довірчими фондами та компаніями або юридичні консультанти, але сам по собі представляє певну загрозу. Використання нерухомого майна не вимагає спеціальних знань або досвіду і може бути досить привабливим з фінансової точки зору, залежно від послуг, що надаються.

Висновки: На основі надійних доказів, зібраних правоохоронними органами, про те, що нерухомість часто використовується у схемах відмивання коштів, та з огляду на те, що такі послуги можуть поєднуватися з послугами, які надаються іншими нефінансовими фахівцями, рівень загрози фінансування тероризму, пов'язаної з нерухомістю, вважається дуже значним (рівень 4).

Вразливість

Фінансування тероризму

Оцінка вразливості до фінансування тероризму, пов'язаної з інвестиціями в нерухомість, розглядається разом із схемами відмивання коштів, пов'язаними з інвестиціями в нерухомість, для приховування незаконного походження коштів. Тому загроза фінансування тероризму не потребує окремої оцінки.

Висновок: Рівень вразливості до фінансування тероризму, пов'язаної з інвестиціями в нерухомість, вважається дуже значним (рівень 4).

Відмивання коштів

Оцінка вразливості до відмивання коштів, пов'язаної з інвестиціями в нерухомість, свідчить про таке:

a) схильність до ризику

Хоча на практиці готівкові кошти використовуються дедалі менше, вони все ще можуть використовуватися для фінансування операцій з нерухомістю у деяких державах-членах. Це збільшує ризик анонімних операцій. Агенти з нерухомості зазвичай підтримують ділові відносини з іншими фахівцями, що ускладнює ефективний моніторинг таких ділових відносин (для здійснення перевірок сектори покладаються один на одного)[92], що збільшує схильність до ризику. Діяльність у секторі нерухомості може ґрунтуватися на фінансових потоках, що надходять з-за меж ЄС та клієнтів високого ризику, таких як впливові політичні особи.

b) обізнаність про ризики

Рівень обізнаності у секторі є нерівномірним і залежить, зокрема, від розміру відповідної організації/компанії. Більші структури можуть бути більш обізнаними про ризик їх неправомірного використання і розглядають можливість відігрівання ними певної ролі у моніторингу своїх клієнтів. Деякі з них розробляють інформаційні та навчальні матеріали, а також оцінки ризиків. Члени сектора є добре обізнаними про свої юридичні зобов'язання, такі як випадки, коли потрібна розширена належна перевірка.

Що стосується невеликих суб'єктів, крім юристів, які є частиною «парасолькової» організації, рівень обізнаності є значно нижчим, оскільки: (i) вони необов'язково інтегровані до централізованої організаційної структури, яка забезпечує надання настанов та навчання; (ii) вони мають справу з меншими обсягами продажу, а тому можуть мати труднощі в розумінні та застосуванні складної системи протидії відмиванню коштів (це стосується, зокрема, окремих підприємців); та/або (iii) вони, як правило, покладаються на інші сектори для проведення належної перевірки клієнтів.

Така сама інформація може бути недоступною на всіх етапах операції, наприклад, якщо особа покупця змінюється з практичних чи комерційних причин і про таку зміну нічого невідомо на початку ділових відносин. Рівень обізнаності невеликих суб'єктів залежить від того, наскільки доступним є навчання.

У будь-якому разі, «розсіювання» залучених зобов'язаних суб'єктів не спрощує здійснення перевірок і розуміння застосування належної перевірки клієнтів. Контроль сектору також є неповним і ґрунтується на слабких інформаційних даних (відсутність письмових угод, використання послуг адвокатів лише для скріплення документа печаткою тощо).

c) законодавча база і засоби контролю

[92] Тим не менш, кінцева відповідальність лежить на відповідному професіоналі, тобто професіоналам не дозволяється покладатися один на одного (див. Преамбулу 35 та статтю 25 Четвертої директиви про боротьбу за відмиванням грошей). Навпаки, наявність більшої кількості людей, які виконують свої зобов'язання щодо належної перевірки, може збільшити шанси виявити діяльність відмивання коштів.

Агенти з нерухомості підпадають під дію вимог ЄС щодо протидії відмиванню коштів. Після внесення змін П'ятою директивою про боротьбу з відмиванням грошей інформація про право власності на нерухоме майно будь-якої фізичної чи юридичної особи має бути надана централізовано органам державної влади. Для цього не потрібно створювати центральний реєстр нерухомості. Крім того, можуть використовуватися електронні системи пошуку даних.

Однак, якщо в операціях з нерухомістю беруть участь декілька зобов'язаних суб'єктів, компетентним органам важко визначити роль агента з нерухомості та виявити тривожні сигнали. Правові практики та процедури для таких операцій з нерухомістю є різними в різних країнах. У деяких країнах агент з нерухомості може готувати попередню юридичну документацію (хоча для завершення операції можуть знадобитися послуги юриста), а в інших країнах адвокат готує юридичну документацію, включно з угодою.

Звітування про підозрілі операції є нерівномірним і є задовільним лише тоді, коли це робиться зобов'язаними суб'єктами, крім агентів з нерухомості (деякі агенти з нерухомості вважають, що оскільки вони не беруть участі у переказі коштів, вони не повинні звітувати про підозрілі операції). Як наслідок, слідчі органи можуть здійснювати свій власний аналіз, але не на основі інформації про нерухомість. Представники приватного сектора вважають головним завданням ідентифікувати бенефіціарне право власності, оскільки наразі реєстрація такої інформації не є обов'язковою. Це особливо стосується випадків, коли продавець і покупець здійснюють операцію на основі «довіри».

Практика у секторі відрізняється тим, що представницькі професійні асоціації докладають зусиль для підвищення обізнаності та обміну прикладами належної практики для своїх членів.[93]

Висновки: Сектор нерухомості є недостатньо організованим, щоб належним чином підвищити рівень обізнаності про ризики. Залучення різних типів зобов'язаних суб'єктів до операцій з нерухомістю/ділових відносин, як правило, відштовхує сектор від здійснення власної належної перевірки клієнтів. Звітування про підозрілі операції є незадовільним. Перевірки важко здійснювати, і не завжди наявні надійні інформаційні дані. Тому рівень вразливості до відмивання коштів, пов'язаної з сектором нерухомості, вважається <u>значним/дуже значним</u> (рівень 3/4).

Пом'якшувальні заходи:

1) <u>для компетентних органів:</u>

- Держави-члени повинні забезпечити, що компетентні органи/органи саморегулювання, які здійснюють нагляд за сектором нерухомості, складатимуть щорічні звіти про заходи нагляду, яких було вжито для забезпечення того, що цей сектор точно виконуватиме свої зобов'язання щодо ПВК/ФТ. Органи саморегулювання повинні щорічно звітувати про кількість звітів про підозрілі операції, поданих до підрозділів фінансової розвідки.

[93] Як приклад належної практики саморегулювання, представницька організація в Бельгії розробила онлайн-інструмент для збирання інформації та передачі її національним органам влади. Цей інструмент наразі впроваджується у всіх інших країнах ЄС, і національні органи влади можуть надавати підтримку для забезпечення нормативно-правового дотримання.

- Перевірки на місцях відповідають кількості представників сектору нерухомості на території держави-члена.

2) для держав-членів:

- Держави-члени повинні надавати настанови щодо факторів ризику, що створюють операції з нерухомістю, а також забезпечувати спеціальне навчання для аналізу ситуацій, коли в операції з нерухомістю бере участь декілька професіоналів (наприклад, агент з нерухомості, юрист, фінансова установа).

3) Багаторівневе управління та місцеве самоврядування: покращення обміну знаннями та співпраці:

Європейські міста часто стикаються з негативними соціальними наслідками відмивання коштів у секторі нерухомості. На цьому було наголошено під час публічних слухань Комітету з питань оподаткування Європейського Парламенту 5 лютого 2019 року. У 2018 році у місті Амстердам відбулася триденна конференція під назвою «Літаючі гроші» (Flying Money), присвячена впливу незаконних грошових потоків, на якій 14 європейських міст поділилися своїм досвідом. Одним із висновків було те, що було б корисно зрозуміти, як різні рівні управління, які беруть участь у боротьбі з відмиванням грошей у секторі нерухомості (місцеві, національні та європейські), можуть надалі співпрацювати, обмінюватися знаннями та досвідом і виробляти рішення, наприклад, в частині подальшого покращення обміну інформацією у межах ЄС та організації навчання/надання настанов для представників сектора (та зобов'язаних суб'єктів).

9. Послуги, які надаються бухгалтерами, аудиторами, радниками і податковими консультантами

Продукт
Послуги, які надаються бухгалтерами, аудиторами, радниками і податковими консультантами

Сектор
Бухгалтери-ревізори, аудитори, податкові консультанти

Загальний опис сектора та відповідного продукту/діяльності

Бухгалтери, аудитори та консультанти працюють у різних якостях та секторах: у невеликих та крупних бухгалтерських фірмах, малих і середніх підприємствах, крупних компаніях, урядах, некомерційних організаціях, у сфері освіти тощо.

Якщо конкретно розглядати питання протидії відмиванню коштів, представники цієї професії пов'язані зобов'язаннями відповідно до національного законодавства щодо ПВК/ФТ та рекомендацій FATF. Інші перевірки представників цієї професії та практики пом'якшення ризиків включають таке:

- процедури перевірки крупних організацій у рамках процесу «знай свого клієнта»/належної перевірки клієнтів;
- використання нових технологій, таких як аналітика даних, аналіз процесів, штучний інтелект, перевірка операцій у режимі реального часу, «блокчейн» та старт-угоди, які можуть допомогти у боротьбі з ризиками шахрайства та відмивання коштів.

Їх різноманітна професійна діяльність може бути згрупована таким чином:

- **Бухгалтери** допомагають організаціям підготувати свої фінансові та нефінансові дані для оцінки ефективності, включаючи соціальний вплив їх економічної діяльності. Таким чином, вони допомагають організаціям управляти ризиками і контролювати їх, а також забезпечують здійснення перевірок та підтримання балансу в області належного управління, етики і сталого розвитку. Вони також повідомляють про результати таких оцінок зовнішньому світу, аби зацікавлені сторони могли ґрунтувати свої рішення на результатах діяльності організації. У деяких випадках вони можуть надавати додаткові послуги (див. пункт про консультантів нижче).
- **Аудитори**[94] засвідчують інформацію шляхом надання незалежної експертної думки для покращення інформації організації чи її контексту. У разі обов'язкового аудиту вони забезпечують здійснення юридично обов'язкової перевірки фінансових звітів крупних та середніх компаній та готують висновок щодо них. У деяких випадках вони можуть надавати додаткові послуги (див. пункт про консультантів нижче).
- **Консультанти:** Багато організацій покладаються на поради, надані спеціалістами з бухгалтерського обліку, наприклад, з питань фінансів, податків, корпоративної соціальної відповідальності, людських ресурсів, захисту даних та кібербезпеки.

Податкові консультанти надають різноманітні послуги. Основна діяльність у сфері податкових консультацій може бути згрупована таким чином:

- Податкова відповідність: підготовка податкових декларацій, соціальні виплати та заробітна плата, дотримання різноманітних вимог щодо обов'язкового звітування, реєстрації або публікації;
- Консультації: консультації з питань оподаткування, які не надаються на регулярній основі (наприклад, спадкування, злиття чи виділення, неплатоспроможність, заснування компанії, купівля нерухомого майна), податкове розслідування, податкове планування/оптимізація податків;
- Судові процеси з питань оподаткування та апеляції, консультації щодо таких судових процесів, представництво у кримінальних податкових справах.

Основна діяльність податкових консультантів є різною в різних країнах, залежно від того, чи організований податковий сектор аналогічно бухгалтерському чи законодавчому.

[94] Додаткова інформація про законодавство ЄС в області аудиту доступна за посиланням: https://ec.europa.eu/info/eu-law-topic/eu-auditing-law_en. Інформація про аудиторську перевірку фінансової звітності компаній доступна за посиланням: https://ec.europa.eu/info/business-economy-euro/company-reporting-and-auditing/auditing-companies-financial-statements_en

- У семи з 22 країн (Бельгія, Іспанія, Греція, Ірландія, Португалія, Румунія та Словаччина) податкові консультанти не можуть представляти своїх клієнтів у податкових (або, якщо застосовується, адміністративних) судах, оскільки це можуть робити лише адвокати. Однак в Ірландії та Іспанії податкові консультанти можуть представляти клієнтів у судах в апеляційному провадженні.
- У восьми країнах (Фінляндія, Італія, Латвія, Люксембург, Нідерланди, Польща, Швейцарія та Сполучене Королівство) податкові консультанти можуть представляти своїх клієнтів у суді у справах, які стосуються фіскальних питань, але не у кримінальних справах (у Люксембургу це стосується представництва бухгалтерами у суді першої інстанції).
- У шести країнах (Австрія, Чехія, Німеччина, Хорватія, Російська Федерація та Україна) податкові консультанти також можуть представляти своїх клієнтів у кримінальних справах (хоча на практиці це не має місця в Чехії та Хорватії).
- У восьми країнах (Австрія, Німеччина, Фінляндія, Латвія, Нідерланди, Польща, Російська Федерація та Україна) податкові консультанти можуть представляти своїх клієнтів у Верховному Суді у податкових справах, хоча в Австрії та Фінляндії це стосується лише Верховного адміністративного суду. У Франції податковими консультантами є адвокати.

Незалежно від того, чи є податковий консультант окремою професією у країні, дуже мало податкових консультантів надають послуги лише з вирішення податкових питань. Оскільки оподаткування часто пов’язано з іншими сферами, податкові консультанти часто надають послуги і в таких інших сферах (бухгалтерський облік, пенсійне забезпечення, консалтинг, юридичні консультації з питань корпоративного права, аудит чи арбітраж).

На рівні ЄС, крім Договору про функціонування ЄС, до податкового сектора застосовується ще низка директив ЄС:
- Директива 2005/36/ЄС про професійну кваліфікацію;
- Директива про послуги (2006/123/ЄС);
- Директиви, які стосуються тимчасових послуг (1977/249/ЄЕС) та заснування (1998/5/ЄС) адвокатів;
- Директива 2005/60/ЄС;
- Директива 2011/83/ЄС застосовується, коли податкові консультанти мають споживчих клієнтів; та
- Директива 2000/31/ЄС застосовується до транскордонних податкових консультаційних послуг.

Змінена Директива про аудит (2014/56/ЄС) та Регламент про аудит (537/2014/ЄС), які набрали чинності 17 червня 2016 року та вводять більш жорсткі вимоги до обов’язкових аудиторських перевірок суб’єктів державного інтересу, таких як котирувані на біржі компанії, кредитні установи та страхові компанії. Це має знизити ризики надмірної фамільярності між законними аудиторами та їх клієнтами, підвищити професійний скептицизм та зменшити конфлікт інтересів. Регламент встановлює вимогу щодо надання послуг, які не пов’язані з аудитом. Крім того, він накладає зобов’язання на зовнішніх аудиторів щодо звітування перед органами нагляду про серйозне порушення правил або про існування істотної загрози чи сумнівів стосовно безперервного функціонування суб’єкта, що перевіряється.

Опис сценарію ризиків

Злочинці можуть використовувати або вимагати надання послуг бухгалтерів, аудиторів або податкових консультантів, хоча і з помірним рівнем участі самих спеціалістів, з метою:

- зловживання облікових записів клієнтів;
- купівлі нерухомого майна;

- заснування довірчих фондів та компаній/управління довірчими фондами та компаніями;
- ведення певних судових проваджень, заснування благодійних організацій та управління ними;
- виставлення рахунків-фактур на надмірні чи недостатні суми або підроблених декларацій на імпорт/експорт товарів;
- надання гарантій; та/або
- надання допомоги у питаннях податкової відповідності.

Експерти у цих сферах можуть залучатися до схем відмивання коштів, допомагаючи створювати «непрозорі структури», визначені як бізнес-структури, де справжня особа власника(-ів) юридичних суб'єктів та юридичних утворень приховується за допомогою, наприклад, призначених директорів. Створення таких структур, які часто засновуються у багатьох юрисдикціях, в тому числі офшорних центрах, є складним процесом і вимагає професійних регулятивних та податкових послуг.

Загроза

Фінансування тероризму

Оцінка загрози фінансування тероризму, пов'язаної з послугами, що надаються бухгалтерами, аудиторами, радниками та податковими консультантами, розглядається разом із схемами відмивання коштів, пов'язаними з послугами, які надаються такими професіоналами для приховування незаконного походження коштів (див. нижче). Тому загроза фінансування тероризму не потребує окремої оцінки.

Висновок: Рівень загрози фінансування тероризму, пов'язаної з послугами, які надаються радниками та податковими консультантами, вважається дуже значним (рівень 4). Рівень загрози фінансування тероризму, пов'язаної з певними додатковими послугами, які надаються бухгалтерами та аудиторами, вважається значним (рівень 3).

Відмивання коштів

Оцінка загрози відмивання коштів, пов'язаної з послугами, які надаються бухгалтерами, аудиторами, радниками та податковими консультантами, має деякі особливості, які є спільними з консультаціями юристів.

Що стосується будь-якої іншої юридичної діяльності, **ризик проникнення або набуття права власності з боку організованих злочинних груп** становить загрозу відмивання коштів для бухгалтерів, аудиторів, радників та податкових консультантів. Ці професіонали можуть ненавмисно брати участь у відмиванні коштів, але також можуть бути співучасниками або навмисно допускати недбалість у виконанні своїх зобов'язань щодо належної перевірки клієнтів.

У правоохоронних органів є докази того, що організовані злочинні групи часто використовують послуги податкових консультантів та залучають цей сектор у свої схеми відмивання коштів. Послуги податкових консультантів вважаються корисними для створення схем відмивання коштів, оскільки вони потрібні для певних видів діяльності та/або тому що доступ до спеціалізованих податкових знань та навичок може допомогти у відмиванні доходів, одержаних злочинним шляхом. Доступ до юридичних послуг податкових консультантів є досить простим і не вимагає конкретних компетенцій чи знань. Злочинні організації використовують навички таких професіоналів для створення схеми відмивання коштів і не змушені самостійно розвивати такі компетенції. Також є докази того, що деякі злочинці агітують та свідомо залучають податкових консультантів до своїх схем відмивання коштів.

Професіонали можуть бути залучені у процес відмивання коштів різною мірою. З ними можна консультуватися щодо того, як обійти конкретні законодавчі бази та як уникнути появи тривожних сигналів, встановлених банківськими установами. Вони також можуть використовувати більш проактивний підхід, безпосередньо надаючи допомогу або керуючи процесом відмивання коштів. Однак часто злочинці залучають податкових консультантів, тому що послуги, які ті пропонують, є важливими для конкретної операції, і вони додають респектабельності такій операції.

Експерти в цих сферах належать до числа професіоналів, які найчастіше використовуються організованими злочинними групами для відмивання злочинних доходів з огляду на типи послуг, які вони можуть надавати своїм клієнтам. Вони можуть створювати корпоративні структури, розробляти системи бухгалтерського обліку, надавати бухгалтерські послуги, готувати документацію (фінансову звітність чи довідки, шахрайські доходи та витрати), надавати послуги у питаннях неплатоспроможності та загальні бухгалтерські консультації. Надаючи такі послуги, деякі бухгалтери можуть допомагати організованим злочинним групам приховувати свою особу та походження коштів, якими вони володіють.

Більшість з цих послуг використовується для законних цілей. Однак вони також можуть підтримувати широкий спектр схем відмивання коштів. Сюди відносяться шахрайська торговельна діяльність, фальшиві рахунки-фактури, підготовка фіктивних декларацій про доходи, шахрайське банкрутство, ухилення від сплати податків та інші види зловживань фінансовими записами.

Висновки: Послуги, які надаються радниками та податковими консультантами, аудиторами та бухгалтерами, часто використовуються у схемах відмивання коштів і розглядаються організованими злочинними групами як спосіб компенсувати відсутність необхідних знань. Рівень загрози відмивання коштів, пов'язаної з послугами, які надаються радниками та податковими консультантами, вважається дуже значним (рівень 4). Рівень загрози відмивання коштів, пов'язаної з певними додатковими послугами, які надаються бухгалтерами та аудиторами, вважається значним (рівень 3).

Вразливість

Фінансування тероризму

Оцінка вразливості до фінансування тероризму, пов'язаної з послугами, які надаються бухгалтерами, радниками та податковими консультантами, розглядається разом із схемами відмивання коштів, пов'язаними з послугами, що надаються такими професіоналами для приховування незаконного походження коштів. Тому загроза фінансування тероризму не потребує окремої оцінки.

Висновки: Аналогічно відмиванню коштів, рівень вразливості до фінансування тероризму, пов'язаної з послугами, які надаються бухгалтерами, аудиторами, радниками та податковими консультантами, вважається значним (рівень 3).

Відмивання коштів

Оцінка вразливості до відмивання коштів, пов'язаної з послугами, які надаються бухгалтерами, аудиторами, радниками та податковими консультантами, свідчить про таке:

а) схильність до ризику

Податкові консультанти досить часто можуть залучатися в управлінні складними операціями, які передбачають надання податкових консультацій. Такі операції можуть обумовлювати схильність цього сектора до клієнтів високого ризику (наприклад, впливові політичні особи) або складних юридичних суб'єктів або юридичних утворень, коли дуже складно ідентифікувати бенефіціарного власника. Цей сектор також може керувати податковими питаннями, пов'язаними з цими складними юридичними суб'єктами та юридичними утвореннями, оскільки це його основна діяльність.

b) обізнаність про ризики

Бухгалтери, аудитори та податкові консультанти зобов'язані дотримуватися суворих етичних та професійних норм, і вони вважають це достатнім захистом від відмивання коштів та фінансування тероризму, що мають місце в їх секторі або через їх сектор. Однак у цей сектор також можуть проникати організовані злочинні групи, і деякі галузеві органи нагляду все ще не мають належних засобів для виявлення подібного роду зловживань (тобто у деяких юрисдикціях відсутні вимоги до належного тестування).

Цей сектор користується вигодами міцної організаційної бази на рівні ЄС. Наприклад, Європейська федерація бухгалтерів та аудиторів для малого та середнього бізнесу (EFAA), «парасолькова» організація національних бухгалтерів та аудиторських організацій, нараховує 17 членів по всій Європі, які представляють понад 320 000 бухгалтерів, аудиторів та податкових консультантів. Європейська податкова конфедерація (The Confédération Fiscale Européenne) охоплює 26 національних організацій з 21 європейських держав, що представляють понад 200 000 податкових консультантів. Ще одним прикладом є компанія Accountancy Europe. Вона об'єднує 51 професійну організацію з 36 країн, що представляють близько мільйона професійних бухгалтерів, аудиторів та радників.

Роль цих організацій полягає у забезпеченні обміну інформацією про національне законодавство, що стосується їх сектора, та координації дотримання законодавства ЄС. Вони також забезпечують, щоб професіонали були обізнані про зміни у законодавстві ЄС, які стосуються, наприклад, їх зобов'язань щодо протидії відмиванню коштів.

Для аудиторів Регламентом про аудит також створено Комітет європейських органів нагляду за аудитом (CEAOB). CEAOB лежить в основі співпраці між національними органами нагляду за аудитом на рівні ЄС. Його роль полягає у посиленні нагляду за аудитом на рівні ЄС.[95]

Сильна організація необов'язково гарантує високу якість співпраці з компетентними органами у всіх сферах.[96] Крім того, деякі компетентні органи та підрозділи фінансової розвідки вважають, що бухгалтери, аудитори та податкові консультанти досі належним чином не обізнані про ризики, що їх створюють непрозорі структури, та про способи приховування бенефіціарного права власності. Однак для покращення ситуації потрібен двосторонній потік інформації, і обмін типологіями та інформацією між правоохоронними органами дозволить краще оцінювати ризики.

---

[95] https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-reforms-and-their-progress/regulatory-process-financial-services/expert-groups-comitology-and-other-committees/committee-european-auditing-oversight-bodies_en

[96] Частина 2 статті 12 Регламенту про аудит накладає зобов'язання на зовнішніх аудиторів щодо звітування органам нагляду про серйозне порушення норм або про існування істотної загрози чи сумнівів стосовно безперервного функціонування суб'єкта, що перевіряється.

c) законодавча база і засоби контролю

Бухгалтери, аудитори,[97] радники та податкові консультанти підпадають під дію вимог ЄС щодо протидії відмиванню коштів з 2001 року. Вони повинні здійснювати належну перевірку клієнтів, якщо вони беруть участь, будь то від імені свого клієнта або замість свого клієнта, у будь-якій фінансовій операції чи операції з нерухомістю, або допомагають у плануванні чи здійсненні операцій для свого клієнта, що стосуються (i) купівлі та продажу нерухомого майна або суб'єктів господарювання; (ii) управління грошами, цінними паперами чи іншими активами клієнтів; (iii) відкриття або управління банківськими, ощадними рахунками чи рахунками у цінних паперах; (iv) організації внесків, необхідних для заснування, функціонування або управління компаніями; (v) заснування, функціонування або управління довірчими фондами, компаніями, фондами чи подібними структурами.

Податкові консультанти, радники, бухгалтери та аудитори є досить складним та різноманітним професійним сектором. Загалом, цей сектор характеризується тривалими діловими відносинами, що підвищують здатність професіоналів виявляти нестандартні угоди або поведінку. Тим не менш, у разі звернення за конкретною порадою щодо нерегулярної або разової операції, професіонал може виконати своє завдання, не розуміючи повною мірою фінансове становище свого клієнта. Це впливає на рівень звітування ними про підозрілі операції, який все ще досить низький, але все ж таки вищий, порівняно із звітуванням адвокатами. Сектор іноді виправдовує цей низький рівень звітування про підозрілі операції тим, що в цій галузі відповідальний професіонал не обробляє і не ініціює фінансову операцію від імені свого клієнта. Тривожні сигнали ґрунтуються не на операції, а на будь-яких незвичних моделях поведінки. Іноді робота бухгалтерів та податкових консультантів може включати елемент розслідування та аудиту, який може стати корисною інформацією для можливих звітів про підозрілі операції.[98]

Зважаючи на те, що непрозорі структури можуть створюватися у багатьох юрисдикціях, у тому числі в офшорних центрах, професіонали можуть користуватися податковими та регулятивними відмінностями для продажу своїх послуг.

Висновки: Бухгалтери, аудитори, радники та податкові консультанти мають належну організацію. Однак у тому, як вони здійснюють перевірки та управляють ризиками, присутні слабкі місця. Рівень вразливості до відмивання коштів, пов'язаної з послугами, які надаються бухгалтерами, аудиторами, радниками та податковими консультантами, вважається значним (рівень 3).

Пом'якшувальні заходи:

1) для Комісії:

Директива (ЄС) 2015/849 із змінами, внесеними Директивою (ЄС) 2018/843, уточняє сферу її застосування, стосовно зовнішніх аудиторів, бухгалтерів та податкових консультантів, розширюючи її до будь-якої іншої особи, яка надає матеріальну допомогу, підтримку або консультації з питань оподаткування в рамках своєї основної діяльності чи професійної діяльності.

[97] Контроль аудиторів суб'єктів державного інтересу не здійснюється компетентними органами/органами саморегулювання.
[98] Див. попередню виноску.

Що стосується бенефіціарного права власності, корпоративні суб'єкти та довірчі фонди повинні володіти інформацією про те, хто є їх бенефіціарним власником. Крім того, бенефіціарні власники повинні надавати корпоративним суб'єктам необхідну їм інформацію. А корпоративні суб'єкти та довірчі фонди повинні надавати цю інформацію своїм бухгалтерам.

У разі недотримання цих правил, застосовується ефективні, відповідні та запобіжні заходи або санкції.

Директива 2018/822/ЄС набирає чинності з 2020 року, коли посередники зобов'язані подавати інформацію про транскордонні податкові механізми[99] своїм національним органам.

З огляду на це, Комісія повинна здійснювати:

- транспозиційні перевірки щодо виконання вимог прозорості стосовно інформації про бенефіціарне право власності (реєстрація) – держави-члени повинні повідомляти про технічні елементи свого національного режиму ПВК/ФТ, забезпечуючи вимоги прозорості до інформації про бенефіціарне право власності; та
- транспозиційні перевірки щодо виконання вимог ідентифікації стосовно інформації про бенефіціарне право власності (визначення бенефіціарного власника) – держави-члени повинні повідомляти про технічні елементи свого режиму ПВК/ФТ, пов'язаного з визначенням бенефіціарного власника.

2) <u>для компетентних органів:</u>

- Держави-члени повинні забезпечити, що компетентні органи/органи саморегулювання (якщо вони відповідають за нагляд), контролюючі зовнішні аудитори, бухгалтери-ревізори та податкові консультанти надаватимуть інформацію про вжиті ними заходи нагляду для забезпечення того, що сектор точно виконуватиме свої зобов'язання щодо ПВК/ФТ. У разі отримання звітів про підозрілі операції, органи нагляду повинні щорічно звітувати про кількість звітів, поданих підрозділам фінансової розвідки.
- Перевірки на місцях відповідають кількості представників зовнішніх аудиторів, бухгалтерів-ревізорів та податкових консультантів на території держави-члена.

3) <u>для держав-членів:</u>

- Держави-члени повинні надавати настанови щодо факторів ризику, які виникають внаслідок операцій за участі бухгалтерів-ревізорів та податкових консультантів.

[99] https://ec.europa.eu/taxation_customs/business/tax-cooperation-control/administrative-cooperation/enhanced-administrative-cooperation-field-direct-taxation_en

Заохочення до покращення розуміння зовнішніми аудиторами, бухгалтерами-ревізорами та податковими консультантами того, як тлумачити і застосовувати юридичний привілей. Держави-члени повинні видати настанови щодо реалізації юридичного привілею – як поділити юридичні послуги, залежно від суті юридичного привілею, та інші юридичними послугами, що не підпадають під дію юридичного привілею, коли вони надаються тому самому клієнту.

10. Юридичні послуги, які надаються нотаріусами та іншими незалежними юристами

Продукт
Юридичні послуги, які надаються юристами

Сектор
Незалежні юристи, адвокати, нотаріуси

Опис сценарію ризиків

Злочинці можуть наймати або користуватися послугами юриста (наприклад, адвоката, нотаріуса чи іншого незалежного спеціаліста з юридичних питань) для:

- зловживання рахунками клієнтів;
- купівлі нерухомого майна;
- заснування довірчих фондів і компаній/управління довірчими фондами і компаніями; або
- ведення певних судових процесів.

Вони можуть залучатися до схем відмивання коштів, допомагаючи створювати «непрозорі структури», визначені як бізнес-структури, де справжня особа власника(-ів) юридичних суб'єктів та юридичних утворень приховується за допомогою, наприклад, призначених директорів. Створення таких структур, які часто засновуються у багатьох юрисдикціях, в тому числі офшорних центрах, є складним процесом і вимагає професійних регулятивних та податкових послуг.

Загроза

Фінансування тероризму

Оцінка вразливості до фінансування тероризму, пов'язаної з юридичними послугами, які надаються спеціалістами з юридичних питань, розглядається разом із схемами відмивання коштів, пов'язаними з послугами, які надаються такими спеціалістами для приховування незаконного походження коштів. Тому загроза фінансування тероризму не потребує окремої оцінки.

Висновок: Рівень загрози фінансування тероризму, пов'язаної з послугами, які надаються спеціалістами з юридичних питань, вважається <u>дуже значною</u> (рівень 4).

Відмивання коштів

Оцінка загрози відмивання коштів, пов'язаної з послугами, які надаються спеціалістами з юридичних питань, має деякі особливості, які є спільними з юридичним послугами, які надаються бухгалтерами, аудиторами та податковими консультантами.

- Що стосується будь-якої іншої юридичної діяльності, ризик проникнення або набуття права власності з боку організованих злочинних груп становить загрозу відмивання коштів для бухгалтерів, аудиторів, радників та податкових консультантів. Ці спеціалісти можуть ненавмисно брати участь у відмиванні коштів, але також можуть бути співучасниками або навмисно допускати недбалість у виконанні своїх зобов'язань щодо належної перевірки клієнтів.

- Правоохоронні органи повідомляють, що організовані злочинні групи часто використовують юридичні послуги, що надаються спеціалістами з юридичних питань, та залучають цей сектор у свої схеми відмивання коштів. Послуги спеціалістів з юридичних питань вважаються корисними для створення схем відмивання коштів, оскільки вони потрібні для певних видів діяльності та/або тому що доступ до спеціалізованих податкових знань та навичок може допомогти у відмиванні доходів, одержаних злочинним шляхом. Найчастіше злочинці використовують адвокатів, адже залучення адвоката додає респектабельності та видимість легітимності

діяльності навіть тоді, коли надана послуга може допомогти злочинцям відмивати кошти.

Спеціалісти з юридичних питань можуть підтримувати відмивання коштів, використовуючи інструменти, які вже є у їх розпорядженні (наприклад, рахунки клієнтів), або допомагаючи своїм клієнтам створювати та управляти рахунками, довірчими фондами та компаніями для приховування та/або легітимізації джерела своїх коштів.

Існує багато способів використання рахунків клієнтів для відмивання коштів, найпоширенішими з яких є:

- здійснення фінансових операцій від імені клієнта, включаючи офшорний банкінг;
- прийняття крупних грошових депозитів на рахунок клієнта з подальшим зняттям готівки або видачею чеків;
- купівля нерухомого майна, компаній або земельних ділянок від імені клієнта; та
- у деяких випадках, використання особистого рахунка самих спеціалістів з юридичних питань для отримання та переказу коштів.

Юристи можуть допомагати у створенні та управління компаніями-оболонками та легітимізації компаній, укладаючи угоди та створюючи корпоративні рахунки. Офшорні компанії і довірчі фонди є особливо привабливими для організованих злочинних груп з огляду на їх суворі правила та практики банківської, правової та адміністративної таємниці, а також анонімність, яку вони забезпечують. На додаток до юридичних консультацій та послуг з оформлення документів, які вони надають, спеціалісти з юридичних питань також можуть відігравати активну роль в управлінні компанією та її активами. Наприклад, вони можуть представляти свого клієнта при купівлі-продажу компанії і відповідають за розпорядження фінансовими активами, замовляючи грошові перекази, купуючи інші компанії або вкладаючи гроші в нерухомість. Так само юристи можуть обіймати посаду в компанії (наприклад, власник, директор та адміністратор), ще більше віддаляючи свого клієнта від злочинних активів.

У більшості країн ЄС юристи надають повну документацію для створення та реєстрації компаній, передачі прав власності, відкриття рахунків у банках, рахунків-фактур та міжнародних торгових документів. Характер цієї документації є складним для розслідувань з огляду на її технічність та секретність.

Злочинні організації не вважають, що одержання доступу до спеціалістів з юридичних питань є складним завданням. Для них, покладання на навички спеціалістів з юридичних питань означає, що їм не потрібно розвивати ці компетенції самостійно. Для відмивання коштів деякі організовані злочинні групи проникають у юридичні фірми, діють як фіктивні адвокати або викрадають особу юристів.

Висновки: Відповідно до інформації, наданої правоохоронними органами, спеціалісти з юридичних питань часто використовуються у схемах відмивання коштів. Використання послуг спеціалістів з юридичних питань позбавляє організованих злочинних організацій необхідності самостійно набувати знання та досвід і забезпечує «підтвердження печатки» для їх діяльності. Рівень загрози відмивання коштів, пов'язаної із спеціалістами з юридичних питань (адвокатами, нотаріусами та іншими незалежними юристами), вважається <u>дуже значним</u> (рівень 4).

Вразливість

Фінансування тероризму

Оцінка вразливості до фінансування тероризму, пов’язаної з юридичними послугами, які надаються спеціалістами з юридичних питань, розглядається разом із схемами відмивання коштів, пов’язаними з послугами, які надаються такими спеціалістами для приховування незаконного походження коштів. Тому загроза фінансування тероризму не потребує окремої оцінки.

Висновок: Рівень загрози фінансування тероризму, пов’язаної з послугами, які надаються спеціалістами з юридичних питань, вважається значним (рівень 3).

Відмивання коштів

Оцінка вразливості до відмивання коштів, пов'язаної з юридичними консультаціями, які надаються спеціалістами з юридичних питань, свідчить про таке:

a) схильність до ризику

Схильність до ризику є результатом характеру деяких послуг/заходів, які надаються спеціалістами з юридичних питань (що вимагають дотримання положень про протидію відмиванню коштів).

На схильність до ризику цього сектора впливає той факт, що він досить часто може використовуватися для управління складними правовими ситуаціями. Зокрема, той факт, що юридичні послуги необов’язково передбачають здійснення належних фінансових операцій, означає, що спеціалістам з юридичних питань доводиться ініціювати інші типи тривожних сигналів, які важче визначити (наприклад, поведінку клієнта).

b) обізнаність про ризики

Організація сектора не є однаковою (сфера дії спеціалістів з юридичних питань є різною у різних державах-членах, але само по собі це не становить ризик), хоча деякі організації ЄС відіграють важливу роль у наданні інформації про те, як застосовувати вимоги щодо протидії відмиванню коштів/фінансуванню тероризму (ПВК/ФТ), у наданні настанов та сприянні обміну інформацією. Зокрема, вони допомагають визначити перелік тривожних сигналів, які можуть використовувати люди, що працюють у цьому секторі, наприклад, поведінка або особа клієнта, способи приховування (використання посередників, уникнення особистого контакту), розмір коштів (непропорційна сума приватного фінансування) тощо. Складається враження, що сектор вже обізнаний про деякі ризики, коли такий клієнт дає настанови щодо операцій на відстані або без законних підстав, або коли за короткий термін мають місце численні зміни юридичного консультанта, або коли використовується велика кількість юридичних консультантів без поважних причин.

Загалом, рівень звітування про підозрілі операції є дуже низьким при роботі із спеціалістами з юридичних питань (хоча, наприклад, звіти про підозрілі операції від спеціалістів з юридичних питань не можна порівнювати з юридичними звітами фінансових установ).

Однак у деяких країнах органи саморегулювання регулюються державою і є незалежними, діючи як посередники між фінансовими органами та залученими спеціалістами. Вони організовують, вивчають та оцінюють факти, допомагаючи фінансовим органам відрізняти відмивання коштів від звичайних випадків.

c) законодавча база і засоби контролю

Нотаріуси, адвокати та інші незалежні спеціалісти з юридичних питань підпадають під дію вимог ЄС щодо протидії відмиванню коштів з 2001 року. Вони повинні здійснювати належну перевірку клієнтів, якщо вони беруть участь, будь то від імені свого клієнта або замість свого клієнта, у будь-якій фінансовій операції чи операції з нерухомістю, або допомагають у плануванні чи здійсненні операцій для свого клієнта, що стосуються (i) купівлі та продажу нерухомого майна або суб'єктів господарювання; (ii) управління грошами, цінними паперами чи іншими активами клієнтів; (iii) відкриття або управління банківськими, ощадними рахунками чи рахунками у цінних паперах; (iv) організації внесків, необхідних для заснування, функціонування або управління компаніями; (v) заснування, функціонування або управління довірчими фондами, компаніями, фондами чи подібними структурами.

Спеціалісти з юридичних питань організовані та регулюються по-різному, залежно від держав-членів. Юридичні послуги також часто надаються безпосередньо, що є специфічним викликом для захисту працівників. Існують також відмінності між різними залученими секторами, оскільки нотаріуси, будучи спеціалістами, також беруть участь у виконанні державного обов'язку і мають у деяких державах-членах статус державних службовців.

У будь-якому разі має бути повністю гарантований захист анонімності спеціаліста з юридичних питань, який повідомляє про підозрілу операцію. У деяких державах-членах існує ризик того, що у звіті про підозрілі операції може зазначатися ім'я нотаріуса на початку декларації, зокрема, якщо вона супроводжується судовим провадженням. Для уникнення цього, слід розробити правила для запобігання розголошенню інформації про походження звіту про підозрілі операції.

Юридичним привілеєм (професійна таємниця) є визнаний принцип на рівні ЄС, що відображає крихкий баланс у світлі судової практики Європейського Суду про право на справедливий судовий розгляд (C-305/05), який, у свою чергу, відображає принципи Європейського суду з прав людини та Хартії (наприклад, Стаття 47). Мають місце випадки, коли такі спеціалісти іноді здійснюють діяльність, що охоплюється юридичним привілеєм (тобто підтвердження правового становища свого клієнта або його захист чи представництво у судових провадженнях), а також діяльність, не охоплена юридичним привілеєм, така як надання юридичних консультацій у разі створення, експлуатації та управління компаніями. Обсяг конфіденційності, юридичного привілею та професійної таємниці відрізняється залежно від країни, і практична основа, на якій такий захист може бути відхилений, має бути уточнена.

Висновки: Обізнаність сектора щодо ризиків все ще є обмеженою. Незважаючи на діючу законодавчу базу, нагляд за сектором не завжди забезпечує належний моніторинг можливих зловживань відмиванням коштів. Тому рівень вразливості до відмивання коштів, пов'язаної з юридичними послугами, які надаються спеціалістами з юридичних питань, вважається <u>значним</u> (рівень 3).

Пом'якшувальні заходи:

1) <u>для Комісії:</u>

- У контексті Директиви (ЄС) 2015/849 із змінами, внесеними Директивою (ЄС) 2018/843:

  - Транспозиційні перевірки щодо виконання вимог прозорості стосовно інформації про бенефіціарне право власності (реєстрація) – держави-члени повинні повідомляти про технічні елементи свого національного режиму ПВК/ФТ, забезпечуючи вимоги прозорості до інформації про бенефіціарне право власності.

  - Транспозиційні перевірки щодо виконання вимог ідентифікації стосовно інформації про бенефіціарне право власності (визначення бенефіціарного власника) – держави-члени повинні повідомляти про технічні елементи свого режиму ПВК/ФТ, пов'язаного з визначенням бенефіціарного власника.

  - Для кращого розповсюдження законодавчої бази ЄС щодо протидії відмиванню коштів та для забезпечення ефективного та послідовного застосування законодавства ЄС, Комісія має підтримувати навчальну діяльність для спеціалістів з юридичних питань (адвокатів та нотаріусів).

  - Для організації консультацій/обговорень із зацікавленими сторонами з метою надання допомоги в інформуванні Комісії про транспозицію директив про відмивання коштів та фінансування тероризму на всій території ЄС, а також для підвищення рівня обізнаності та обміну найкращими практиками щодо різних аспектів дотримання законодавства про протидію відмиванню коштів спеціалістами з юридичних питань.

- Директива 2018/822/ЄС набирає чинності з 2020 року, коли посередники зобов'язані подавати інформацію про транскордонні податкові механізми[100] своїм національним органам.

2) <u>для компетентних органів:</u>

- Держави-члени повинні забезпечити, що компетентні органи/органи саморегулювання, які здійснюють нагляд за незалежними спеціалістами з юридичних питань, адвокатами і нотаріусами, складатимуть щорічні звіти про наглядові заходи, яких було вжито для забезпечення того, що цей сектор точно виконуватиме свої зобов'язання щодо ПВК/ФТ. Отримуючи звіти про підозрілі операції, органи саморегулювання повинні щорічно звітувати про кількість звітів, поданих підрозділам фінансової розвідки.

- Перевірки на місцях відповідають кількості представників незалежних юристів, адвокатів, нотаріусів на території держави-члена.

3) <u>для держав-членів:</u>

- Держави-члени повинні надавати настанови щодо факторів ризику, які виникають внаслідок операцій за участі незалежних юристів, адвокатів, нотаріусів.

---

[100] https://ec.europa.eu/taxation_customs/business/tax-cooperation-control/administrative- cooperation/enhanced-administrative-cooperation-field-direct-taxation_en

Органи саморегулювання повинні докладати зусиль для збільшення кількості тематичних перевірок та звітування. Вони також повинні організовувати навчальні курси для забезпечення кращого розуміння ризиків та зобов'язань щодо дотримання норм ПВК/ФТ.

ПРОДУКТИ СЕКТОРА ГРАЛЬНОГО БІЗНЕСУ

1. Загальний опис сектора грального бізнесу

Загальний опис сектора та відповідного продукту/діяльності

Відповідно до чинної законодавчої бази ЄС щодо протидії відмиванню коштів (Четверта директива про боротьбу з відмиванням грошей), послуги грального бізнесу визначаються як послуги, які включають розміщення ставок з грошовою вартістю в азартних іграх, в тому числі тих, які мають елемент навичок, наприклад, лотереї, казино, покер та букмекерська діяльність, які надаються у фізичному місці або будь-яким способом на відстані, електронними засобами або з використанням будь-яких інших комунікаційних технологій та на індивідуальний запит одержувача послуг.

Отже, термін «гральний бізнес» відноситься до низки різних послуг та каналів розповсюдження. Для цієї оцінки ризиків, сектор грального бізнесу був поділений на фізичні (офлайн) та онлайн-ігри, а фізичний сектор у свою чергу був поділений на такі підсектори: букмекерська діяльність, бінго, казино, ігрові автомати, лотереї та покер. Подальший поділ на різні продукти онлайн-ігор не вважався необхідним, оскільки відповідні ризики, загрози та вразливості пов'язані в першу чергу з характером онлайн-операцій, а не з конкретними формами онлайн-ігор.

Усі провайдери послуг грального бізнесу є зобов'язаними суб'єктами відповідно до Четвертої директиви про боротьбу з відмиванням грошей. Держави-члени повинні регулювати та контролювати їх на предмет фінансування тероризму та відмивання коштів і надавати своїм компетентним органам повноваження з розширеного нагляду для їх моніторингу та гарантування того, що особи, які ефективно керують діяльністю таких суб'єктів, та бенефіціарні власники таких суб'єктів матимуть відповідні повноваження та компетенції.

Провайдери послуг грального бізнесу зобов'язані здійснювати належні перевірки клієнтів у випадках збирання виграшів, розміщення ставок або в обох таких випадках, при здійсненні операцій на суму понад 2 000 євро, незалежно від того, чи здійснюється операція у формі одиничної операції або у формі декількох пов'язаних операцій. Хоча держави-члени можуть звільняти певні послуги грального бізнесу від деяких або всіх вимог, передбачених Четвертою директивою про боротьбу з відмиванням грошей після здійснення відповідної оцінки ризиків, це не стосується казино. Звільнення, яке надається державою-членом, має застосовуватися лише у суворо обмежених та обґрунтованих обставинах, якщо ризики відмивання коштів або фінансування тероризму є низькими, і про такі звільнення необхідно повідомляти Комісії. Четверта директива про боротьбу з відмиванням грошей мала бути перенесена у національне законодавство до 26 червня 2017 року, тому наслідки змін, внесених Директивою щодо сектора грального бізнесу, важко оцінити на цьому ранньому етапі.

Не існує будь-якого спеціального для сектора законодавства ЄС про азартні ігри. Держави-члени можуть встановлювати цілі своєї політики та необхідний рівень захисту споживачів і запобігати злочинності, в тому числі відмиванню коштів. Однак застосовуються положення Договорів ЄС. Суд Європейського Союзу видав загальні настанови щодо тлумачення основних свобод внутрішнього ринку у сфері азартних ігор з урахуванням їх специфіки. Хоча держави-члени можуть обмежувати транскордонне надання гральних послуг з метою захисту населення, вони повинні довести, що відповідні заходи є відповідним та необхідними, і що вони вживаються послідовно та систематично.

Таким чином, сектор грального бізнесу в ЄС є дуже різноманітним, починаючи з монополій (якими керує державний оператор, що контролюється державою, або приватний оператор на основі ексклюзивного права), закінчуючи ліцензійними систем або ними обома. У відповідь на соціальні, технологічні та регулятивні виклики та події, значна кількість держав-членів переглянули або перебувають у процесі перегляду свого законодавства в області азартних ігор. У ході таких переглядів враховуються нові форми азартних ігор, що призвели до збільшення кількості гральних послуг, які пропонуються операторами, уповноваженими у державі-члені ЄС, а також транскордонних пропозицій, не дозволених згідно з національними положеннями держави-члена одержувача.

Сектор грального бізнесу характеризується швидким економічним зростанням і технологічним розвитком. Наприклад, дохід від онлайн-ігор в ЄС у 2015 році становив приблизно 16,5 млрд євро, і очікується, що до 2020 року він зросте приблизно до 25 млрд євро. Дохід від ринку офлайн/фізичних азартних ігор, за оцінками, збільшиться з приблизно 77,5 млрд євро у 2015 році до приблизно 82-84 млрд євро у 2020 році.

За допомогою незаконодавчих заходів, викладених у Повідомленні 2012 року «На шляху до всеосяжної європейської бази для онлайн-ігор» (COM (2012) 596 final), Комісія закликала держави-члени забезпечити високий рівень захисту споживачів, особливо у світлі інформації про ризики, пов’язані з азартними іграми, які включають адиктивні розлади та інші негативні особисті та соціальні наслідки. Зокрема, у Рекомендації щодо принципів захисту споживачів та гравців онлайн-ігор, а також запобігання участі в онлайн-іграх неповнолітніми (2014/478/ЄС) Комісія визначила практики, спрямовані на обмеження соціальної шкоди, деякі з яких можуть бути актуальними для цілей протидії відмиванню коштів, наприклад, процедури реєстрації та верифікації.

Крім того, ефективний нагляд є необхідним для належного виконання цілей державного інтересу. Держави-члени повинні призначити компетентні органи та викласти чіткі настанови для операторів, у тому числі щодо протидії відмиванню коштів. Комісія також підтримує співпрацю між національними регулятивними органами у рамках Угоди про адміністративне співробітництво стосовно онлайн-ігор (підписаної більшістю держав-членів Європейського економічного простору у 2015 році).

Контроль над зростаючою кількістю так званих несанкціонованих пропозицій щодо азартних ігор та їх спрямування в уповноважений регульований сектор грального бізнесу є найбільшими та найскладнішими завданнями регуляторів. На всій території ЄС, за оцінками, мільйони споживачів грають в азартні ігри на несанкціонованих сайтах онлайн-ігор. Тому необхідно підвищити рівень обізнаності щодо ризиків нерегульованих веб-сайтів азартних ігор, наприклад, шахрайство, яке не контролюється на рівні ЄС. Обсяг таких несанкціонованих, як правило онлайн, азартних ігор значно відрізняється між державами-членами, залежно від того, наскільки добре функціонує санкціонований ринок.

Контроль за несанкціонованим ринком та пов’язаними з ним ризиками виходить за межі цього звіту з огляду на те, що неможливо відмити гроші безпосередньо через незаконну діяльність (виграші залишатимуться незаконними). Однак регулятори та зобов’язані суб’єкти мають бути обізнані про онлайн-методи, які дозволяють маскувати справжню особу користувачів та джерела грошових коштів, створюючи при цьому видимість законних операцій і тим самим дозволяючи використовувати гроші у майбутніх операціях на законних ринках.

2. Букмекерська діяльність

Продукт
Букмекерська діяльність (фізичні/офлайн ігри)

Сектор
Сектор грального бізнесу

Загальний опис сектора та відповідного продукту/діяльності

Офлайн або фізичні послуги букмекерської діяльності (включаючи кінські скачки та собачі перегони, ставки на події), що пропонуються у спеціальних санкціонованих торгових точках уповноваженими роздрібними торговцями (які отримують комісію за кожну ставку, але пропонують й інші послуги) або у місцях проведення спортивних змагань (часто доріжки для кінських скачок або собачих перегонів). Сума виграшу може залежати від загальної суми попередньо розміщених ставок (тобто так звані «тоталізаторські системи», тоталізатори (*pari mutuel*) або укладення парі за сукупністю ставок) чи від коефіцієнта виграшу, який узгоджується між букмекером та гравцем (тобто ставки з фіксованими шансами (*pari à la cote*)). Держава-член може мати фіксовану кількість операторів (включаючи єдиного провайдера монополії) або необмежену кількість операторів, якщо вони відповідають певним критеріям. Також може бути встановлена мінімальна та/або максимальна кількість торгових точок на одного ліцензованого провайдера.

Опис сценарію ризиків

Було виявлено три основні сценарії:

(1) злочинець розміщує ставку і обмінює виграш на готівку (конвертація);

(2) злочинець вносить готівку на свій рахунок розміщення ставок та знімає гроші через певний проміжок часу без фактичного розміщення ставок (приховування);

(3) злочинець вносить гроші на рахунок розміщення ставок в одному місці, а співучасник знімає кошти в іншому (приховування, маскування та переказ).

Злочинець може збільшити свої шанси на виграш, розміщуючи ставки на низку подій, що забезпечить більш сприятливі накопичені коефіцієнти, або зменшити ризик програшу шляхом хеджування ставок (тобто розміщуючи ставки на обидва можливі результати однієї події).

Злочинець також може повністю усунути будь-які невизначеності шляхом контактування з переможцем і придбання в нього виграшної ставки.

Загроза

Фінансування тероризму

Оцінка загрози фінансування тероризму, пов'язаної з букмекерською діяльністю, не вважається такою, що має значення. У цьому контексті, загроза фінансування тероризму не є частиною оцінки.

Висновки: не застосовується

Відмивання коштів

Оцінка вразливості до відмивання коштів, пов'язаної з букмекерською діяльністю, свідчить про таке:

- як і у разі всіх інших видів азартних ігор, однією із загроз відмивання коштів, пов'язаних з букмекерською діяльністю, є **ризик проникнення або набуття права власності з боку організованих злочинних груп**.

Рівень цієї загрози є різним, залежно від типу організації, яка приймає ставки. У разі національних монополій на розміщення спортивних ставок, ризик набуття права власності самого оператора букмекерської діяльності майже відсутній. Однак можливо, що окремі роздрібні торговці, на яких покладаються оператори букмекерської діяльності для продажу своїх букмекерських послуг кінцевим споживачам, могли б стати об'єктом проникнення.

Проникнення з боку організованих злочинних організацій у букмекерську діяльність вимагає помірного рівня планування або технічних знань, і головним чином здійснюється за допомогою механізмів, що дозволяють приховувати особу бенефіціарного власника, наприклад, реєстрація активів під іменем третіх осіб (підставні особи).

- Ще однією частою загрозою є **незаконний вплив на результати спортивних змагань**. Розслідування показали, що злочинні групи використовують укмекерську діяльність для отримання доходу від впливу на результати спортивних змагань у ЄС. Спортивні агенти та посередники підкуповують або залякують гравців та/або суддів, щоб забезпечити бажаний результат матчу, тоді як інші агенти вкладають величезні грошові суми в онлайн та офлайн ставки за межами ЄС. У таких випадках незаконний вплив на результати спортивних змагань вимагає контакту (та здійснення грошових переказів) між учасниками азартних ігор, гравцями, керівниками команд та/або суддями. Пов'язаною загрозою є розміщення ставок на фіктивні матчі або події, хоча це більше пов'язано з букмекерською діяльністю онлайн.

- Придбання **виграшних квитків** для забезпечення виграшів може бути ще одним наміром злочинної групи відмити кошті.

<u>Висновок:</u> Правоохоронні органи визначили декілька методів або каналів, які можуть використовуватися організованими злочинними групами у зв'язку з діяльністю, пов'язаною з розміщенням ставок. Крім горизонтальної загрози, яку становить ризик проникнення та набуття права власності, ще одним важливим аспектом є незаконний вплив на результати спортивних змагань. Організовані злочинні групи потребують помірного рівня планування, знань та досвіду для використання цих методів, з огляду на те, що вони вважаються досить привабливими, безпечними та вигідними з фінансової точки зору.

У цьому контексті, рівень загрози відмивання коштів, пов'язаної з розміщенням ставок, вважається дуже <u>значним</u> (рівень 3).

Вразливість

Фінансування тероризму

Оцінка вразливості до фінансування тероризму, пов'язаної з букмекерською діяльністю, не вважається такою, що має значення. У цьому контексті загроза фінансування тероризму не є частиною оцінки.

<u>Висновки</u>: не застосовується

Оцінка вразливості до відмивання коштів, пов’язаної з букмекерською діяльністю, свідчить про таке:

a) схильність до ризику:

Букмекерська діяльність характеризується значними обсягами швидких та анонімних операцій, часто на основі готівкових коштів. Хоча використання готівки зменшується з огляду на альтернативні методи розміщення ставок, вона все ще становить понад 50 % обороту у деяких країнах. Багато гравців, які розміщують ставки, використовують готівку для збереження конфіденційності або з репутаційних причин.

На думку галузевих експертів, можливими тривожними сигналами є:

- ставки, прийняті на крупні грошові суми за надзвичайно малих шансах, які, ймовірно, гарантують віддачу;
- клієнти, які регулярно просять надати їм копії виграшних ставок або квитанцій на виграшні квитки;
- клієнти, які сплачують готівкою і регулярно вимагають виплати виграшів чеком або дебетовою карткою;
- клієнти, які регулярно просять надати їм квитанції, коли забирають виграш з грального автомата.

b) обізнаність про ризики:

- за даними підрозділів фінансової розвідки, букмекерський сектор недостатньо обізнаний про ризики, про що свідчить низька кількість звітів про підозрілі операції, а також їх низька якість.

- вразливість до ризиків відмивання коштів зростає значною мірою в результаті покладання на дистриб’юторські мережі (кіоски, роздрібні торговці, торгові точки), які необов'язково підпадають під дію вимог ПВК/ФТ. За ідентифікацію клієнта відповідають окремі роздрібні торговці, що працюють на оператора букмекерської діяльності, які не завжди здатні виявити підозрілі операції (наприклад, кумулятивні ставки, поділ високих ставок або незвичні ставки), залежно від типу відносин між операторами та роздрібними торговцями. Кількість звітів про підозрілі операції є нерівномірною, і частина сектора все ще недостатньо обізнана про ризики та/або про типи операцій, про які необхідно звітувати (немає узгоджених зобов’язань щодо звітування).

- на думку представників букмекерського сектора, підрозділи фінансової розвідки та інші компетентні органи мають неправильне сприйняття та недостатнє розуміння факторів ризику, притаманних букмекерській діяльності. Складається враження, що у підрозділів фінансової розвідки вже є очікування щодо типу підозр, про які повинен повідомляти оператор азартних ігор (підрозділи фінансової розвідки очікують на підозрілі випадки незаконного впливу на результати спортивних змагань, в той час як оператори схильні повідомляти про невідповідні суми в операції). Оператори букмекерської діяльності страждають від браку зворотної інформації від підрозділів фінансової розвідки стосовно звітів про підозрілі операції.
Крім того, оператори букмекерської діяльності розробляють вимоги щодо ретельної перевірки клієнтів, які можуть зменшити ризики відмивання коштів; деякі оператори букмекерської діяльності накладають вимогу щодо системної ідентифікації переможців (понад певну суму), акцентуючи увагу, наприклад, на бенефіціарному власнику. Вони також можуть пропонувати різні способи виплати виграшів, щоб обмежити використання готівки та використовувати «картки гравців»[101], аби збільшити знання операторів про своїх клієнтів.

[101] «Карти гравців» - це пристрої, які використовуються провайдерами послуг грального бізнесу для відстеження часу та суми ставок, на які грають гравці. Виграші та програші відображаються у формі «балів», які гравці накопичують. Потім «бали» можна обміняти на готівку або товар.

c) законодавча база і перевірки:

Букмекерська діяльність підпадає під дію законодавчої бази ЄС щодо протидії відмиванню коштів, починаючи з Четвертої директиви про боротьбу з відмиванням грошей. Однак, виходячи з принципів мінімальної гармонізації Директиви, все ще можуть мати місце розбіжності між державами-членами в частині регулювання, нагляду за сектором та приведення у виконання норм ПВК/ФТ.

Деякі держави-члени мають законодавство, яке охоплює пов'язані з відмиванням коштів аспекти букмекерської діяльності, та/або спеціальні вимоги у ліцензійних угодах. У таких випадках чинні нормативні акти, як правило, є суворими, коли йдеться про надання дозволу (перевірка основного персоналу на професійну придатність та доброчесність в області ПВК) та виконання поточних зобов'язань щодо звітування. Такі зобов'язання щодо звітування мають виконуватися у разі виникнення будь-якого занепокоєння щодо клієнта, наприклад, знання того, чи є розміщення ставок та програші причиною для занепокоєння щодо ПВК/ФТ, та чи відповідають звички клієнтів грати в азартні ігри їх стилю життя. Це означає, що потрібен ефективний процес внутрішнього звітування, і керівництво та персонал мають бути добре обізнаними з питань ПВК. У цьому відношенні деякі національні законодавства вимагають, щоб сектор букмекерської діяльності проводив галузеву оцінку ризиків, демонструючи здійснення відповідних перевірок та процедур.

Однак компетентні органи все ще занепокоєні тим, як здійснювати перевірки, зокрема, моніторинг розміщення ставок для виявлення ризиків відмивання коштів у режимі реального часу та можливого припинення розміщення ставок у разі підозри. З огляду на характер букмекерської діяльності (включаючи великі обсяги ставок, а іноді розміщення ставок в останню хвилину), складається враження, що визначення точного порядку здійснення належної перевірки клієнтів є проблемою, яка має бути вирішена. Покладання на роздрібних торговців створює додатковий рівень невизначеності в частині належної перевірки клієнтів, з урахуванням того, що деякі пункти продажу не призначені виключно для розміщення ставок і не в змозі здійснювати такі перевірки (наприклад, бари, ресторани, супермаркети, книгарні або АЗС).

Висновок:

Букмекерська діяльність не є однорідною бізнес-моделлю. Що стосується оцінки вразливості, хоча, без сумнівів, на національному рівні деякі оператори букмекерської діяльності добре обізнані про свої ризики відмивання коштів/фінансування тероризму та свої відповідні зобов'язання, все ще незрозуміло, чи здатні вони здійснювати точні та всебічні перевірки з огляду на особливості букмекерської діяльності (значні обсяги швидких та анонімних операцій, часто з використанням готівки). Чинне законодавство або норми, які стосуються ліцензійних умов, можуть бути поліпшені для забезпечення здійснення відповідних перевірок, хоча оцінка вразливості вказує на те, що оператори букмекерської діяльності є більш обізнаними про ризики, оскільки вони вже почали розробляти деякі пом'якшувальні заходи (наприклад, систематичні перевірки у разі перевищення граничного значення або альтернативні платіжні інструменти для обмеження використання готівки).

Явна відсутність розуміння компетентними органами та підрозділами фінансової розвідки стосовно функціонування букмекерської діяльності є ще однією перешкодою для належної оцінки ризиків ПВК/ФТ та надання настанов. Пом'якшення ризиків ПВК/ФТ також ослаблене низьким рівнем зворотного зв'язку з боку підрозділів фінансової розвідки.

У цьому контексті, рівень вразливості до відмивання коштів, пов'язаної з букмекерсбкою діяльністю, вважається <u>значним</u> (рівень 3).

Пом'якшувальні заходи:

1) Для компетентних органів:

- Держави-члени повинні поліпшувати співпрацю між відповідними органами влади (підрозділи фінансової розвідки, правоохоронні органи, поліція, галузеві регулятивні органи, такі як регулятори азартних ігор), аби вони могли краще зрозуміти фактори ризику, пов'язані з букмекерською діяльністю, та надавати ефективні настанови.
- Держави-члени повинні забезпечити регулярну співпрацю між відповідними органами влади та операторами букмекерської діяльності, яка повинна фокусуватися на:
    - посиленні виявлення підозрілих операцій та збільшенні кількості та якості звітів про підозрілі операції;
    - організації навчальних занять для співробітників та службовців з питань нормативно-правового дотримання, приділяючи особливу увагу ризикам проникнення або набуття права власності з боку організованих злочинних груп, та регулярно переглядаючи оцінки ризиків щодо продуктів/бізнес-моделі операторів букмекерської діяльності;
    - забезпеченні того, що органи нагляду надаватимуть чіткіші настанови щодо ризиків ПВК/ФТ, щодо належної перевірки клієнтів та щодо вимог до звітування про підозрілі операції, а також щодо того, як визначати найбільш доцільні показники для виявлення ризиків відмивання коштів;
    - забезпеченні того, що підрозділи фінансової розвідки надаватимуть зворотній зв'язок операторам букмекерської діяльності про якість звіту про підозрілі операції та шляхи поліпшення звітування, а також про те, як використовується інформація, що міститься у звіті, бажано протягом встановленого періоду часу;
    - розробці стандартного(-их) шаблону(-ів) на рівні ЄС для звітів про підозрілі операції або підозрілу діяльність з урахуванням особливостей сектора грального бізнесу.

2) Для сектора:

- Держави-члени повинні забезпечити, що оператори букмекерської діяльності організовуватимуть регулярні навчальні заняття для співробітників, службовців з питань нормативно-правового дотримання та роздрібних торговців, приділяючи особливу увагу ризикам проникнення або набуття права власності з боку організованих злочинних груп, та регулярно переглядаючи оцінки ризиків щодо їх продуктів/бізнес-моделі;
- Європол підписав Меморандум про взаєморозуміння з Глобальною системою моніторингу лотереї (GLMS) щодо обміну інформацією та регулярного консультування стосовно маніпуляцій зі спортивними змаганнями та пов'язаних з ними розслідувань організованої злочинності.
- Європол та держави-члени ЄС тісно співпрацюють із системою виявлення випадків шахрайства у букмекерській діяльності УЄФА, яка здійснює моніторинг понад 30 000 матчів УЄФА та Європи на рік.
- Держави-члени повинні гарантувати, що оператори букмекерської діяльності будуть просувати: і) картки гравців[102] або використання електронних схем ідентифікації з

[102] «Карти гравців» - це пристрої, які використовуються провайдерами послуг грального бізнесу для відстеження часу та суми ставок, на які грають гравці. Виграші та програші відображаються у формі

метою полегшення ідентифікації клієнтів та обмеження використання готівки, та ii) використання систем моніторингу в режимі реального часу для виявлення підозрілих операцій у точках продажу.

- Держави-члени повинні забезпечити, що оператори букмекерської діяльності призначатимуть службовця з питань ПВК у приміщеннях, якщо він ще не призначений.
- Держави-члени повинні забезпечити, що оператори букмекерської діяльності сприятимуть систематичній належній перевірці клієнтів на основі ризику стосовно переможців, а також сприятимуть зниженню граничних значень виграшів за умови належної перевірки клієнтів (наразі 2 000 євро, як передбачено пунктом (d) статті 11 Директиви (ЄС) 2015/849).

3) Для Комісії:

Комісія може надавати настанови щодо пункту (d) статті 11 стосовно здійснення належної перевірки клієнтів у разі здійснення «декількох пов'язаних операцій».

«балів», які гравці накопичують. Потім «бали» можна обміняти на готівку або товар.

3. Бінго

Продукт
Бінго (фізичні/офлайн ігри)

Сектор
Сектор грального бізнесу

Загальний опис сектора та відповідного продукту/діяльності

Офлайн або фізична гра бінго – це азартна гра, в якій гравець використовує табло, яке може бути електронним та мати цифри. У гру бінго грають шляхом відмічання або заповнення цифр, ідентичних тим, що обираються випадковим чином, будь то вручну або електронним способом. Виграє той гравець, який першим відмічає або заповнює «рядок», що має місце тоді, коли випадають усі п'ять цифр в одному горизонтальному рядку на одному табло, або коли гравець першим заповнює «будинок» чи «бінго», коли випадають усі цифри на одному табло.

Призи можуть видаватися у натуральній формі (ваучери), виплачуватися безпосередньо у місці проведення азартної ігри або надаватися у формі грошового призу. Вони також можуть складатися з предметів домашнього вжитку, новинок або продуктів харчування. У деяких державах-членах все-таки можливі обмежені грошові призи, а в інших державах-членах ніщо не заважає провайдерам послуг бінго пропонувати чисто грошові призи. Бінго – це насамперед місцева діяльність, яку здійснюють МСП, яка рідко перетинає національні кордони. Хоча у більшості державах-членах бінго вважається азартною грою, у багатьох інших вона вважається видом лотереї.

Опис сценарію ризиків

Злочинець купує картки – як правило, готівкою – на яких надрукований випадковий набір цифр. Гравці відмічають цифри на своїх картках, які випадковим чином витягує ведучий (найнятий оператором азартних ігор), переможцем стає особа, яка першою відмітила всі свої цифри. Виграшну картку можна придбати за більшу суму, подібно до лотерейного квитка або квитанції з інформацією про ставку.

Загроза

Фінансування тероризму

Оцінка загрози фінансування тероризму, пов'язаної з грою бінго, не вважається такою, що має значення. У цьому контексті, загроза фінансування тероризму не є частиною оцінки.

Висновки: не застосовується

Відмивання коштів

Оцінка загрози відмивання коштів, пов'язаної з грою бінго, свідчить про таке:

- як і для всіх інших азартних ігор, однією із загроз відмиванням коштів, пов'язаних з грою бінго, є **ризик проникнення або набуття права власності з боку організованих злочинних груп**. Рівень загрози, пов'язаної з ризиком проникнення, є різним, залежно від оператора, який організовує гру бінго. Складається враження, що проникнення у бінго має місце тоді, коли вуличні злочинці керують барами, де розіграші бінго не контролюються і їх можна використовувати для цілей відмивання коштів (що робить кошти ліцензованими, незважаючи на те, що вони надходять з незаконного джерела).

- за винятком ризику проникнення, цей сценарій ризику рідко використовується злочинцями для відмивання доходів, одержаних злочинним шляхом, оскільки він є не дуже привабливим з фінансової точки зору, тому що поставлені на карту суми є досить невеликими, а результат незабезпеченим (виграш залежить від випадковості).

Висновки:

Крім горизонтальної загрози проникнення та набуття права власності, бінго не вважається правоохоронними органами та іншими компетентними органами привабливим способом відмивання доходів, одержаних злочинним шляхом. Компонент випадковості у грі бінго робить її досить непривабливою і дуже незабезпеченою. Є кілька показників того, що злочинці мають можливості здатність і намір використовувати гру бінго, але у будь-якому разі, вірогідно, на дуже невеликі суми виграшу.

У цьому контексті, рівень загрози відмивання коштів, пов'язаної з грою бінго, вважається дуже значним (рівень 1).

Вразливість

Фінансування тероризму

Оцінка вразливості до фінансування тероризму, пов'язаної з грою бінго, не вважається такою, що має значення. У цьому контексті, загроза фінансування тероризму не є частиною оцінки.

Висновки: не застосовується

Відмивання коштів

Оцінка вразливості до відмивання коштів, пов'язаної з грою бінго, свідчить про таке:

a) схильність до ризику

Масштаб діяльності, пов'язаної з грою бінго, є досить обмеженим і представляє лише невелику кількість фінансових операцій. Якщо у бінго грають у режимі офлайн, здебільшого використовуються готівкові кошти. У грі використовуються відносно низькі ставки та виграші, при цьому призами часто є товари замість готівки. Гра передбачає дуже низький рівень клієнтів високого ризику та/або зон високого ризику.

b) обізнаність про ризики

Враховуючи відсутність випадків, коли бінго використовується для відмивання доходів, одержаних злочинним шляхом, цей компонент важко оцінити. Так само не вдалося визначити, чи обумовлюється відсутність випадків відмивання коштів високим рівнем обізнаності про ризики відмивання коштів або низьким рівнем намірів злочинних організацій використовувати цей метод.

c) законодавча база і перевірки

Діяльність, пов'язана з грою бінго, підпадаю під дію законодавчої бази ЄС щодо протидії відмиванню коштів, починаючи з Четвертої директиви про боротьбу з відмиванням грошей. Однак, виходячи з принципів мінімальної гармонізації Директиви, між державами-членами все ще можуть мати місце розбіжності в частині регулювання, нагляду за сектором та приведення у виконання норм ПВК/ФТ.

Бінго існує не в усіх державах-членах, але там, де ця гра існує, вона має підпорядковуватися положенням щодо протидії відмиванню коштів. На національному рівні оператори бінго можуть підпорядковуватися нормативно-правовим актам, які стосуються казино, або спеціальним правилам (наприклад, футбольний клуб, який має власний будинок для бінго). Представники сектора бінго зазначили, що встановлено граничні значення для систематичної ідентифікації, що було підтверджено компетентними органами, які схильні підтверджувати проведення ефективних перевірок. Знову ж таки, відносно низький рівень поставлених на карту сум та/або виграшів є фактором у загальній оцінці вразливості.

Висновок: Характеристики гри бінго роблять її дещо вразливою до ризиків відмивання коштів. Гра багато в чому ґрунтується на випадковості, з досить низькими ставками та виграшами (часто у натуральній формі). Хоча використовується здебільшого готівка, ця діяльність не передбачає особливо великих сум ставок. У країнах, де гра бінго є популярною, вона має підпадати під дію положень щодо ПВК/ФТ та підлягати ефективним перевіркам. Компонент обізнаності про ризики не вдалося належним чином оцінити з огляду на відсутність повідомлених випадків. У цьому контексті, рівень вразливості до відмивання коштів вважається <u>незначним</u> (рівень 1).

Пом'якшувальні заходи:

Держави-члени повинні забезпечити, що оператори гри бінго організовуватимуть регулярні навчальні заняття для співробітників та службовців з питань нормативно-правового дотримання, приділяючи особливу увагу ризикам проникнення або набуття права власності з боку організованих злочинних груп, та регулярно переглядаючи оцінки ризиків щодо їх продуктів/бізнес-моделі. З огляду на це держави-члени також повинні продовжувати моніторинг діяльності, пов'язаної з грою бінго, для виявлення можливих майбутніх ризиків.

4. Казино

Продукт
Казино (фізична/офлайн установа)

Сектор
Сектор грального бізнесу

Загальний опис сектора та відповідного продукту/діяльності

У декількох країнах (Бельгія, Чехія, Франція, Люксембург, Португалія та Словаччина) казино (офлайн/фізична установа) визначається як місце, де проводяться азартні ігри (будь то з використанням гральних автоматів або ні) та де проводяться інші культурні та соціальні заходи (театр, ресторани). В інших країнах (Австрія, Данія, Естонія, Фінляндія, Німеччина, Латвія, Мальта, Нідерланди та Швеція) у казино необов'язково проводяться інші соціальні чи культурні заходи, тоді як деякі держави-члени (Данія, Фінляндія, Ірландія та Сполучене Королівство) безпосередньо не визначили поняття казино.

Казино можуть бути державними або приватними, а в деяких державах-членах ліцензію має лише один оператор (Фінляндія, Австрія, Нідерланди та Швеція).

Діяльність казино регулюється законодавством ЄС з питань протидії відмиванню коштів понад 10 років, і хоча державам-членам дозволяється звільнити певні послуги азартних ігор від деяких або всіх вимог, встановлених у Четвертій директиві про боротьбу з відмиванням грошей, після здійснення належної оцінки ризиків, це не стосується казино.

Опис сценарію ризиків

Злочинець купує фішки в казино у спеціальному пункті продажу (за готівку або використовуючи анонімні передплачені картки), і такі фішки можуть використовуватися в найрізноманітніших іграх (з чітко визначеними правилами). Співробітники казино (круп'є) взаємодіють з гравцями у багатьох належним чином регульованих іграх, таких як «Баккара» та «Блекджек». У разі виграшу, гравець отримує фішки за столом, які він має конвертувати назад у готівку у спеціальному пункті продажу (таким чином легітимізуючи незаконні кошти).

Злочинець може використовувати «мулів» або посібників, які купують фішки від його імені за незаконні гроші. Злочинець отримує фішки в казино і обмінює їх на готівку, роблячи вигляд, що він виграв ці фішки в казино.

Злочинець також може скористатися тим, що певні ігри в казино передбачають високу віддачу від ставок (залежно від того, чи мають ставки високий або низький ризик). Два гравці також можуть співпрацювати і одночасно робити ставки на рулетному столі на червоний і чорний колір з лише 3 % шансів втратити накопичені ставки.

Злочинець може також передавати кошти з одного казино в інше (якщо це дозволено законом), надаючи іншому гравцеві доступ до фішок. У таких випадках казино використовуються як фінансові установи, де кошти переказуються з одного рахунка на інший.

Загроза

Фінансування тероризму

Оцінка загрози фінансування тероризму, пов'язаної з діяльністю казино, не вважається такою, що має особливе значення. У цьому контексті, загроза фінансування тероризму не є частиною оцінки.

Висновки: не застосовується

Відмивання коштів

Оцінка загрози відмивання коштів, пов'язаної з діяльністю казино, як і для всіх інших видів ігорної діяльності, вказує на **ризик проникнення або набуття права власності з боку організованих злочинних груп**. Правоохоронні органи зазначили, що казино можуть, зокрема, стикатися із загрозами проникнення. Однак казино, якими керують державні монополії чи державні компанії, є менш схильними до загрози проникнення, з огляду на діючі нормативно-правові положення, які передбачають, наприклад, вимогу щодо прозорості для бенефіціарного права власності. Цей елемент може мати вплив на намір та здатність організованих злочинних груп проникати у діяльність казино. Крім того, зацікавлені сторони зазначили, що національні ліцензійні системи гарантують, що право власності (та будь-які зміни у ньому) регулюється положеннями національного законодавства та нормативно-правових актів. Відповідно до цих законів, національні регулятивні органи здійснюють суворі перевірки на професійну придатність та доброчесність, а також перевірки походження залучених коштів. Ними також можуть бути досвідчені оператори, ключовий персонал та працівники високого рангу. Зацікавлені особи також зазначають, що казино зазвичай мають жорсткі системи для запобігання шахрайству та захисту від будь-якої злочинної діяльності. Тим не менш, правоохоронні органи в цілому вважають, що казино є найбільш використовуваним каналом для відмивання коштів за допомогою азартних ігор, хоча діяльність казино підпадає під дію попереднього законодавства ЄС щодо протидії відмиванню коштів.

Висновки: **Вважається, що казино є схильними до загрози проникнення, хоча що стосується казино, які належать державі або державним компаніям, цей рівень ризику є нижчим. Тим не менш, правоохоронні органи все ще вважають казино найбільш використовуваним каналом відмивання коштів за допомогою азартних ігор. Отже, ризик використання казино для відмивання коштів є високим, а рівень загрози відмивання коштів через казино, вважається дуже <u>значним</u> (рівень 4).**

Вразливість

Фінансування тероризму

Оцінка вразливості до фінансування тероризму, пов'язаної з діяльністю казино, не вважається такою, що має значення. У цьому контексті, вразливість до фінансування тероризму не є частиною оцінки.

Висновки: не застосовується

Відмивання коштів

Оцінка вразливості до відмивання коштів вказує на те, що ринок є різним в різних державах-членах.

a) схильність до ризику

Хоча цей сектор розробив альтернативні способи оплати, на практиці використання готівки є важливим, і цей сектор може за певних обставин стикатися з клієнтами високого ризику (впливові політичні особи або ті, хто походить з третіх країн високого ризику). Крім того, казино характеризуються високим обсягом фінансових операцій з огляду на велику кількість азартних ігор, які воно організовує.

b) обізнаність про ризики

Включення казино до переліку зобов'язаних суб'єктів раніше у законодавстві ЄС щодо протидії відмиванню коштів сприяє підвищенню обізнаності сектора про ризики. Наприклад, вже існуюча законодавча база для казино заохочує здійснювати навчання персоналу та покращувати перевірки. Співробітники казино регулярно інформуються та проходять навчання з питань ідентифікації, моделей та поведінки, що становлять загрозу відмивання коштів. Такі навчальні заняття включають, наприклад, заходи та інструкції щодо поводження з готівкою. Багато фізичних казино розробили системи інспекцій та перевірок зовнішніми та незалежними інститутами тестування, які зменшують вразливість до відмивання коштів та злочинної діяльності. Більше того, переважна більшість фізичних казино має систему відеоспостереження, яка здійснює нагляд за зонами, де здійснюються операції. Деякі процедури належної перевірки клієнтів здійснюються автоматично у ході процесу ідентифікації: ідентифікація усіх відвідувачів перед тим, як потрапити в казино, ідентифікація відвідувачів перед придбанням фішок/квитків та ідентифікація після досягнення певного грошового граничного значення, який у більшості випадків становить 2 000 євро, як передбачено Четвертою директивою про боротьбу з відмиванням грошей, але може бути і нижчим. Деякі казино можуть прийняти рішення не ідентифікувати клієнта, що перевищує певне граничне значення, якщо особа була ідентифікована іншими засобами (тобто при вході у казино або при купівлі фішок). Розширена належна перевірка клієнтів може застосовуватися для заздалегідь визначених критеріїв високого ризику, таких як конкретні грошові суми, операції або структурування операцій.

На думку деяких компетентних органів та підрозділів фінансової розвідки, деякі недоліки все ще залишаються в частині заходів належної перевірки клієнтів (які недостатньо розуміються сектором) та їх застосування, які у жодному разі не вважаються задовільними органами нагляду: наприклад, коли здійснюються перевірки ідентифікаційних карток, але вимоги щодо ведення документації не виконуються або виконуються неналежним чином; коли належна перевірка клієнта здійснюється, коли він входить у казино, але не тоді, коли він купує фішки. Однак, хоча рівень звітування про підозрілі операції є різним у різних державах-членах, низька кількість таких звітів є виправданою, оскільки цей сектор вважається регульованим та взагалі добре контрольованим. Вимога щодо отримання схвалення вищого органу для здійснення будь-яких операцій високого ризику вважається такою, що обмежує ризик проникнення.

Що стосується звітів про підозрілі операції, зацікавлені особи підкреслили відсутність зворотного зв'язку від підрозділів фінансової розвідки. Вони також наголосили на тому, що якість звітування може покращитися, якщо підрозділи фінансової розвідки надаватимуть настанови та зворотній зв'язок, бажано протягом встановленого періоду часу. Відсутність зворотного зв'язку від підрозділів фінансової розвідки щодо поданих звітів в окремих випадках спричиняє труднощі для казино (коли незрозуміло, чи мають бути кошти виплачені гравцю, який, у свою чергу, може вжити заходів проти казино) та перешкоджає покращенню практики протидії відмиванню коштів загалом.

c) законодавча база і перевірки

Включення казино до переліку зобов'язаних суб'єктів у Четвертій директиві про боротьбу з відмиванням грошей, а також у попередньому законодавстві ЄС щодо ПВК, безумовно, підвищує якість здійснюваних перевірок. Складається враження, що в цілому казино справляються з потребою у наявності кількох шарів перевірок, розуміючи, що в казино можуть здійснюватися кілька видів азартних ігор.

З точки зору компетентних органів, перевірки на професійну придатність та доброчесність пом'якшують основну вразливість для казино, тобто проникнення. Власники (акціонери), працівники високого рангу та ключовий персонал систематично перевіряються операторами казино, що дає досить ефективні гарантії від ризиків проникнення. Незважаючи на цілком непогану загальну картину, правоохоронні органи все ще виявляють деякі недоліки, що свідчить про те, що чинна законодавча база застосовується неправильно. Кількість випадків відмивання коштів, розслідуваних правоохоронними органами, схоже, вказує на те, що ще є над чим працювати.

Висновки:

Незважаючи на те, що схильність до ризику залишається досить високою (значна кількість фінансових операцій на основі готівки), включення казино до законодавчої бази з питань ПВК на понад 10 років підвищило рівень обізнаності сектора про вразливість до відмивання коштів. Перевірки стали більш ефективними, а персонал краще підготовленим. Однак деякі недоліки залишаються в частині виконання вимог щодо ПВК/ФТ, зокрема вимог щодо належної перевірки клієнтів. Рівень звітування є різним у різних державах-членах, що може бути пов'язано з належним рівнем нагляду. У цьому контексті, рівень вразливості до відмивання коштів, пов'язаної з казино, вважається помірно значним (рівень 2)

Пом'якшувальні заходи:

1) Для компетентних органів:

- Держави-члени повинні покращувати співпрацю між відповідними органами (підрозділи фінансової розвідки, правоохоронні органи, поліція, галузеві регулятивні органи, такі як регулятори азартних ігор), аби вони могли краще зрозуміти фактори ризику, притаманні діяльності казино, та надавати ефективні настанови.

- Держави-члени повинні забезпечити регулярну співпрацю між відповідними органами та казино, яка має фокусуватися на:

- посиленні виявлення підозрілих операцій та збільшенні кількості та якості звітів про підозрілі операції;
- організації навчальних занять для співробітників та службовців з питань нормативно-правового дотримання, з приділенням особливої уваги ризикам проникнення або набуття права власності з боку організованих злочинних груп, та регулярно переглядаючи оцінки ризиків щодо продуктів/бізнес-моделі операторів букмекерської діяльності;
- забезпеченні того, що органи нагляду надаватимуть чіткіші настанови щодо ризиків ПВК/ФТ, щодо належної перевірки клієнтів та щодо вимог до звітування про підозрілі операції, а також щодо того, як визначити найбільш відповідні показники для виявлення ризиків відмивання коштів;
- забезпеченні того, що підрозділи фінансової розвідки надаватимуть зворотній зв'язок казино про якість звітування про підозрілі операції та шляхи поліпшення звітування, а також про те, як використовується надана у звіті інформація, бажано протягом встановленого періоду часу;
- розробці стандартних шаблонів на рівні ЄС для звітів про підозрілі операції або про підозрілу діяльність з урахуванням особливостей сектора грального бізнесу;
- рекомендуванні не видавати сертифікати на виграшні квитки в казино.

- Держави-члени повинні вимагати від компетентних органів надання звіту про те, чи ефективно казино застосовують режим ПВК/ФТ, зокрема, щодо ефективності перевірок, які здійснюються через системи відеоспостереження, а також ефективності належної перевірки клієнтів на основі граничного значення.

2) <u>Для сектора:</u>

- Держави-члени повинні забезпечити, що казино організовуватимуть регулярні навчальні заняття для співробітників та службовців з питань нормативно-правового дотримання, приділяючи особливу увагу ризикам проникнення або набуття права власності з боку організованих злочинних груп, та регулярно переглядаючи оцінки ризиків щодо їх продуктів/бізнес-моделі;
- Держави-члени повинні гарантувати, що казино будуть просувати: і) картки гравців[103] або використання електронних схем ідентифікації з метою полегшення ідентифікації клієнтів та обмеження використання готівки, та іі) використання систем моніторингу в режимі реального часу для виявлення підозрілих операцій.
- Держави-члени повинні забезпечити, що казино призначатимуть службовця з питань ПВК у приміщеннях, якщо він ще не призначений.
- Держави-члени повинні забезпечити, що оператори казино сприятимуть систематичній належній перевірці клієнтів на основі ризику стосовно переможців, а також сприятимуть зниженню граничних значень виграшів за умови належної перевірки клієнтів (наразі 2 000 євро, як передбачено пунктом (d) статті 11 Директиви (ЄС) 2015/849).

3) <u>Для Комісії:</u>

[103] «Карти гравців» - це пристрої, які використовуються провайдерами послуг грального бізнесу для відстеження часу та суми ставок, на які грають гравці. Виграші та програші відображаються у формі «балів», які гравці накопичують. Потім «бали» можна обміняти на готівку або товар.

Комісія може надавати настанови щодо пункту (d) статті 11 стосовно здійснення належної перевірки клієнтів у разі здійснення «декількох пов'язаних операцій.

5. Гральні автомати (за межами казино)

Продукт
Гральні автомати (фізичні/офлайн та зовнішні казино)

Сектор
Сектор грального бізнесу

Загальний опис сектора та відповідного продукту/діяльності

Гральні автомати (офлайн) на основі генератора випадкових чисел зазвичай поділяються на кілька підкатегорій, залежно від максимальної ставки, максимального виграшу або типу приміщення, в якому може бути розміщений гральний автомат. Існує різниця між традиційними гральними автоматами («фруктові машини») і терміналами відео-лотереї, які підключені до центрального терміналу і пропонують більш широкий спектр ігор.

Ринок гральних автоматів за межами казино в ЄС є різним у різних державах-членах (або регіонах, оскільки на цьому рівні можуть надаватися дозволи та забезпечуватися контроль). У деяких державах-членах гральні автомати не можуть розташовуватися за межами казино, тоді як в інших дозволені лише автомати з низькими ставками та маленьким виграшем.

У деяких державах-членах гральні автомати можна знайти у різноманітних приміщеннях, таких як пункти прийому ставок, аркади, бари та кафе. Такі термінали приймають готівку та надають квитанцію, представляючи докази стосовно джерела грошей. Там, де дозволені гральні автомати, вони можуть підпорядковуватися суворим положенням щодо фіксованих ставок та обмеженням щодо гральних опцій. Однак гравець може мати можливість взаємодіяти більш вільно (наприклад, термінали для ставок з фіксованими шансами, у формі електронної рулетки, де гравець може обирати кількість опцій та змінювати ставки).

Опис сценарію ризиків

Злочинець вносить незаконні кошти (готівку) у гральні автомати або використовує їх (її) для придбання жетонів для автоматів. Деякі гральні автомати також дозволяють поставити на карту лише невелику частину (внесеної) суми, тоді злочинець може вимагати виплати решти коштів на банківський рахунок або готівкою з квитанцією (тим самим надаючи можливість для легітимізації більшої суми, ніж та, на яку була здійснена азартна гра).

Злочинець використовує електронну рулетку для відмивання коштів, роблячи однакові ставки як на червоний, так і на чорний, а також меншу ставку на 0; переважна частина ставки ніколи не буде втрачена, оскільки шанси представляють 50/50, і будуть надані квитанції, що підтверджують виграш. Більше того, ваучери «Ticket In Ticket Out» (TITO)[104] з автоматів у казино, аркад чи пунктів прийняття ставок можуть використовуватися для відмивання коштів та конвертуватися у готівку пізніше або третіми особами.

[104] Ваучери «Ticket in, ticket out (TITO)» використовуються у гральних автоматах, розташованих у казино, для друку аркуша паперу зі штрих-кодом із зазначенням відповідної грошової суми. Вони, у свою чергу, можуть бути погашені за готівку в автоматизованому кіоску.

Злочинець може здійснювати операцію декілька разів та/або на кількох майданчиках, щоб мінімізувати підозру та обійти обмеження щодо розміру ставки або тривалості гри.

Загроза

Фінансування тероризму

Оцінка загрози фінансування тероризму, пов'язаної з використанням гральних автоматів, не вважається такою, що має значення. У цьому контексті, загроза фінансування тероризму не є частиною оцінки.

Висновки: не застосовується

Відмивання коштів

Оцінка загрози відмивання коштів, пов'язаної з використанням гральних автоматів, як і для всіх інших видів діяльності в області азартних ігор, вказує на **ризик проникнення або набуття права власності з боку організованих злочинних груп**. Однак, згідно з розслідуваннями правоохоронних органів, випадки є досить рідкісними або не повідомляються. Це не вважається життєздатним та привабливим з фінансової точки зору методом, оскільки шанс виграти великі суми є порівняно низьким (результат, оснований на випадковості, часто із низькими ставками та низьким виграшем), хоча у разі використання деяких машин існують способи збільшити шанси на перемогу або навіть уникнути гри і просто внести гроші, після чого негайного їх зняти.

Висновки: Гральні автомати не є привабливим способом відмивання коштів з огляду на характерний елемент випадковості, низьку суму ставок та виграшу у поєднанні з часом та зусиллями, необхідними для відмивання будь-яких значних грошових сум. Однак деякі типи гральних автоматів дозволяють вносити більші ставки та/або забезпечують більший виграш; вони також можуть дозволяти злочинцю внести лише невелику частину суми, вимагаючи виплати решти коштів (на банківський рахунок або готівкою з квитанцією). У цьому контексті, хоча рівень загрози відмивання коштів може бути різним для різних типів гральних автоматів (низькі/високі ставки та/або виграші), як правило, він вважається <u>помірно значним</u> (рівень 2).

Вразливість

Фінансування тероризму

Оцінка вразливості до фінансування тероризму, пов'язаної з використанням гральних автоматів, не вважається такою, що має значення. У цьому контексті, вразливість до фінансування тероризму не є частиною оцінки.

Висновки: не застосовується

Відмивання коштів

Оцінка вразливості до відмивання коштів, пов'язаної з використанням гральних автоматів, свідчить про таке:

a) схильність до ризику

Гральні автомати (фізичні) здебільшого використовують готівку. Суми операцій різняться, як правило, досить низькі, але деякі автомати пропонують можливість розміщення більшої суми.

b) обізнаність про ризики

Для гральних автоматів, розташованих за межами казино, рівень обізнаності щодо ризику є різним в різних державах-членах, і здається, що незалежні оператори гральних автоматів менш обізнані зі своїми зобов'язаннями щодо ПВК/ФТ, оскільки вони є менш організованими, порівняно з операторами у фізичних казино.

Крім того, компетентні органи помітили новий ризик, пов'язаний з терміналами відео-лотереї, які зумовлюють зростаючу кількість звітів про підозрілі операції (адже загалом виграші знову вводяться у темну економіку).

c) законодавча база і засоби контролю

Гральні автомати охоплюється законодавчою базою ЄС щодо протидії відмиванню коштів, починаючи з Четвертої директиви про боротьбу з відмиванням грошей. Однак, виходячи з принципів мінімальної гармонізації Директиви, між державами-членами все ще можуть мати місце розбіжності в частині регулювання, нагляду та приведення у виконання норм ПВК/ФТ. Деякі держави-члени прийняли рішення регулювати цей сектор, якщо він працює окремо від казино. За даними компетентних органів та підрозділів фінансової розвідки, рівень перевірок є недостатнім, а рівень санкцій є недостатньо переконливим (наприклад, букмекер у державі-члені X отримав штраф у розмірі понад 100 000 євро за нездатність торговця запобігти відмиванню понад 1 млн євро у його точках продажу). Однак наразі оператори гральних автоматів розробляють деякі пом'якшувальні заходи, наприклад, забороняють виплачувати виграші у грошовій формі, якщо вони перевищують певну суму.

Висновки:
Що стосується гральних автоматів, розташованих за межами казино, перевірки не є ефективними і рівень звітування про підозрілі операції є досить низьким, хоча пом'якшувальні заходи для обмеження готівкових платежів, як правило, обмежують ризик відмивання коштів. Навіть якщо суми ставок та виграшів часто є відносно низькими, гральні автомати дозволяють здійснювати швидкі та анонімні (а також повторні) операції, часто на основі готівки. Операції також можуть здійснюватися на кількох майданчиках, щоб мінімізувати підозри та обійти обмеження щодо розміру ставок або тривалості гри. У цьому контексті, рівень вразливості до відмивання коштів, пов'язаної з використанням гральних автоматів, вважається помірно значним (рівень 2).

Пом'якшувальні заходи:

1) Для компетентних органів
   - Держави-члени повинні покращувати співпрацю між відповідними органами влади (підрозділи фінансової розвідки, правоохоронні органи, поліція, галузеві регулятивні органи, такі як регулятори азартних ігор), аби вони могли краще зрозуміти фактори ризику, пов'язаного з використанням гральних автоматів, та надати ефективні настанови.
   - Держави-члени повинні забезпечити регулярну співпрацю між відповідними органами та операторами гральних автоматів, яка повинна фокусуватися на:
     - посиленні виявлення підозрілих операцій та збільшенні кількості та якості звітів про підозрілі операції;
     - організації навчальних занять для співробітників та службовців з питань нормативно-правового дотримання, приділяючи особливу увагу ризикам проникнення або набуття права власності з боку організованих злочинних груп, та регулярно переглядаючи оцінки ризиків;
     - забезпеченні того, що органи нагляду надаватимуть чіткіші настанови щодо ризиків ПВК/ФТ, щодо належної перевірки клієнтів та щодо вимог до звітування про підозрілі операції, а також щодо того, як визначати найбільш доцільні показники для виявлення ризиків відмивання коштів;
     - забезпеченні того, що органи нагляду надаватимуть більш чіткі рекомендації щодо нових ризиків, пов'язаних з використанням терміналів відео-лотереї;
     - забезпеченні того, що підрозділи фінансової розвідки надаватимуть зворотній зв'язок операторам гральних автоматів про якість звіту про підозрілі операції та шляхи поліпшення звітування, а також про те, як використовується надана у звіті інформація, бажано протягом встановленого періоду часу;
     - розробці стандартного(-их) шаблону(-ів) на рівні ЄС для звітів про підозрілі операції або підозрілу діяльність з урахуванням особливостей сектора грального бізнесу.

2) Для сектора
   - Держави-члени повинні забезпечити, що оператори гральних автоматів організовуватимуть регулярні навчальні заняття для співробітників, службовців з питань нормативно-правового дотримання та роздрібних торговців, приділяючи особливу увагу ризикам проникнення або набуття права власності з боку організованих злочинних груп, та регулярно переглядаючи оцінки ризиків щодо їх продуктів/бізнес-моделі;
   - Держави-члени повинні гарантувати, що оператори гральних автоматів будуть просувати: і) картки гравців[105] або використання електронних схем ідентифікації з метою полегшення ідентифікації клієнтів та обмеження використання готівки, та іі) використання систем моніторингу в режимі реального часу для виявлення підозрілих операцій у точках продажу;

[105] «Карти гравців» - це пристрої, які використовуються провайдерами послуг грального бізнесу для відстеження часу та суми ставок, на які грають гравці. Виграші та програші відображаються у формі «балів», які гравці накопичують. Потім «бали» можна обміняти на готівку або товар.

- Держави-члени повинні забезпечити, що оператори грального автоматів призначатимуть службовця з питань ПВК у приміщеннях, якщо він ще не призначений.
  Держави-члени повинні забезпечити, що оператори грального автоматів сприятимуть систематичній належній перевірці клієнтів на основі ризику стосовно переможців, а також сприятимуть зниженню граничних значень виграшів за умови належної перевірки клієнтів (наразі 2 000 євро, як передбачено пунктом (d) статті 11 Директиви (ЄС) 2015/849).

3) Для Комісії

Комісія може надавати настанови щодо пункту (d) статті 11 стосовно здійснення належної перевірки клієнтів у разі у разі здійснення «декількох пов'язаних операцій».

6. Лотереї

Лотереї

Сектор
Сектор грального бізнесу

Загальний опис сектора та відповідного продукту/діяльності

Лотереї охоплюють широкий спектр цифрових ігор, коли переможець обирається випадково. Лотереї бувають різними – починаючи з національних лотерей, яким надається ексклюзивна ліцензія на проведення лотерейних ігор на території держави-члена (державні та приватні оператори, як комерційні, так і некомерційні, які діють від імені держави), до дрібних благодійних лотерей, які приносять доходи як для суспільної користі, так і для неприбуткових організацій (наприклад, благодійні організації, громадянське суспільство, спорт, культура, спадщина, соціальне забезпечення). Визначення лотереї – або вимог для отримання ліцензії – є різним у різних державах-членах.

Квитки національної лотереї зазвичай продаються через агентів за готівку або шляхом здійснення операцій з картками чи безпосередньо гравцю у режимі онлайн. У більшості випадків грають на невеликі суми. Переможці можуть обиратися миттєво (наприклад, «скретч-карти») або за результатами щотижневих розіграшів (найчастіше рекламованих і телевізійних). Виграші виплачуються агентами при пред'явленні виграшного квитка (невеликі суми) або безпосередньо перераховуються на банківський рахунок гравця (крупні суми та джекпоти). Віддача від ставок зазвичай є нижчою, ніж для інших продуктів азартних ігор, оскільки метою є збирання коштів на суспільне благо (40-50 % зібраних коштів, як правило, повертаються у формі виграшу – але є приклади, коли віддача є вищою. Шанс виграти джекпот є дуже низьким (наприклад, вірогідність коливається у межах одного зі 140 мільйонів для джекпота 1-го раунду у мільйонах євро).

Опис сценарію ризиків

Відносно низька віддача для гравців робить пряму купівлю лотерейних квитків затратною і непривабливою формою відмивання коштів. Тому купівля лотерейних квитків безпосередньо для виграшу призу не вважається можливим сценарієм ризику. Навпаки, метод придбання виграшного квитка – коли злочинець купує лотерейний квиток у переможця (можливо, шляхом

змови з торговим агентом) та конвертує приз у готівку з видачею квитанції – є більш життєздатним сценарієм, про який повідомляють правоохоронні органи.

Загроза

Фінансування тероризму

Оцінка загрози фінансування тероризму, пов'язаної з лотереями, не вважається такою, що має значення. У цьому контексті, загроза фінансування тероризму не є частиною оцінки.

Висновки: не застосовується

Відмивання коштів

Оцінка загрози, пов'язаної з відмиванням коштів за допомогою лотереї, свідчить про таке:

- як і для всіх інших азартних ігор, **існує ризик проникнення або набуття права власності з боку організованих злочинних груп**. У разі державних лотерей ризик здається мінімальним, але зростає на рівні роздрібної торгівлі.

- Для інших типів загроз, за даними правоохоронних органів, злочинці мають лише невиразні наміри використовувати лотереї для відмивання доходів, одержаних злочинним шляхом. Правоохоронні органи виявили декілька випадків, коли, наприклад, виграшні квитки були виявлені разом з готівкою або наркотиками в результаті конфіскації. Однак, у разі використання, цей сценарій може дозволити зібрати великі суми готівкових коштів (наприклад, 1,2 млн євро були зібрані за допомогою виграшних квитків згідно з нещодавнім розслідуванням). Однак потрібні певні навички планування і технічні знання, що в цілому вимагає співучасті оператора лотереї та використання підставних осіб. Це може обмежити намір злочинців використовувати цей сценарій ризику. Лотереї також пропонують менше можливостей для відмивання коштів з огляду на меншу частоту розіграшів, низькі середні ставки та виграші (миттєві квитки та чисельні ігри та низький коефіцієнт виплат). Взагалі, лотереї як такі не були б особливо привабливими для відмивання доходів, одержаних злочинним, з огляду на відносно низьку віддачу (лише 50 % від продажу квитків використовується для призів).

Висновки: Є повідомлення про випадки, коли лотереї використовуються для відмивання доходів, отриманих злочинним шляхом. Однак це вимагає планування та експертних знань, що може обмежувати намір та здатність організованих злочинних груп використовувати цей метод. Однак метод придбання виграшних квитків є більш життєздатним сценарієм. У цьому контексті, рівень загрози відмивання коштів, пов'язаної з лотереями, вважається помірно значним (рівень 2).

Вразливість

Фінансування тероризму

Оцінка вразливості до фінансування тероризму, пов'язаної з лотереями, не вважається такою, що має значення. У цьому контексті загроза фінансування тероризму не є частиною оцінки.

Висновки: не застосовується

Відмивання коштів

Оцінка вразливості до відмивання коштів, пов'язаної з лотереями, свідчить про таке:

a) схильність до ризику

Оцінюючи рівень схильності до ризику, також враховується, що в багатьох державах-членах лотереями керує державна монополія. Виплати вищих сум виграшу підлягають суворому контролю, і більшість операторів лотерей обмежують призи, які можуть виплачуватися роздрібними торговцями. Основні призи обмінюються на готівку у штаб-квартирі лотереї та/або банках (за договірною угодою між оператором та обраним банком) відповідно до суворих процедур верифікації як чинності заявки на одержання виграшу, так і особи переможця. Однак виграші нижче певного граничного значення (тобто невеликі суми), які є різними у різних державах-членах, виплачуються безпосередньо торговими агентами/уповноваженими дистриб'юторами. Крім того, анонімність гравця у багатьох державах-членах є гарантованою, що ускладнює злочинцям ідентифікацію власника виграшного квитка з метою його придбання для злочинних цілей, якщо їм активно не допомагають співучасники.

b) обізнаність про ризики

Хоча зловживання лотерейних ігор шляхом придбання виграшних квитків є головним занепокоєнням підрозділів фінансової розвідки та правоохоронних органів (включаючи доволі часто змову з агентами з продажу), загальний рівень обізнаності досить важко оцінити. Незважаючи на те, що ідентифікація гравців підпадає під прямий контроль роздрібних торговців, які працюють за дозволом оператора, з накладенням на них певних санкцій, було зазначено, що оператори лотерей здійснюють активний контроль над уповноваженими роздрібними торговцями та координують навчальні програми для роздрібних торговців щодо підвищення обізнаності про ПВК/виявлення випадків відмивання коштів.

c) законодавча база і перевірки

Лотереї охоплюються законодавчою базою ЄС щодо протидії відмиванню коштів, починаючи з Четвертої директиви про боротьбу з відмиванням грошей. Однак, виходячи з принципів мінімальної гармонізації Директиви, між державами-членами все ще можуть мати місце розбіжності в частині регулювання, нагляду за сектором та приведення у виконання норм ПВК/ФТ.

Проте на національному рівні нагляд з боку компетентних органів працює добре і зазвичай здійснюється державними органами. Наприклад, було зазначено, що більшість ігорних органів вже ввели рекомендовані процедури та перевірки, щоб утримати злочинців від використання лотерейних інструментів для відмивання коштів. Крім того, оператори лотерей встановили внутрішні перевірки та посилили пильність у цих питаннях. Наприклад, у більшості державах-членах вже встановлена процедура верифікації особи переможця джекпота, коли приз перевищує задане граничне значення.

Висновки: Виходячи з оцінки вразливості, виявляється, що лотереї як такі не є життєздатним сценарієм ризику, але ризики більше пов'язані з (придбанням) виграшними квитками. Чинна національна законодавча база запровадила заходи щодо перевірки особи переможців, зокрема тих, хто має високі виграші. Тим не менш, сценарій ризику (придбання) виграшних квитків залишається головною проблемою. У цьому контексті, рівень вразливості до відмивання коштів, пов'язаної з лотереями, вважається помірно значним (рівень 2).

Пом'якшувальні заходи:

1) Для компетентних органів:

- Держави-члени повинні покращувати співпрацю між відповідними органами влади (підрозділи фінансової розвідки, правоохоронні органи, поліція, галузеві регулятивні органи, такі як регулятори азартних ігор), аби вони могли краще зрозуміти фактори ризику, пов'язаного з лотереями, та надати ефективні настанови.
- Держави-члени повинні забезпечити регулярну співпрацю між відповідними органами та операторами гральних автоматів, яка повинна фокусуватися на:
    - посиленні вимог до належної перевірки клієнтів та виявленні підозрілих операцій, особливо у контексті виграшних квитків, а також збільшенні кількості та якості звітів про підозрілі операції;
    - організації навчальних занять для співробітників та службовців з питань нормативно-правового дотримання, приділяючи особливу увагу ризикам проникнення або набуття права власності з боку організованих злочинних груп, та регулярно переглядаючи оцінки ризиків щодо їх продуктів/бізнес-моделі;
    - забезпеченні того, що органи нагляду надаватимуть чіткіші настанови щодо ризиків ПВК/ФТ, щодо належної перевірки клієнтів та щодо вимог до звітування про підозрілі операції, а також щодо того, як визначати найбільш доцільні показники для виявлення ризиків відмивання коштів;
    - забезпеченні того, що підрозділи фінансової розвідки надаватимуть зворотній зв'язок операторам лотереї про якість звіту про підозрілі операції та шляхи поліпшення звітування, а також про те, як використовується надана у звіті інформація, бажано протягом встановленого періоду часу;
    - розробці стандартного(-их) шаблону(-ів) на рівні ЄС для звітів про підозрілі операції або підозрілу діяльність з урахуванням особливостей сектора грального бізнесу.

2) Для сектора:

- Держави-члени повинні забезпечити, що оператори лотерей організовуватимуть регулярні навчальні заняття для співробітників, службовців з питань нормативно-правового дотримання та роздрібних торговців, приділяючи особливу увагу ризикам проникнення або набуття права власності з боку організованих злочинних груп, та регулярно переглядаючи оцінки ризиків щодо їх продуктів/бізнес-моделі. Навчання також буде включати елементи, пов'язані з відповідними тривожними сигналами щодо повторних виграшів.

- Держави-члени повинні гарантувати, що лотереї будуть сприяти: і) використанню систем для систематичної ідентифікації переможців, наприклад, картки гравців[106] або електронні схеми ідентифікації з метою полегшення ідентифікації клієнтів, та іі) використанню переказів коштів на основі рахунків для виплат крупних сум;
- Держави-члени повинні заохочувати операторів лотереї призначити службовця з питань ПВК у приміщеннях, якщо він ще не призначений.
- Держави-члени повинні забезпечити, що оператори букмекерської діяльності сприятимуть систематичній належній перевірці клієнтів на основі ризику стосовно переможців, а також сприятимуть зниженню граничних значень виграшів за умови належної перевірки клієнтів (наразі 2 000 євро, як передбачено пунктом (d) статті 11 Директиви (ЄС) 2015/849).

3) Для Комісії:

Комісія може надавати настанови щодо пункту (d) статті 11 стосовно здійснення належної перевірки клієнтів у разі у разі здійснення «декількох пов'язаних операцій».

7. Покер

Продукт
Покер (фізична/офлайн гра)

Сектор
Сектор грального бізнесу

Загальний опис сектора та відповідного продукту/діяльності

Загальний опис сектора (розмір) та статистичні дані, а також відповідного продукту/діяльності

Покер – це карткова гра, яка передбачає процедури здійснення ставок та в якій переможець кожного раунду визначається відповідно до комбінацій карт гравців, принаймні деякі з яких залишаються прихованими до кінця гри, та ставок.

Покер організовується приватними операторами або державними провайдерами послуг грального бізнесу в ліцензованих приміщеннях (таких як казино), приватних клубах або у мережі онлайн (залежно від національного законодавства). Він організовується як турнір, в якому гравець бере участь, сплачуючи фіксований внесок на початку гри, і отримує певну кількість фішок для гри в покер (переможцем турніру, як правило, стає особа, яка виграє кожну фішку на турнірі), або як настільна гра, в якій гравець може купувати більше фішок у процесі гри. На відміну від багатьох інших продуктів грального бізнесу, учасники грають один проти одного, а не проти організатора заходу. Організатор отримує фіксовану суму обороту (ставок) або виграш.

[106] «Карти гравців» - це пристрої, які використовуються провайдерами послуг грального бізнесу для відстеження часу та суми ставок, на які грають гравці. Виграші та програші відображаються у формі «балів», які гравці накопичують. Потім «бали» можна обміняти на готівку або товар.

У покер також можна грати у приватних клубах (*cercles de jeux*), які існують у деяких юрисдикціях, але заборонені в інших, а турніри можуть організовуватися за межами казино.

Опис сценарію ризиків

Злочинець купує фішки в казино (або у відповідних ліцензованих приміщеннях) у спеціалізованій точці продажу (за готівку чи використовуючи анонімні передплачені картки), і ці фішки можуть бути передані іншому гравцеві шляхом понесення навмисних втрат (здавання виграшної комбінації для забезпечення отримання фішок співучасником). Фішки обмінюються на готівку або передаються клієнту в інший спосіб.

Злочинець (організовані злочинні групи) також може проникати в організаційну структуру ліцензованих приміщень, де організовуються ігри в покер або турніри (наприклад, казино чи приватні клуби) або прямо чи опосередковано подавати заявку на отримання ліцензії на організацію покерного турніру, участь в якому може бути відкритою або лише за запрошенням.

Загроза

Фінансування тероризму

Оцінка загрози фінансування тероризму, пов'язаної з грою в покер, не вважається такою, що має значення. У цьому контексті, загроза фінансування тероризму не є частиною оцінки.

Висновки: не застосовується

Відмивання коштів

Оцінка загрози відмивання коштів, пов'язаної з грою в покер, свідчить про таке:

- як і для всіх інших азартних ігор, **існує ризик проникнення або набуття права власності з боку організованих злочинних груп**.

- цей канал вважається досить привабливим, хоча він вимагає помірного рівня планування (співучасті) або технічних знань (сама стратегія ігри), щоб використовувати незаконні турніри або свідомо програвати, аби зміг виграти співучасник.

Висновки: Крім ризику того, що компанія, яка володіє ліцензією на організацію покерних ігор або турнірів у фізичних приміщеннях, може стати об'єктом проникнення (що становить горизонтальну загрозу, яка також є чинною для інших провайдерів гральних послуг), у деяких державах-членах існує можливість організовувати індивідуальні турніри, що може призвести до того, що злочинні організації легально організовуватимуть покерні ігри/турніри. Прямий характер покеру (можливість понесення навмисних втрат/забезпечення виграшу іншого гравця) робить покер привабливим для відмивання коштів, хоча це вимагає певних знань та планування. У цьому контексті, рівень загрози відмивання коштів, пов'язаної з покером, вважається <u>значним</u> (рівень 3).

Вразливість

Фінансування тероризму

Оцінка вразливості до фінансування тероризму, пов'язаної з грою в покер, не вважається такою, що має значення. У цьому контексті, загроза фінансування тероризму не є частиною оцінки.

Висновки: не застосовується

Відмивання коштів

Оцінка вразливості до відмивання коштів, пов'язаної з грою в покер, свідчить про таке:

a) схильність до ризику

Здебільшого ігри в покер організовуються у межах ліцензованих казино. «Приватний» покерний клуб заборонений і вважається незаконною діяльністю у більшості держав-членів. Однак, навіть якщо в покер грають у казино, покер є вразливим до відмивання коштів, оскільки він передбачає операції на основі готівки та гравців, які грають проти інших гравців, що є відомим як «прямий елемент» (що передбачає навмисні програші або забезпечення переходу виграшу до іншого гравця). Покерні ігри дозволяють здійснювати значні обсяги швидких та анонімних операцій між гравцями (фішки часто купують за готівку).

b) обізнаність про ризики

Рівень обізнаності важко оцінити на цьому етапі, оскільки ігри в покер здебільшого організовуються у межах казино. Здійснення спеціального аналізу є складним завданням.

c) законодавча база і перевірки

Пов'язана з покером діяльність охоплюється законодавчою базою ЄС щодо протидії відмиванню коштів, починаючи з Четвертої директиви про боротьбу з відмиванням грошей. Однак, виходячи з принципів мінімальної гармонізації Директиви, все ще можуть мати місце розбіжності між державами-членами в частині регулювання, нагляду за сектором та приведення у виконання норм ПВК/ФТ.

Гравці грають проти інших гравців, і немає записів про те, «хто кому програв». Також створюються несанкціоновані приватні покерні клуби, які є добре організованими та конкурують із законним сектором. Підрозділи фінансової розвідки вважають, що ці клуби мають лише низьку здатність виявляти підозрілі операції, особливо тому що сам сектор недостатньо обізнаний про ризики та/або недостатньо регулюється/контролюється на національному рівні.

Висновки:
Враховуючи «прямий елемент», очевидну відсутність ведення документації та належного нагляду, а також те, що сам сектор недостатньо обізнаний про ризики та/або неналежно підготовлений для подолання зловживань відмиванням коштів, рівень вразливості до відмивання коштів, пов'язаної з покером, вважається <u>значним</u> (рівень 3).

Пом'якшувальні заходи:

1) <u>Для компетентних органів:</u>

- Держави-члени повинні покращувати співпрацю <u>між відповідними органами влади</u> (підрозділи фінансової розвідки, правоохоронні органи, поліція, галузеві регулятивні органи, такі як регулятори азартних ігор), аби вони могли краще зрозуміти фактори ризику, пов'язаного з покером, та надати ефективні настанови.

- Держави-члени повинні забезпечувати регулярну співпрацю між відповідними органами та операторами покерних ігор, яка повинна фокусуватися на:
    - посиленні вимог до належної перевірки клієнтів та виявленні підозрілих операцій, а також збільшенні кількості та якості звітів про підозрілі операції;
    - організації навчальних занять для співробітників та службовців з питань нормативно-правового дотримання, приділяючи особливу увагу ризикам проникнення або набуття права власності з боку організованих злочинних груп, та регулярно переглядаючи оцінки ризиків щодо їх продуктів/бізнес-моделі;
    - забезпеченні того, що органи нагляду надаватимуть чіткіші настанови щодо ризиків ПВК/ФТ, щодо належної перевірки клієнтів та щодо вимог до звітування про підозрілі операції, а також щодо того, як визначати найбільш доцільні показники для виявлення ризиків відмивання коштів;
    - забезпеченні того, що підрозділи фінансової розвідки надаватимуть зворотній зв'язок операторам покеру про якість звіту про підозрілі операції та шляхи поліпшення звітування, а також про те, як використовується надана у звіті інформація, бажано протягом встановленого періоду часу;
    - розробці стандартного(-их) шаблону(-ів) на рівні ЄС для звітів про підозрілі операції або підозрілу діяльність з урахуванням особливостей сектора грального бізнесу.

2) Для сектора:

- Держави-члени повинні забезпечити, що оператори покерних ігор організовуватимуть регулярні навчальні заняття для співробітників, службовців з питань нормативно-правового дотримання та роздрібних торговців, приділяючи особливу увагу ризикам проникнення або набуття права власності з боку організованих злочинних груп, та регулярно переглядаючи оцінки ризиків щодо їх продуктів/бізнес-моделі.
- Держави-члени повинні гарантувати, що оператори покерних ігор сприятимуть використанню карток гравців або електронних схем ідентифікації для полегшення ідентифікації клієнтів;
- Держави-члени повинні забезпечити, що оператори покерних ігор призначать службовця з питань ПВК у приміщеннях, якщо він ще не призначений.
- Держави-члени повинні забезпечити, що оператори букмекерської діяльності сприятимуть систематичній належній перевірці клієнтів на основі ризику стосовно переможців, а також сприятимуть зниженню граничних значень виграшів за умови належної перевірки клієнтів (наразі 2 000 євро, як передбачено пунктом (d) статті 11 Директиви (ЄС) 2015/849).

3) Для Комісії:

Комісія може надавати настанови щодо пункту (d) статті 11 стосовно здійснення належної перевірки клієнтів у разі здійснення «декількох пов'язаних операцій».

8. Азартні ігри онлайн

Продукт
Азартні ігри онлайн

Сектор
Сектор грального бізнесу

Загальний опис сектора та відповідного продукту/діяльності

У контексті цього звіту, азартні ігри онлайн означають будь-які послуги, які включають розміщення ставок з грошовою вартістю в азартних іграх, в тому числі тих, які мають елемент навичок, наприклад, лотереї, казино, покер та букмекерська діяльність, які надаються будь-яким способом на відстані, електронними засобами або з використанням будь-яких інших комунікаційних технологій та на індивідуальний запит одержувача послуг.

Усі азартні ігри доступні у режимі онлайн. До них відносяться: і) ігри, в яких клієнт розміщує ставку проти провайдера послуг азартних ігор з фіксованими шансами (наприклад, лотереї, розміщення ставок на спортивні змагання, рулетка тощо); та іі) азартні ігри, в яких клієнти можуть грати один проти одного та провайдер послуг бере невелику комісію за організацію діяльності, як правило, відсоток чистого виграшу для кожного клієнта на кожному заході (наприклад, біржі для покерних ігор та букмекерської діяльності, де клієнти можуть розміщувати та приймати ставки).

Однак подальший поділ на різні продукти онлайн-ігор не вважався необхідним у цьому звіті, оскільки відповідні ризики, загрози та вразливості пов’язані в першу чергу з характером онлайн-операцій, а не з конкретними формами онлайн-ігор.

Опис сценарію ризиків

Азартні ігри онлайн можуть передбачати будь-який продукт у секторі азартних ігор або комбінацію таких продуктів. На додаток до деяких ризиків, визначених для кожного сектора у режимі офлайн, можуть бути додаткові ризики, пов'язані з відсутністю прямого контакту в результаті використання мережі Інтернет. Одночасно з цим, електронні азартні ігри пропонують значну пом'якшувальну особливість – можливість відстежувати всі операції.

Злочинець використовує сайти азартних ігор для внесення незаконних коштів і вимагає виплати виграшів або незіграного залишку.

На законні онлайн-ігор вносяться брудні кошти (зарахування), після чого відбувається гра лише на невелику суму коштів, а решта коштів передається іншому гравцеві (або іншому оператору онлайн-ігор). Решта коштів конвертується у готівку так, ніби вони були законним прибутком від ігор.

Злочинні організації можуть використовувати декілька «смурфів» (smurfs)[107], які розміщують ставку безпосередньо один проти одного, використовуючи брудні кошти. Один з таких «смурфів» отримує всі кошти як явний переможець, який згодом конвертує кошти у готівку, ніби це законний прибуток від азартних ігор.

Злочинні організації можуть купувати онлайн-аккаунти в казино, що містять кошти, вже завантажені гравцями, які не є злочинцями, за вищою ціною, ніж реальна.

Злочинні організації можуть також розміщувати ставки на вигадані або фіктивні (неіснуючі) матчі чи події, аби забезпечити виграш.

Загроза

Фінансування тероризму

Оцінка загрози фінансування тероризму, пов'язаної з азартними іграми онлайн, не вважається такою, що має значення. Тому ця загроза не є частиною оцінки.

Висновки: не застосовується

Відмивання коштів

Оцінка загрози відмивання коштів, пов'язаної з азартними іграми онлайн, свідчить про таке:

- як і для всіх інших азартних ігор, **існує ризик проникнення або набуття права власності з боку організованих злочинних груп**. Правоохоронні органи повідомляють декілька прикладів таких випадків.

[107] *«Смурф»* – це досвідчений гравець, який використовує новий акаунт, щоб грати «анонімно» на ігровому сервері, аби обдурити інших гравців, які думають, що він новачок в азартних іграх. Мета – створити нові акаунти, починаючи з нуля, щоб протистояти гравцям нижчого рівня.

- крім того, організовані злочинні групи можуть легко отримувати доступ до такого каналу, в якому вони можуть дешево і практично організовувати свою діяльність. Азартні ігри онлайн є привабливим інструментом для відмивання доходів, одержаних злочинним шляхом. Вони можуть дозволяти легко конвертувати одержані злочинним шляхом кошти у законний прибуток від азартних ігор. Вони передбачають величезний обсяг операцій та фінансових потоків. За даними Європол, деякі злочинні мережі використовують законну мережу компаній з букмерекерської діяльності та азартних ігор, розташованих у деяких державах-членах, для відмивання коштів.

Азартні ігри онлайн з використанням віртуальних активів забезпечують чудові можливості для кіберзлочинців, і цей метод використовувався у нещодавніх атаках в цілях вимагання викупу. Серед відомих методів можна виділити наступні:

- На аккаунти онлайн-ігор вносяться брудні кошти (зарахування), після чого відбувається гра лише на невелику грошову суму, а решта коштів передається іншому гравцеві (або іншому оператору азартних ігор). Решта коштів конвертується у готівку так, ніби вони є законним прибутком від ігор.
- Використання «смурфів» (smurfs), які розміщують ставки безпосередньо один проти одного, використовуючи брудні кошти. Один із «смурфів» отримує всі кошти як явний переможець, який згодом конвертує кошти у готівку, ніби це був законний прибуток від азартних ігор.
- Купівля онлайн-аккаунтів у казино, що містять кошти, вже завантажені гравцями, які не є злочинцями, за вищою ціною, ніж реальна.
- Оператор використовується як підприємство з високим оборотом готівки для змішування брудних грошей від злочинної діяльності та чистих грошей від законних клієнтів.
- Злочинці фіксують ігрові шанси та результати, щоб «смурфи» могли розміщувати ставки, використовуючи брудні гроші, за попередньо вибраними програшними результатами на користь онлайн-казино («матчі-привиди»).
- Злочинці використовують третіх осіб, які діють як «сфурфи», і створюють фіктивні рахунки клієнтів, щоб грати і програвати брудні гроші через мережу Інтернет. Усі зіграні кошти обліковуються як прибуток онлайн-казино зі сплатою податків.

Крім того, в онлайн-середовищі існують різні типи розміщення ставок, які недоступні в режимі офлайн. Букмекерська діяльність онлайн передбачає специфічний ризик надійних ставок, коли гравець використовує кілька аккаунтів для розміщення ставок на кожен можливий результат і тим самим знижує ризики програшу. Що стосується онлайн-покеру, тут також існує специфічний ризик змови.

- ризики, пов’язані з відсутністю прямого контакту, хоча анонімність може бути зведена до мінімуму шляхом здійснення належних перевірок та заходів верифікації, а також відстеження електронних операцій, залежно від рівня нагляду відповідними органами.

Висновки: Правоохоронні органи вважають азартні ігри онлайн потенційно привабливим інструментом для відмивання коштів, що вимагає помірного рівня знань та являє собою життєздатну опцію. Крім того, складається враження, що азартні ігри онлайн пропонують недорогу можливість відмити кошти. У цьому контексті, рівень загрози відмивання коштів, пов’язаної з азартними іграми онлайн, вважається <u>значним</u> (рівень 3).

Вразливість

Фінансування тероризму

Оцінка вразливості до фінансування тероризму, пов'язаної з азартними іграми онлайн, не вважається такою, що має значення. У цьому контексті, загроза фінансування тероризму не є частиною оцінки.

Висновки: не застосовується

Відмивання коштів

Оцінка вразливості до відмивання коштів, пов'язаної з азартними іграми онлайн, свідчить про таке:

а) схильність до ризику

Схильність до ризику, пов'язаного з азартними іграми онлайн, характеризується такими двома компонентами:

- непрямий елемент ділових відносин (вважається високим ризиком як у законодавстві ЄС, так і у вимогах Групи з розробки фінансових заходів з відмиванням грошей (FATF)); та

- можливість використовувати менш відстежувані засоби платежу на веб-платформі (тобто анонімні/передплачені електронні гроші або навіть віртуальні валюти, якщо дозволені).

Фактично, азартні ігри онлайн дозволяють здійснювати операції у всьому світі цілодобово без вихідних. Вони передбачають величезний обсяг операцій та фінансових потоків. Вони не передбачають фізичних продуктів і ускладнюють виявлення будь-яких підозр. Хоча в азартних іграх онлайн не використовуються готівкові кошти, вони тісно пов'язані з використанням інших продуктів, таких як електронні гроші або віртуальні валюти, які представляють власний набір ризиків відмивання коштів. Однак наразі схильність до ризику анонімних/передплачених карток відстежується за допомогою обмежень, встановлених у Четвертій директиві про боротьбу з відмиванням грошей та у майбутній транспозиції П'ятої директиви про боротьбу з відмиванням грошей, що істотно зменшить можливість використання таких платіжних засобів. Крім того, провайдери послуг обміну між віртуальними та фіатними валютами, а також провайдери зберігальних гаманців[108] вважатимуться зобов'язаними суб'єктами відповідно до П'ятої директиви про боротьбу з відмиванням грошей. Процедури належної перевірки клієнтів, які вони повинні будуть застосовувати, також мають забезпечити більшу прозорість у контексті азартних ігор онлайн. Непрямий характер азартних ігор онлайн збільшує ступінь анонімності, навіть якщо такі ініціативи, як eIDAS, мають сприяти частковому зменшенню ризику, пов'язаного з цим аспектом бізнесу, шляхом забезпечення проведення процедур «знай свого клієнта». Крім того, правоохоронні органи (включаючи ЄВРОПОЛ) помітили посилення тенденції у створенні неліцензійних гральних сайтів, які не підпорядковуються вимогам належної перевірки клієнтів, ведення обліку та звітування. Вони не перевіряються органом нагляду. Це може мати значні наслідки для внутрішнього ринку ЄС, якщо такі неліцензійні азартні майданчики зареєстровані за межами ЄС та легко взаємодіють з клієнтами ЄС через мережу Інтернет.

[108] Суб'єкт, який надає послуги захисту приватних криптографічних ключів від імені своїх клієнтів, володіння, зберігання та передачі віртуальних валют.

Одночасно з цим, такі вразливості повинні враховувати той факт, що азартні ігри онлайн можуть також розраховувати на банківські або платіжні рахунки, коли клієнт уже ідентифікований та пройшов основну належну перевірку клієнтів.

b) обізнаність про ризики

Рівень обізнаності у секторі азартних ігор онлайн повинен був збільшитися після включення сектора у законодавчу базу ЄС щодо протидії відмиванню коштів. Якщо він підпадає під дію вимог ПВК/ФТ, рівень звітування про підозрілі операції буде досить належним і здійснюватимуться автоматичні перевірки. Деякі національні законодавства передбачають, що у разі використання електронних гаманців кошти повертаються гравцю на той самий рахунок. Крім того, якщо використовуються передплачені картки, загалом під ризиком опиняються лише невеликі суми.

У значній частині сектора проводяться навчальні програми з питань протидії відмиванню коштів для кожного працівника у межах компанії. Співробітники також проходять навчання з практичних питань, таких як характеристика підозр, як довести їх до відома працівника з питань нормативно-правового дотримання та як вирішити питання на операційному рівні. Представники операторів азартних ігор онлайн зазначають, що підрозділи фінансової розвідки не пропонують зворотного зв'язку щодо звітів про підозрілі операції, які подаються, що в окремих випадках ускладнює роботу операторів (коли незрозуміло, чи мають бути кошти виплачені гравцю, який, у свою чергу, може вжити заходів проти операторів) та перешкоджає покращенню практики протидії відмиванню коштів загалом. Це навіть може перешкоджати майбутньому звітуванню. Має місце також конфлікт з правилами захисту даних, що може знизити рівень звітування. Тим не менш, вони також зазначили, що здебільшого компетентні органи надають оцінку ризиків, щоб допомогти зобов'язаним суб'єктам покращити своє розуміння ризиків. Хоча загальний підхід на основі ризиків залишається чинним, деякі оператори скаржаться на відсутність чітких рекомендацій щодо того, коли та як оператор повинен виконувати свої зобов'язання щодо ПВК/ФТ. Таким чином, у багатьох випадках існує невідповідність між розумінням компетентними органами ризиків та реальною перевіркою, запропонованою операторами азартних ігор онлайн.

c) законодавча база і перевірки

Весь сектор азартних ігор онлайн підпадаю під дію законодавчої бази ЄС щодо протидії відмиванню коштів, починаючи з Четвертої директиви про боротьбу з відмиванням грошей. Однак, виходячи з принципів мінімальної гармонізації Директиви, між державами-членами все ще можуть мати місце розбіжності в частині регулювання, нагляду за сектором та приведення у виконання норм ПВК/ФТ.

Деякі оператори, які мають ліцензію в одній або більше державах-членах, також пропонують послуги азартних ігор в інших державах-членах без дозволу. Крім того, оператори азартних ігор, розташовані за межами юрисдикції ЄС, діють несанкціоновано на території ЄС (тобто без ліцензії у будь-якій державі-члені ЄС і, таким чином, поза контролем ЄС).

Мають місце ситуації, коли платформа азартних ігор онлайн розташована в одній державі-члені, а емітент електронних грошей надає кошти в іншій державі-члені. Іноді платформи ліцензуються на одній території, але діють на іншій через посередника (який може або не може вважатися установою). У таких ситуаціях деякі органи влади не завжди роз'яснюють, де саме має здійснюватися звітування (приймаючий/державний підрозділ фінансової розвідки) та де мають здійснюватися заходи нагляду (приймаючі/державні органи нагляду). Отже, компетентні органи та зобов'язані суб'єкти вважають, що чинна законодавча база не завжди є достатньо зрозумілою в частині того, який орган має компетенцію застосовувати вимоги щодо ПВК/ФТ.

Не існує обов'язку взаємного визнання дозволів, виданих державами-членами Європейського економічного простору. Крім того, з огляду на велику свободу дій держав-членів в області регулювання азартних ігор, включаючи азартні ігри онлайн, і враховуючи той факт, що питання нагляду та правозастосування входять до компетенції національних органів влади, чинні положення та перевірки є різними в різних державах-членах.

Висновки:

Незважаючи на декілька заходів на основі ризиків, які вже впроваджуються багатьма онлайн-операторами (наприклад, навчальні програми з питань протидії відмиванню коштів для співробітників, процедури належної перевірки клієнтів та «знай свого клієнта»), схильність до ризику відмивання коштів, пов'язаного з азартними іграми онлайн, все ще є досить високою, оскільки вона охоплює такі важливі фактори, як непрямий елемент, величезні та складні обсяги операцій і фінансових потоків. Хоча така діяльність не передбачає використання готівки, вона тісно пов'язана з використанням електронних грошей, а також цифрових і віртуальних валют, що також підвищує анонімність клієнтів. У багатьох державах-членах оператори азартних ігор онлайн розробили належний рівень самостійного регулювання та оцінки ризиків, хоча їх співпраця з компетентними органами та підрозділами фінансової розвідки може бути покращена. Оператори вважають, що вони не отримують чітких настанов про те, як правильно усувати ризики, враховуючи, зокрема, відсутність зворотного зв'язку від підрозділів фінансової розвідки стосовно звітів про підозрілі операції. У цьому контексті, рівень вразливості до відмивання коштів, пов'язаної з азартними іграми онлайн, вважається значним (рівень 3).

Пом'якшувальні заходи:

1) Для компетентних органів/регуляторів:

- Держави-члени повинні покращувати співпрацю між відповідними органами влади (підрозділи фінансової розвідки, правоохоронні органи, поліція, галузеві регулятивні органи, такі як регулятори азартних ігор), аби вони могли краще зрозуміти фактори ризику, пов'язаного з азартними іграми онлайн, та надати ефективні настанови.
- Держави-члени повинні забезпечувати регулярну співпрацю між відповідними органами та операторами азартних ігор онлайн, яка повинна фокусуватися на:
    - посиленні вимог до належної перевірки клієнтів та виявленні підозрілих операцій, а також збільшенні кількості та якості звітів про підозрілі операції, зокрема, у ситуаціях, коли платформа азартних ігор онлайн використовується через кордони;
    - організації навчальних занять для співробітників та службовців з питань нормативно-правового дотримання, приділяючи особливу увагу ризикам проникнення або набуття права власності з боку організованих злочинних груп, та регулярно переглядаючи оцінки ризиків щодо їх продуктів/бізнес-моделі;
    - забезпеченні того, що органи нагляду надаватимуть чіткіші настанови щодо ризиків ПВК/ФТ, щодо належної перевірки клієнтів та щодо вимог до звітування про підозрілі операції, а також щодо того, як визначати найбільш доцільні показники для виявлення ризиків відмивання коштів;
    - підвищенні обізнаності операторів азартних ігор онлайн про нові ризики, які можуть збільшити вразливість сектора, такі як використання анонімних електронних грошей або віртуальних валют та виникнення несанкціонованих операторів азартних ігор онлайн;
    - підвищенні обізнаності та збільшенні здатності/знань регуляторів та компетентних органів про оцінювання ризиків в онлайн-середовищі та

кібербезпеці, а також про виявлення та запобігання відмиванню коштів; у зв'язку з цим може бути розглянута можливість об'єднання ресурсів з іншими державами-членами (наприклад, організація спільної навчальної програми).

- Державам-членам рекомендується вимагати від компетентних органів нагляду, якщо доцільно, публікування звіту про заходи безпеки, встановлені операторами азартних ігор онлайн для обмеження ризиків, пов'язаних з непрямими діловими відносинами (ідентифікація та перевірки, моніторинг операцій у режимі онлайн).
- Держави-члени повинні забезпечити, що підрозділи фінансової розвідки надаватимуть зворотній зв'язок операторам азартних ігор онлайн про якість звіту про підозрілі операції та шляхи поліпшення звітування, а також про те, як використовується надана у звіті інформація, бажано протягом встановленого періоду часу.
- Держави-члени повинні розробити стандартні шаблони на рівні ЄС для звітів про підозрілі операції та про підозрілу діяльність з урахуванням специфіки сектора грального бізнесу.
- Держави-члени повинні забезпечити використання спеціальних заходів безпеки для непрямих ділових відносин, такі як електронна ідентифікація (ідентифікація E-IDAS, електронний підпис).
- Держави-члени повинні надавати настанови щодо взаємодії між вимогами щодо належної перевірки клієнтів та правил захисту даних, а також щодо порядку звітування.

2) <u>Для сектора:</u>

- Держави-члени повинні забезпечити, що оператори азартних ігор онлайн організовуватимуть регулярні навчальні програми для співробітників та службовців з питань нормативно-правового дотримання, приділяючи особливу увагу ризикам проникнення або набуття права власності з боку організованих злочинних груп, та регулярно переглядаючи оцінки ризиків щодо їх продуктів/бізнес-моделі. Такі навчальні програми можуть бути обов'язковими для певних категорій персоналу, залежно від їх посади.
- Держави-члени повинні забезпечити, що оператори азартних ігор онлайн сприятимуть систематичній належній перевірці клієнтів на основі ризиків стосовно переможців, а також сприятимуть зниженню граничних значень виграшів за умови належної перевірки клієнтів (наразі 2 000 євро, як передбачено пунктом (d) статті 11 Директиви (ЄС) 2015/849).
- Держави-члени повинні забезпечити, що оператори азартних ігор онлайн призначать службовця з питань ПВК у приміщеннях, якщо він ще не призначений.
- Держави-члени можуть забезпечити, що клієнтам не дозволятиметься відкривати декілька рахунків у одного оператора (а також заборонятимуться перекази між рахунками клієнтів), якщо вони не належать до різних брендів, з якими оператори можуть зв'язатися. Якщо це правило буде порушено, оператор може залишити за собою право заблокувати та/або видалити додатковий рахунок, який має гравець, і перерозподілити всі кошти на один рахунок.
- Держави-члени також можуть встановити зобов'язання щодо відповідності між назвою рахунка гравця та назвою платіжної картки або іншими способами оплати, які використовуються для внесення/зняття коштів, і забезпечити, що рахунок гравця не буде переданий, тобто гравцям забороняється продавати, присвоювати або передавати рахунки чи придбавати рахунки в інших гравців.

3) Для Комісії:

Комісія може надавати настанови щодо пункту (d) статті 11 стосовно здійснення належної перевірки клієнтів у разі здійснення «декількох пов'язаних операцій».

НЕКОМЕРЦІЙНІ ОРГАНІЗАЦІЇ

1. Одержання та переказ грошових коштів через некомерційну організацію

Продукт

Одержання та переказ грошових коштів через некомерційну організацію

Сектор

Некомерційні організації

Загальний опис сектора та відповідного продукту/діяльності

Некомерційні організації можуть мати різноманітні правові форми, залежно від країни, в якій вони засновані. Група з розробки фінансових заходів боротьби з відмиванням грошей (FATF) ухвалила функціональне визначення некомерційної організації, яке використовується Європейською Комісією у контексті цієї наднаціональної оцінки ризиків (SNRA). **Таким визначенням** є «юридичний суб'єкт або юридичне утворення чи організація, яка переважним чином бере участь в одержанні або виплаті коштів для благодійних, релігійних, культурних, освітніх, соціальних чи братських цілей, або для здійснення інших видів «добрих справ».[109]

[109] Це визначення використовується у Пояснювальній примітці до Рекомендації 8: http://www.fatf-gafi.org/publications/fatfgeneral/documents/plenary-outcomes-june-2016.html#npo
Слід зазначити, що не існує єдиного правового визначення ЄС для некомерційної організації, та що їх форми та визначення значною мірою відрізняються на національному рівні. Однак FATF акцентує увагу на **організаціях з надання послуг** і не включає некомерційні організації, які здійснюють представницьку або адвокатську діяльність, у межах Рекомендації 8. Рекомендація 8 посилається лише на ризики фінансування тероризму, пов'язані з некомерційними організаціями, а не ризики відмивання коштів.

Існує широкий спектр підсекторів некомерційних організацій, включаючи гуманітарну допомогу, підтримку розвитку, спорт, адвокатську діяльність тощо.

Що стосується гуманітарних некомерційних організацій, метою їх діяльності є захист та збереження життя людей, постраждалих від природних або техногенних катастроф, при повному дотриманні міжнародного гуманітарного права та принципів гуманітарної дії (нейтралітет, неупередженість, людяність та незалежність[110]). Гуманітарні некомерційні організації можуть здійснювати діяльність на території Європи та поза її межами, а також у різних операційних умовах.

Більша частина гуманітарної допомоги надається у регіонах, що постраждали від збройного конфлікту чи іншого насильства, або мають справу з його наслідками. Гуманітарні організації також можуть діяти у регіонах та країнах, де присутні люди та суб'єкти, визначені як «терористичні», які вірогідно будуть продовжувати свою діяльність. Хоча у секторі гуманітарної допомоги розміщено широке коло організацій з різним ступенем операційної та організаційної спроможності, значний сегмент некомерційних організацій отримує фінансування інституційної гуманітарної допомоги, в тому числі від ЄС та держав-членів, відповідальних за управління коштами ЄС. Вони підпадають під жорсткі договірні вимоги з високим ступенем безпеки.[111]

Опис сценарію ризиків[112]

- Для одержання коштів можуть бути створені некомерційні організації або використовуватися існуючі некомерційні організації. Після цього злочинні кошти надсилаються некомерційним організаціям, і:

    - некомерційні організації-співучасники можуть навмисно підтримувати терористичну групу чи злочинну організацію;
    - законні некомерційні організації можуть використовуватися сторонніми особами;
    - законні некомерційні організації можуть використовуватися інсайдерами.

[110] Відповідно до гуманітарного принципу неупередженості, гуманітарна допомога повинна надаватися виключно за необхідності, без дискримінації між чи у межах постраждалого населенням.

[111] Гуманітарна допомога ЄС фінансується Європейською Комісією та спрямовується через партнерів, включаючи некомерційні організації, які вибираються на основі конкретних правових, фінансових та операційних критеріїв та які підписали Рамкову угоду про партнерство (FPA). Донори та некомерційні організації мають спільну мету – забезпечити, що допомога буде надана тим, хто найбільше її потребує, і не буде спрямована в інше місце. Хоча існує ризик, притаманний функціонуванню у середовищах, де можуть бути присутні визначені терористичні групи, цей ризик випливає з самого операційного середовища, а не з правового статусу діючого суб'єкта.

[112] Відповідно до зобов'язань міжнародної політики, взятих на себе Комісією з метою підвищення ефективності та результативності, гуманітарна допомога ЄС все більше надається у вигляді грошових переказів. Це дає змогу бенефіціарам та їх родинам гідно та гнучко задовольняти найактуальніші потреби та привносити відчуття нормальності у їхнє порушене життя. Такі грошові перекази, здійснені в рамках операцій з надання гуманітарної допомоги, не є предметом цієї оцінки.

- Злочинці можуть використовувати некомерційні організації для фінансування локалізованої терористичної діяльності або можуть намагатися використовувати некомерційні організації для сприяння транскордонному фінансуванню шляхом спрямовування грошових коштів у регіони, де некомерційні організації працюють поблизу зон терористичної діяльності, та:

    - некомерційні організації-співучасники можуть навмисно підтримувати терористичну групу чи злочинну організацію;
    - законні некомерційні організації можуть використовуватися сторонніми особами;
    - законні некомерційні організації можуть використовуватися інсайдерами.

Загальні зауваження

У цій оцінці ризиків некомерційні організації мають значення, наведене у Рекомендації FATF 8. Сценарій ризику охоплює одержання коштів некомерційною організацією та переказ коштів партнерам/бенефіціарам проекту.

Слід підкреслити, що оцінка всього сектора є складною діяльністю з огляду на загальне розмаїття сектору і тому що кожен підсектор некомерційних організацій передбачає різний рівень ризику/загрози.

Оскільки оцінка стосується відмивання коштів та фінансування тероризму, що впливає на внутрішній ринок і транскордонну діяльність, вона застосовується до одержання та переказу коштів на внутрішньому ринку, а також до одержання коштів у межах ЄС для переказу третім країнам.

Загроза

Фінансування тероризму

Оцінка загрози фінансування тероризму, пов’язаної з одержанням та переказом коштів некомерційними організаціями, вказує на те, що цей метод нечасто використовується терористичними групами. Враховуючи велику кількість зареєстрованих некомерційних організацій, використовується дуже мало з них. Однак у рідкісних випадках некомерційні організації можуть стати предметом проникнення з боку терористичних груп, що може становити значну загрозу, зокрема, що стосується фінансування іноземних терористів-бойовиків.

Загалом, одержання та переказ коштів через некомерційні організації регулюється різними національними, а іноді й регіональними положеннями. Дотримання таких положень вимагає наявності певних технічних знань та передбачає різні рівні прозорості та підзвітності. Процедури належної перевірки для реєстрації некомерційних організацій, ліцензування та доступу до фінансових послуг в ЄС стали суворішими. Терористи, які мають на меті фінансувати терористичну діяльність під прикриттям некомерційної організації, повинні розуміти такі процедури, і суворі вимоги можуть стримувати використання ними некомерційних організацій.

Деякі види діяльності некомерційних організацій можуть спричинити більш високий ризик, якщо йдеться про джерела фінансування (невідомі/готівкові/міжнародні джерела/країни високого ризику), види діяльності або бенефіціари (невідомі/країни високого ризику/клієнти високого ризику/використання неформальних каналів для надіслання коштів через кордони). Ризики збільшуються, коли не існує офіційних банківських каналів для переказу грошових коштів некомерційним організаціям та некомерційними організаціями. Основними причинами використання неформальних систем грошових переказів є те, що банки дедалі менше надають фінансові послуги некомерційним організаціям (тенденція, відома як зниження банківських ризиків) та скорочення послуг банків-кореспондентів. Отже, ризик певною мірою пов’язаний з фінансовим відчуженням. Нові технологічні інструменти, такі як «краудфандинг» та блокчейн-

системи, можуть неправильно використовуватися сектором некомерційних організацій, і регуляторам, можливо, доведеться оцінювати та усувати будь-які пов'язані з цим ризики. І навпаки, такі нові інструменти також можуть використовуватися для підвищення відстежуваності коштів.[113]

Робота гуманітарних некомерційних організацій може здійснюватися у регіонах, які є схильними до підвищеного ризику і в яких присутні недержавні збройні групи чи особи, визначені як терористи. Спеціальні ризики залежать від різних факторів, таких як рівень професіоналізації некомерційної організації та ситуація в цій конкретній країні, включаючи політичну динаміку відповідного конфлікту.

<u>Висновки:</u> Ландшафт некомерційної організації є дуже різноманітним. Хоча некомерційні організації стають об'єктом проникнення лише у небагатьох випадках, і загалом потрібні більш спеціальні знання для доступу до коштів, які одержують або переказують некомерційні організації для фінансування терористичної діяльності, рівень загрози фінансування тероризму вважається <u>значним</u> (рівень 3).

Що стосується некомерційних організацій, які отримують інституційне фінансування, зокрема, від ЄС або держав-членів, відповідальних за управління коштами ЄС, рівень загрози вважається <u>незначним</u> (рівень 1).

Відмивання коштів

Оцінка загрози відмивання коштів, пов'язаної з отриманням та переказом коштів через некомерційні організації, розглядається разом із схемами фінансування тероризму, пов'язаними з отриманням та переказом коштів через некомерційні організації з метою фінансування терористичної діяльності. У цьому контексті загроза відмивання коштів не виграє від окремої оцінки.[114]

<u>Висновки:</u> У цьому контексті, рівень загрози відмивання коштів вважається <u>помірно значним</u> (рівень 2).

Що стосується некомерційних організацій, які отримують інституційне фінансування, зокрема, від ЄС або держав-членів, відповідальних за управління коштами ЄС, рівень загрози вважається <u>незначним</u> (рівень 1).

[113] Деякі благодійні організації та організації із збирання коштів спеціально використовують мусульманські громади для фінансової підтримки під виглядом гуманітарної допомоги, наприклад, для підтримки родин та сиріт «мучеників», а також для будівництва мечетей і свердловин. Серед прихильників джихадистів існує високий мобілізаційний потенціал для збирання коштів. У більшості випадків заклики до пожертвувань здійснюються у мечетях, на веб-сайтах, веб-форумах та платформах «краудфандингу», розташованих в Європі, і дають мало інформації про кінцеве використання коштів, які часто знімаються готівкою. У кількох закликах про пожертвування прямо вимагалося внесення пожертвування у біткойнах.

[114] Нещодавно організована злочинна група (ОЗГ) на чолі з прелатом католицької церкви, який офіційно проживає в Римі, більшу частину часу подорожуючи по всьому світу, запропонувала відмивання коштів іншим ОЗГ. Прелат та його сподвижники змогли запропонувати своїм «клієнтам» банківські рахунки благодійних організацій в якості законного засобу для переміщення коштів в усьому світі, не викликаючи підозр. Італійська влада підозрювала, що кошти, спрямовані через такі банківські рахунки, пов'язані з ухиленням від сплати податків, карусельним шахрайством та шахрайськими операціями з ПДВ, а також із серйозними злочинами (такими як торгівля наркотиками).

Вразливість

Фінансування тероризму

Нижче викладено оцінку ризику вразливості до фінансування тероризму, пов'язаної з одержанням та переказом коштів некомерційними організаціями.

Загальні зауваження

Аналіз ризиків сектора некомерційних організацій з точки зору вразливості є важким з огляду на розмаїття сектора.

a) схильність до ризику

Як зазначалося вище, деякі некомерційні організації можуть бути схильні до ризиків. Невеликі обсяги фінансування здійснюються готівкою, що ускладнює правоохоронним органам та підрозділам фінансової розвідки відслідковувати джерела коштів та перекази, що надсилаються за кордон. Ризики збільшуються, коли не існує офіційних банківських каналів для переказу грошових коштів некомерційним організаціям та некомерційними організаціями. Як зазначалося вище, Основними причинами використання неформальних систем грошових переказів є те, що банки дедалі менше надають фінансові послуги некомерційним організаціям (тенденція, відома як зниження банківських ризиків) та скорочення послуг банків-кореспондентів. Отже, ризик певною мірою пов'язаний з фінансовим відчуженням.

Робота гуманітарних некомерційних організацій може здійснюватися у регіонах, які є схильними до підвищеного ризику і в яких присутні недержавні збройні групи чи особи, визначені як терористи. Спеціальні ризики залежать від різних факторів, таких як рівень професіоналізації некомерційної організації та ситуація в цій конкретній країні, включаючи політичну динаміку відповідного конфлікту.

b) обізнаність про ризики

Обізнаність про ризики зростає у секторі некомерційних організацій. Некомерційні організації здійснюють власні оцінки ризиків, які враховують місцезнаходження, тип діяльності, попередню участь організації в цьому регіоні та відносини з іншими секторами. Вони починають розробляти засоби контролю та заходи належної перевірки для переказу та одержання коштів (в цьому допомагають санкційні переліки, перевірки та реформи кримінального права). Сектор також розвиває обмін досвідом щодо практик належної перевірки, питань прозорості та підзвітності та управління ризиками, а також підвищення обізнаності щодо фінансування тероризму. Некомерційні організації (зокрема, гуманітарні) дедалі більше усвідомлюють про ризики, зокрема, коли фінансові операції відбуваються поза фінансовою системою. Також має місце більша співпраця з банківським сектором, що сприяє безпечним та регульованим каналам для законних гуманітарних цілей. Це підвищує прозорість і допомагає захистити некомерційні організації від неправомірного використання терористами, одночасно дозволяючи надання гуманітарної допомоги регіонам, які потребують її найбільше.

Цей сектор також залучений у саморегулювання, а кодекси поведінки розробляються секторами збирання коштів та надання послуг, які часто охоплюють питання управління, звітування, моніторингу використання коштів та принципи, такі як «знай своїх донорів» та «знай своїх бенефіціарів».

У відповідь на вимоги донорів та для забезпечення досягнення допомогою своїх призначених бенефіціарів, некомерційні організації дедалі більше інвестують у суворі функції дотримання та внутрішнього аудиту, а також у розвиток потенціалу у відповідних питаннях, таких як корупція та антикорупційні заходи. Некомерційні організації, які отримують фінансування гуманітарної допомоги від ЄС та держав-членів, відповідальних за управління коштами ЄС, підпадають під сувору договірну законодавчу базу з низкою заходів безпеки.

Спільнота некомерційних організацій є життєво важливою для надання гуманітарної допомоги в усьому світі. Для захисту законних цілей такої допомоги потрібно більше інформації про ризики фінансування тероризму у межах некомерційних організацій для покращення обізнаності про ризики.

c) законодавча база і перевірки

Сектор некомерційних організацій регулюється на національному, а іноді і на регіональному рівні (у цивільному та податковому законодавстві). Не існує централізованої організаційної бази і правила не узгоджені на рівні ЄС. Некомерційні організації безпосередньо не включені до законодавчої бази щодо протидії відмиванню коштів/фінансуванню тероризму (ПВК/ФТ) на рівні ЄС, але опосередковано включені через зобов'язання суб'єктів, які мають некомерційні організації як клієнти, та через зобов'язання держав-членів щодо структур бенефіціарного права власності. Умови реєстрації та експлуатації некомерційних організацій є різними в різних країнах. Компетентні органи схильні вважати, що здійснювані перевірки щодо збирання та переказу коштів у межах ЄС є досить надійними. Однак є повідомлення про деякі недоліки, що стосуються переказу коштів за межами ЄС.

Крім вимог щодо ПВК/ФТ, гуманітарні некомерційні організації регулюються принципами гуманності, неупередженості, нейтралітету та незалежності. Крім того, певні категорії гуманітарних некомерційних організацій, особливо ті, які були оцінені Європейською Комісією, підлягають постійній перевірці протягом періоду існування товариства та конкретним гуманітарним заходам. Такі перевірки, які передбачають докладне звітування про заходи, зобов'язання щодо ведення документації та регулярні аудити як у штаб-квартирі, так і на місцях, виходять за межі суворих критеріїв прийнятності та придатності, які перевіряються шляхом детального процесу вибору до підписання Рамкової угоди про партнерство.

Майже у всіх державах-членах некомерційні організації підлягають певному державному нагляду, будь то податкові органи, регулятори благодійних організацій чи інші типи органів нагляду. Що стосується законодавчої бази, необхідно знайти баланс між програмою боротьби з тероризмом та законними цілями гуманітарних некомерційних організацій.[115]

[115] Наприклад, преамбула Директиви (ЄС) 2017/541 Європейського Парламенту та Ради від 15 березня 2017 року про боротьбу з тероризмом та заміну Рамкового рішення Ради 2002/475/ЈНА та внесення змін до Рішення Ради 2005/671/ЈНА передбачає звільнення для гуманітарної діяльності неупередженими гуманітарними організаціями.

<u>Висновки:</u> на схильність до ризику, пов'язаного з некомерційними організаціями, впливає характер їх діяльності, і ступінь обізнаності щодо ризиків є різним в різних країнах. Чинні правові і податкові норми та національна практика є різними, але забезпечують контроль та перевірки, хоча має бути визнаний спеціальний режим гуманітарного сектора, описаний вище. У цьому контексті, рівень вразливості до фінансування тероризму вважається <u>помірно значним</u> (рівень 2).

Що стосується некомерційних організацій, які отримують інституційне фінансування, зокрема, від ЄС або держав-членів, відповідальних за управління коштами ЄС, рівень загрози вважається <u>незначним</u> (рівень 1).

Відмивання коштів

Оцінка загрози відмивання коштів, пов'язаної з одержанням та переказом коштів через некомерційні організації, розглядається разом із схемами фінансування тероризму, пов'язаними з одержанням та переказом коштів через некомерційні організації з метою фінансування терористичної діяльності. У цьому контексті, загроза відмивання коштів не виграє від окремої оцінки.

<u>Висновки:</u> У цьому контексті, рівень вразливості до відмивання коштів вважається <u>помірно значним</u> (рівень 2).

Що стосується некомерційних організацій, які отримують інституційне фінансування, зокрема, від ЄС або держав-членів, відповідальних за управління коштами ЄС, рівень вразливості вважається <u>незначним</u> (рівень 1).

Пом'якшувальні заходи:

1) <u>Для Комісії</u>

- Продовження співпраці з некомерційними організаціями, які отримують фінансування ЄС, щодо відповідної законодавчої бази ЄС, а також щодо того, як ідентифікувати ризики та відповідати вимогам належної перевірки.
- Продовження участі в обмінах між зацікавленими сторонами, в яких беруть участь усі професійні сектори, зокрема фінансовий сектор, залучені до діяльності з некомерційними організаціями.
- Продовження співпраці з гуманітарними некомерційними організаціями та надання їм настанов щодо отримання фінансування ЄС у зв'язку з ризиками, пов'язаними з ВК/ФТ, та щодо вимог належної перевірки, враховуючи найкращі практики гуманітарних організацій.

2) <u>Для компетентних органів</u>

- Держави-члени повинні покращити участь некомерційних організацій у національних оцінках ризиків та розробці програм інформування та обізнаності, спрямованих на протидію ризикам зловживань, і повинні підтримувати некомерційні організації шляхом надання їм матеріалів для підвищення обізнаності (на рівні держав-членів, а також на рівні ЄС).
- Державам-членам слід додатково проаналізувати ризики, з якими стикається сектор некомерційних організацій.

ПРОФЕСІЙНИЙ СПОРТ

1. Інвестиції у професійний футбол і договори трансферу професійних футболістів

Продукт
Інвестиції у професійний футбол і трансфертні угоди з гравцями професійного футболу

Сектор
Професійний спорт

Загальний опис сектора та відповідного продукту/діяльності

Спортивна індустрія є одним з багатьох секторів, який може приваблювати злочинців для відмивання коштів, і заслуговує на більш детальний розгляд з огляду на його соціальний та культурний вплив, великі масштаби грошових операцій та збільшення кількості залучених осіб.

Подібно до інших галузей, спорт та азартні ігри використовуються злочинцями для відмивання коштів та отримання незаконного доходу. Як і у секторі предметів мистецтва, злочинці у секторі спорту не завжди мотивуються одержанням економічної вигоди. Соціальний престиж, поява на публіці разом із знаменитостями, а також перспектива зв'язків з представниками влади можуть також приваблювати приватних інвесторів, які мають сумнівні наміри.

Опис сектора

У футбол грають понад 265 мільйонів людей у світі. За даними Міжнародної федерації футбольних асоціацій (FIFA), існує 38 мільйонів зареєстрованих професійних гравців та близько 301 000 клубів. Футбол зазнав надзвичайного зростання з початку 1990-х років завдяки набуттю телевізійних прав та спонсорству. Ринок професійних гравців пережив безпрецедентну інтернаціоналізацію, що призвело до зростання кількості трансферів між континентами.

У футболі договори про імідж, рекламу та спонсорські угоди можуть бути інструментами злочинної діяльності, особливо для ухилення від сплати податків, оскільки кошти, передбачені цими договорами, зазвичай переказуються на рахунки, які належать компаніям третіх країн. Це призводить до серйозного ризику шахрайства, оскільки легко уникати декларування отриманих коштів, навіть якщо це вимагає використання сторонніх осіб у різних фінансових операціях.

Найпоширеніша форма грошових виплат включає юрисдикції, розташовані за кордоном, які дозволяють замаскувати остаточне призначення платежів. Іміджеві права також використовуються для приховування фактично виплачених гравцям сум.

Крім того, азартні ігри безпосередньо пов'язані з футболом через розміщення ставок на ігри та матчі.

Відповідні суб'єкти

Футболом керує FIFA, штаб-квартира якої знаходиться у місті Цюріх, Швейцарія. Це приватна установа, яка регулюється швейцарським законодавством, що контролює весь світ футболу через конфедераційну систему. Вона має повноваження сприяти та розвивати футбол у всьому світі. У кожній країні є асоційований партнер, який повинен дотримуватися правил та законів FIFA. FIFA несе чітку відповідальність за захист репутації та доброчесності спортивного сектора.

З цієї причини у 2004 році FIFA затвердила Кодекс етики (який пізніше кілька разів переглядався)[116], який дав можливість створити новий Комітет з питань етики, який є ключовим членом. У рамках своєї роботи з посилення етики у спорті FIFA пропонує технічну підтримку через компанію Early Warning Systems GmbH, засновану спеціально для контролю за букмекерською діяльністю у секторі спорту та запобігання негативним наслідкам неетичної поведінки у футболі.

Як орган нагляду, який уважно стежить за футбольним сектором, включаючи його керівництво клубами, які часто мають борги, несумісні з ефективними фінансовими можливостями, FIFA включає шість конфедерацій: Азіатська конфедерація футболу в Азії та Австралії (AFC), Африканська конфедерація футболу (CAF), Конфедерація футболу Північної та Центральної Америки і країн Карибського басейну (CONCACAF), Південноамериканська конфедерація футболу (CONMEBOL), Конфедерація футболу Океанії (OFC) та Союз Європейських футбольних асоціацій (UEFA). UEFA – найбільша з шести континентальних конфедерацій.

[116] З 12 серпня 2018 року набрав чинності новий Етичний кодекс FIFA 2018.

FIFA покладається на Систему відстеження трансферів (TMS) для отримання інформації про міжнародні трансфери гравців, яка раніше була обмеженою для зацікавлених сторін цього бізнесу. За допомогою цієї системи у мережі Інтернет реєструється понад 30 типів інформації, таких як історія гравців, клуби, залучені у цей бізнес, платежі, суми, контракти та інша інформація.

Національні асоціації несуть відповідальність за дисципліну, координування та адміністрування футболом у відповідних країнах. Ці національні організації вважаються ключовими регуляторами у своїх країнах, але вони все рівно повинні дотримуватися конкретних норм, встановлених FIFA. У свою чергу, національні асоціації можуть поділятися на регіональні органи. Клубами вважаються осередки, які лежать в основі кожного регіонального органу.

Протягом історії FIFA її статути декілька разів переглядалися, що дозволило модернізувати їх і перетворити на зростаючий обсяг робіт. Вони визначають основні закони міжнародного футболу, включаючи численні правила щодо змагань, трансферів, незаконного вживання наркотиків та різних інших питань. Ці підзаконні акти були затверджені на 59-му Конгресі FIFA в Нассау, Багамські острови, 3 червня 2009 року і набрали чинності 2 серпня того самого року. Зміни до статутів FIFA можуть бути внесені лише на сесії Конгресу і вимагають голосів 75 % національних федерацій, які присутні на сесії та мають право голосу. Це робить статути FIFA та їх імплементаційні положення рівнозначними конституції керівного органу міжнародного футболу.

Опис сценарію ризиків

Перший документ ЄС, який визнав важливість спорту, був опублікований у липні 2007 року (Біла книга ЄС про спорт).[117] У ньому зазначається, що «спорт стикається з новими загрозами та викликами, такими як комерційний тиск, експлуатація молодих гравців, допінг, корупція, расизм, незаконні азартні ігри, насильство, відмивання коштів та інші види діяльності, згубні для спорту». До використання нелегальних ресурсів у футболі призвели багато факторів, не в останню чергу його складна організація і недостатня прозорість.

У березні 2013 року Європейський Парламент ухвалив резолюцію про практику договірних матчів та корупції у спорті.[118] Після цього 11 червня 2015 року була прийнята резолюція про розкриття корупційних справ високого рівня у FIFA[119], а 2 лютого 2017 року була ухвалена резолюція про інтегрований підхід до спортивної політики, що охоплює належне управління, доступність та доброчесність.[120] Під час пленарного засідання у липні 2016 року комітет CULT виніс на розгляд Комісії усне запитання щодо практики договірних матчів, вимагаючи повного схвалення ратифікації Конвенції Ради Європи про маніпуляції зі спортивними змаганнями.[121] Відповідь Уповноваженого підкреслила підтримку Комісією Конвенції як цінного інструменту у боротьбі з практикою договірних матчів, оскільки вона є надійною основою для забезпечення загальноєвропейської координації та співпраці у такій боротьбі. Однак для забезпечення

---

[117] *Біла книга про спорт*; Європейська Комісія, Брюссель, 11.07.2007; COM(2007) 391 final.

[118] Резолюція Європейського Парламенту від 14 березня 2013 року про практики договірних матчів та корупцію у спорті (2013/2567(RSP)). Доступна за посиланням: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52007DC0391

[119] Резолюція Європейського Парламенту від 11 червня 2015 року про нещодавні розкриття корупційних справ високого рівня у FIFA (2015/2730(RSP)). Доступна за посиланням: www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2015- 0233+0+DOC+XML+V0//EN

[120] Резолюція Європейського Парламенту від 2 лютого 2017 року про інтегрований підхід до політики в області спорту: належне управління, доступність та доброчесність. Доступна за посиланням: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P8-TA-2017-0012

[121] **Конвенція про маніпуляції спортивними змаганнями (Конвенція Маколін)** була відкрита для підписання 18 вересня 2014 року на 13-й Конференції міністрів Ради Європи з питань спорту у м. Маколін, Швейцарія: https://www.coe.int/en/web/sport/about-the-convention-on- the-manipulation-of-sports-competitions

набрання чинності Конвенцією в ЄС необхідна співпраця між державами-членами та установами.

Соціальний статус також сприяє привабливості і призводить до інвестування великих грошових сум без очевидних або обґрунтованих фінансових прибутків чи надходжень, крім соціального престижу інвестування у професійний спорт. Популярність професійного спорту, зокрема, професіонального футболу, може стати інструментом злочинців для легітимізації своєї діяльності шляхом появи на публіці разом з відомими людьми, підприємцями або органами влади.

Футбол є надзвичайно актуальним кандидатом для вивчення з огляду на його швидку трансформацію від популярного спорту до світової індустрії із значним економічним впливом. З огляду на його соціальну важливість, він є засобом передачі культурних та загальнолюдських цінностей.

Багато випадків показали, що футбольній індустрії притаманна протизаконна практика, включаючи відмивання коштів, корупцію та наркотики.

Недостатня прозорість в частині трансферу гравців та справжніх власників або менеджерів футбольних клубів може призвести до того, що в цій галузі домінуватиме купка людей, та може викликати серйозне занепокоєння щодо запобігання та припинення відмивання коштів.

Крім того, Група з розробки фінансових заходів боротьби з відмиванням грошей.(FATF) також виявила випадки використання нефінансових фахівців, таких як члени родини, адвокати, консультанти та бухгалтери, для створення структур для переміщення незаконних коштів. Гроші, передбачені подібними іміджевими договорами (за використання зовнішності гравця як частини крупної рекламної кампанії), часто переказуються на рахунки компаній третіх країн з серйозними ризиками шахрайства. Для відмивання коштів також можуть використовуватися рекламні та спонсорські угоди. Організована злочинність може спонсорувати спорт і стати мостом до законного бізнесу. Найпоширеніша форма платежів включає юрисдикції, розташовані за кордоном, завжди як спосіб приховати останній пункт призначення.

Крім того, дані FIFA не є загальнодоступними і їх складно отримати, і нешвейцарські органи влади змушені будуть вимагати міжнародної правової співпраці для отримання доступу до них, оскільки штаб-квартира FIFA знаходиться у Швейцарії.

Загроза

Фінансування тероризму

Оцінка загрози фінансування тероризму, що виникає внаслідок одержання та переказу коштів у секторі футболу, вказує на те, що такий спосіб фінансування тероризму нечасто використовується терористичними групами. Дійсно, не існує жодних відомих випадків фінансування тероризму за рахунок коштів, які переміщуються через сектор футболу.

Висновок: У цьому контексті, рівень загрози фінансування тероризму, пов'язаної з футболом, вважається помірно значним (рівень 2).

Відмивання коштів

У деяких державах-членах органи влади вважають футбольні клуби сферою занепокоєння в частині того, що цей сектор використовується для відмивання брудної готівки, а клуби не повідомляють про підозрілу поведінку.[122]

Методи

Методи, за рахунок яких функціонують організовані злочинні групи, можна проілюструвати на прикладі декількох нещодавніх випадків:

- У травні 2016 року під час операції *«Матріоскас» (Matrioskas)* португальська поліція (Polícia Judiciária), за підтримки Європолу, виявила транснаціональну організовану злочинну групу, яка здебільшого складалася з громадян Російської Федерації, що займалися відмиванням коштів через сектор футболу. Діючи з принаймні 2008 року, ця злочинна мережа вважається осередком важливої російської мафіозної групи, безпосередньо відповідальної за відмивання кількох мільйонів євро у багатьох країнах ЄС, більшість з яких походять від полікримінальної діяльності, вчинюваної за межами ЄС.

  Відомий алгоритм дій групи полягав у тому, щоб ідентифікувати футбольні клуби ЄС, які мають фінансові труднощі, а потім впроваджувати в них благодійників, які надають необхідні короткострокові пожертвування чи інвестиції.

  Завоювавши довіру через пожертвування, такі благодійники організовують купівлю клубів. У купівлі таких клубів допомагають особи, які виступають в якості підставних осіб для непрозорих і складних мереж холдингових компаній, що незмінно належать компаніям-оболонкам, зареєстрованим в офшорних зонах і в третіх країнах високого ризику. У результаті цього, справжні власники і ті, хто врешті-решт контролює клуб, залишаються невстановленими, як і справжнє походження коштів, які були використані для їх купівлі.

  Після того, як клуби потрапили під контроль російської мафії, великі обсяги фінансових операцій, транскордонний грошовий потік та недоліки в управлінні дозволили використовувати їх для відмивання брудних коштів (як правило, через завищену або занижену оцінку гравців на трансфертному ринку та в угодах на телевізійні права) та для букмекерської діяльності (як для генерування незаконних доходів за допомогою практики договірних матчів, так і чисто для цілей відмивання коштів). Використовуючи цей метод, злочинна група спочатку здійснила низку пожертвувань та інвестицій у клуб, який змагався в основній португальській футбольній лізі, поки не зіткнувся з фінансовими труднощами у 2012 році, через що він перейшов у нижчі підрозділи. У липні 2015 року група придбала клуб.

[122] https://kyc360.com/news/uk-football-clubs-in-live-money-laundering-investigations/

Поліцейське розслідування розпочалося з виявлення небезпечних показників тривожних сигналів щодо підозрюваних. Зокрема, підозру викликав високий рівень життя підозрюваних з використанням активів високої вартості, зареєстрованих на імена третіх осіб (використання підставних осіб). Вони імпортували велику кількість готівки з Росії до Португалії у порушення положень ЄС про готівкові кошти (використання кур'єрів готівкових коштів) і створювали та використовували непрозорі мережі офшорних компаній-оболонок, призначені для збереження особи їх власників.

З липня 2015 року було зібрано вагомі докази того, що ця злочинна група діє як злочинне об'єднання, яке здійснює відмивання коштів, податкове шахрайство, корупцію та підробку документів для здійснення різних транснаціональних кримінальних злочинів.

- Європейські футбольні клуби, придбані злочинними організаціями, можуть також використовуватися для відмивання коштів за допомогою букмекерської діяльності у договірних футбольних матчах.
- Корупція в області спорту та практика договірних матчів часто здійснюються злочинними мережами, пов'язаними з торгівлею наркотиками, незаконною контрабандою тютюну та крадіжками.
- Організована злочинна група створила різні веб-сайти як частину онлайн-платформи букмекерської діяльності, яка використовувалась для розміщення ставок на маніпульовані спортивні змагання, що відбувалися у багатьох європейських країнах. Злочинців підозрюють у причетності до спроб практикувати договірні футбольні матчі, зокрема, у Сербії, Північній Македонії та Чехії. Організована злочинна група, яка стоїть за цією діяльністю, раніше діяла в основному на азіатському ринку, де отримувала значні фінансові вигоди, знаючи про кінцевий результат матчів. Вона об'єдналася з іншими крупними злочинними групами в різних країнах, щоб інвестувати кошти, отримані від інших серйозних злочинів, включаючи торгівлю наркотиками.

<u>Висновки:</u> У цьому контексті, рівень загрози відмивання коштів, пов'язаної з футболом, вважається значним (рівень 3).

Вразливість

Фінансування тероризму

Оцінка вразливості до фінансування тероризму, пов'язаної з професійним футболом, свідчить про таке:

a) схильність до ризику

Як зазначалося вище, футбольні клуби та пов'язана з футболом діяльність схильні до ризику, коли частина фінансування спрямовується у формі готівки, що ускладнює простежуваність джерела коштів і трансферів (у разі надіслання за кордон) з точки зору правоохоронних органів та підрозділів фінансування тероризму.

b) обізнаність про ризики

Сектор футболу має централізовану організаційну структуру, але застосовувані до нього правила не узгоджені на рівні ЄС і є різними у різних державах-членах. Централізована організація сектора є обмеженою з огляду на здатність органів влади забезпечувати ефективне управління або допомогу. Обізнаність про ризики у секторі зростає.

c) законодавча база і засоби контролю

Сектор не включений до законодавчої бази щодо ПВК/ФТ на рівні ЄС. Питання підпорядкування положенням щодо ПВК/ФТ залишається на розсуд держав-членів. Існуючі вимоги щодо ПВК/ФТ необов'язково вважаються достатніми для задоволення конкретних потреб сектора, а здійснювані перевірки залежать від країни-члена.

Висновок: У цьому контексті, рівень вразливості до відмивання коштів, пов'язаної з професійним футболом, вважається помірно значним/значним (рівень 2/3).

Відмивання коштів

Оцінка вразливості до відмивання коштів, пов'язаної з професійним футболом, свідчить про таке:

a) схильність до ризику

Спроби FIFA отримувати інформацію через Систему відстеження трансферів є на сьогоднішній день ефективними, але недостатніми. Це життєво важливий інструмент для отримання інформації про міжнародний трансфер гравців, раніше обмежений лише зацікавленими особами цього бізнесу. Але зусилля FIFA, які інколи зосереджуються на суто комерційних та приватних інтересах, не повинні замінити роботу органів влади.

Мають бути встановлені певні зобов'язання, такі як вимагання від клубів, федерацій та конфедерацій, а також тих, хто надає консультативні, аудиторські, бухгалтерські послуги та консультації в цій галузі, повідомляти про підозрілі операції підрозділам фінансової розвідки. За даними FATF, клуби навмисно використовуються для відмивання коштів, і тому потрібно робити більше. Дані FIFA не є загальнодоступними і їх складно отримати, і тому органи влади змушені будуть вимагати міжнародної правової співпраці для отримання доступу до них, оскільки штаб-квартира FIFA знаходиться у Швейцарії.

b) обізнаність про ризики

Крім збирання інформації, для органів влади важливо відстежувати активи, отримані від злочинної діяльності у спорті та азартних іграх.

Одних зусиль FIFA недостатньо для запобігання неправомірній практиці. Асоціації, федерації та конфедерації повинні брати участь та надавати належні посилання або настанови в області футболу, а також необхідну підтримку клубам шляхом організації професійного навчання для просування звітування про підозрілі операції.

c) законодавча база і засоби контролю

Принцип конфіденційності не повинен застосовуватися для знехтування звітуванням про підозрілі операції, відповідно до Рекомендації 9 FATF. Дійсно, обов'язок фахівців, не пов'язаних з фінансовим сектором, щодо звітування, який також передбачений у Рекомендаціях 18, 21 та 22 FATF, є важливим інструментом боротьби з неправомірним використанням передових практик менеджерами при найманні гравців. Законодавство, яке пропагує анонімність в організації та функціонуванні спортивних органів, також повинно вимагати

ефективної фінансової та адміністративної прозорості і встановлювати цивільно-правові та кримінальні зобов'язання їх керівників.

Висновок: сектор наразі вразливий до відмивання коштів. Хоча рівень обізнаності сектора щодо ризиків відмивання коштів здається вищим, ніж для фінансування тероризму, здатність сектора забезпечити спеціальні ресурси та навчання у цій галузі залишається досить низькою. Чинна законодавча база посилила перевірки, здійснювані у секторі, але вони залишаються невідповідними. У цьому контексті, рівень вразливості до відмивання коштів у секторі професійного футболу, вважається помірно значним/значним (рівень 2/3).

Пом'якшувальні заходи:

Європейський Парламент закликав держави-члени визнати злочин шахрайства у секторі спорту.[123] Крім того, у 2014 році Виконавчий комітет FIFA затвердив Положення про роботу з посередниками.[124]

У Додатку до рішення Комісії про прийняття Угоди про співпрацю між Європейською Комісією та Союзом Європейських футбольних асоціацій (UEFA)[125] чітко йдеться про амбіції обох підписантів запобігти використанню футбольного сектора для відмивання коштів. UEFA зобов'язалася брати участь у цьому процесі, щоб допомогти Комісії оцінити ризики відмивання коштів у футбольному секторі.

Держави-члени також повинні враховувати наступне:

- визначення того, як агенти гравців (у тому числі фізичні чи юридичні особи, які рекламують, виступають посередниками, торгують, наймають або обговорюють трансферні права спортсменів), повинні повідомляти про підозрілі операції. Особи, корпорації, асоціації, федерації, конфедерації та клуби, які беруть участь у просуванні, посередництві, маркетингу чи торгівлі спортсменами, також повинні підпадати під дію цієї вимоги щодо переговорів;
- вимагання від футбольних клубів зберігати кожен контракт та відповідні угоди про посередництво протягом принаймні 5 років;
- вимагання повної ідентифікації інвесторів, навіть коли їх представляють корпорації у країні;

[123] Резолюція Європейського Парламенту від 23 жовтня 2013 року про організований злочин, корупцію та відмивання коштів: рекомендації щодо заходів та ініціатив, які мають бути реалізовані (заключний звіт) (2013/2107(INI)); OB C 208, 10.06.2016, с. 89-116. Доступна за посиланням: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013IP0444

[124] https://www.fifa.com/about-fifa/who-we-are/news/fifa-executive-committee-approves-regulations- working-with-intermediarie-2301236

[125] Європейська комісія, Брюссель, 19.02.2018, C(2018) 876 final.

- застосування більших вимог до контролю та реєстру походження власників рахунків та бенефіціарів коштів, які перераховуються до податкових гаваней. Додаткові механізми мають бути розроблені для того, щоб спробувати змусити треті країни своєчасно надавати всю інформацію за запитом;
- пропонування навчання клубам та агентам трансферу у федераціях, конфедераціях та будь-якому іншому органі нагляду з метою зміцнення їх ролі;
- вимагання від клубів, федерацій та конфедерацій виконання, під загрозою санкцій, реєстрації національних або міжнародних трансферів гравців. Вони повинні надати повну інформацію про операцію, деталізуючи її фінансову структуру, а також додати договір агента та доказ особи агента та гравця до договору про трансфер між покупцями та продавцями;
- створення зобов'язання здійснювати незалежний аудит у спортивних федераціях та конфедераціях.

Зокрема, що стосується агентів, держави-члени повинні:

- вимагати від тих, хто виступає агентами спортсменів, навіть родичів або адвокатів, отримати ліцензію для уникнення відсутності прозорості в їх діяльності;
- регламентувати законодавчу базу для футбольних агентів для включення будь-якої торговельної діяльності за межами клубів;
- вимагати ліцензування агентів гравців для збільшення прозорості у своїх угодах;
- регулювати та контролювати всі дії агентів гравців, забезпечуючи наявність у них необхідного ліцензування чи дозволу;
- встановлювати юридичні обмеження на ведення бізнесу в якості агента гравця, вимагаючи від агентів наявності реєстрації з докладним резюме в регуляторному органі, на додаток до FIFA;
- накласти заборону на всіх, хто має кримінальні судимості, або хто програв цивільні справи, пов'язані з шахрайством, ухиленням від сплати податків чи іншими цивільними зобов'язаннями, на державному, муніципальному або федеральному рівнях;
- вимагати від агентів інформування всіх клієнтів про своїх підрядників.

ЗОНИ ВІЛЬНОЇ ТОРГІВЛІ

1. Порти вільної торгівлі

Продукт

Порти вільної торгівлі

Сектор

Зони вільної торгівлі, вільні зони — Митниці, пряме оподаткування

Загальний опис сектора та відповідного продукту/діяльності

Зони вільної торгівлі (ЗВТ) – це тип спеціальної економічної зони (СЕЗ), тобто регіон, в якій законодавство про комерційну і торговельну діяльність відрізняється від законодавства решти країни. У ЗВТ або у СЕЗ товари можуть відвантажуватися, зберігатися, транспортуватися, вироблятися або реконфігуруватися та реекспортуватися відповідно до спеціальних митних норм і, як правило, без сплати митного збору. ЗВТ зазвичай організовані навколо крупних морських портів, міжнародних аеропортів та національних кордонів – територій, що мають багато географічних переваг для торгівлі.

ЗВТ також відомі як **вільні зони** – митні домовленості, які широко використовується в усьому світі для полегшення торгівлі. Вони передбачені Кіотською конвенцією (Спеціальний додаток D), підписаною ЄС та 115 іншими сторонами. Переглянута Кіотська конвенція 1999 року визначає їх як «частину території договірної сторони, в межах якої розміщені на ній товари, як правило, розглядаються як такі, що знаходяться за межами митної території, якщо йдеться про ввізні мита і податки».

Митний кодекс Союзу також передбачає створення вільних зон.[126] Держава-член ЄС може визначити частину своєї митної території як вільну зону. Вільні зони мають бути закритими, а периметр і вхідні/вихідні пункти мають підлягати митному нагляду. Їх створення вимагає попереднього погодження з митними органами, які повинні бути заздалегідь поінформовані про заходи, що будуть здійснюватися, і можуть встановлювати заборони чи обмеження.

У вільних зонах держави-члени можуть застосовувати:

- пільги та звільнення від сплати ПДВ та акцизних зборів відповідно до спеціальних норм законодавства ЄС щодо непрямого оподаткування; та
- такі схеми прямого оподаткування, які вони вважають за потрібне, з урахуванням:
    - правил державної допомоги ЄС (які взагалі застосовуються до вільних зон); і
    - кодексу поведінки з оподаткування бізнесу[127] (який вони погодилися застосувати для обмеження шкідливої податкової практики).

[126] Стаття 243 Регламенту (ЄС) № 952/2013 Європейського Парламенту та Ради від 9 жовтня 2013 року про створення Митного кодексу Союзу (OB L 269, 10.10.2013, с. 1).

[127] Група з питань Кодексу поведінки (оподаткування бізнесу) була створена Радою з економічних та фінансових питань (ЕКОФІН) 9 березня 1998 року. Її основна функція полягає в оцінці податкових заходів, що підпадають під дію Кодексу поведінки щодо оподаткування бізнесу від грудня 1997 року, та нагляді за наданням інформації про такі заходи.

Опис сектора

Вільні порти – це склади у вільних зонах, які спочатку були призначені як місця для зберігання транзитних товарів. Вони стали популярними для зберігання замінних активів, включаючи предмети мистецтва, дорогоцінне каміння, антикваріат, золото та вино – часто на постійній основі. Крім відповідального зберігання, вони пропонують відстрочення ввізного мита та непрямих податків, таких як ПДВ чи податки на кінцевих користувачів, та високу ступінь секретності.

У 2016 році на складське зберігання припадало 30 % загальної світової діяльності ЗВТ, при чому вартість товарів, що зберігалася, становила 536 млрд доларів США.[128]

В ЄС:

В ЄС є 82 вільні зони.[129] Єдиним вільним портом (тобто ЗВТ, що спеціалізується на зберіганні товарів розкоші високої вартості) є Люксембургський вільний порт, який був відкритий у вересні 2014 року та має лише п'ять аналогів в інших містах світу: Женеві, Монако, Сінгапурі, Пекіні і Делаварі (США).

Інші вільні зони розташовані у 22 державах-членах. Вони підпадають під різні категорії СЕЗ, затверджуються Комісією і в основному використовуються як логістичні та торгові центри, а не спеціально для цілей управління капіталом або для зберігання предметів розкоші.

Опис сценарію ризиків

ЗВТ продовжують створювати загрозу підробки, оскільки вони дозволяють підробникам розвантажувати вантажі, адаптувати або іншим чином підробляти вантажі чи пов'язані з ними документи, а потім реекспортувати продукцію без митного втручання, таким чином маскуючи справжнє походження та характер товарів, а також особу оригінального постачальника.

Наразі в усьому світі існує 3 500 вільних зон та СЕЗ. ЗВТ не обслуговують тільки морські перевезення – багато з них розташовані у міжнародних аеропортах та на державних кордонах, звідки вантажі можуть транспортуватися по суші.

Слабкі місця і досі присутні у декількох ЗВТ, і деякі з них використовуються для вчинення організованих злочинів, в тому числі:

- торгівля наркотиками;

[128] https://www.cps.org.uk/files/reports/original/161114094336-TheFreePortsOpportunity.pdf

[129] Вільні зони, які діють на митній території Союзу, про що повідомляють держави-члени Комісії: https://ec.europa.eu/taxation_customs/sites/taxation/files/resources/documents/customs/procedural_aspects/imports/free_zones/list_freezones.pdf

- нелегальна торгівля слоновою кісткою;
- контрабанда людей; та
- підроблення.

Організовані злочинні групи, які зловживають ЗВТ, часто є полізлочинними, наприклад, діяльність організованих злочинних груп, залучених у злочин, пов'язаний з правами інтелектуальної власності, часто тягнуть за собою шахрайство з ПДВ, корупцію та відмивання коштів.

Законні підприємства, що належать злочинцям, залишаються ключовими у діяльності з відмивання коштів. Вони уможливлюють схеми на основі торговельної діяльності, які не часто передбачають фізичне переміщення готівки та передбачають підставну особу для здійснення грошових переказів.

Більшість портів вільної торгівлі та митних складів ЄС (крім порту вільної торгівлі Люксембургу) не мають точної інформації про кінцевих бенефіціарних власників. П'ята директива про боротьбу з відмиванням грошей (AMLD5) чітко охоплює операторів портів вільної торгівлі та інших суб'єктів на ринку мистецтв, оскільки з 10 січня 2020 року вони будуть «зобов'язаними нефінансовими суб'єктами» і тому мають підпорядковуватися тим самим вимогам до належної перевірки клієнтів, наприклад, агенти з нерухомості та нотаріуси. Вони також візьмуть на себе роль «вратарів» у протидії відмиванню коштів (ПВК), оскільки їм доведеться повідомляти про підозрілі операції підрозділам фінансової розвідки.

Вартість товарів, що зберігаються у вільних портах, оцінюється в мільярдах євро. З огляду на застереження про захист персональних даних та конфіденційність (схожі на положення про банківську таємницю), власники вільних портів не розголошують інформацію про вартість товарів, що зберігаються у їхніх приміщеннях, як заявляють клієнти, тому складно дати точну оцінку.

Щоб використовувати вільні порти Швейцарії в якості прикладу, у вересні 2012 року *The Economist* зазначив, що у вільних портах у Женеві та Цюріху зберігаються «картини, скульптури, золото, килими та інші предмети» на суму понад 10 млрд доларів США.[130] У 2016 році уряд Швейцарії зазначив, що вільні порти країни містять цінності вартістю близько 100 млрд євро.[131]

Загроза

Група розробки фінансових заходів боротьби з відмиванням грошей (FATF) вважає, що ЗВТ, такі як вільні порти, збільшують економічні можливості, але їм не вистачає ефективного нагляду з боку правоохоронних органів та регулювання.[132]

Вільні порти сприймаються як засоби, що захищають особу та фінансові операції своїх клієнтів, як раніше приватні банки. Вони були описані як установи, звільнені від обов'язку щодо збирання інформації та звітування про цінні дані, що стосуються потенційних випадків ухилення від сплати податків, корупції та відмивання коштів.[133]

---

[130] https://www.economist.com/finance-and-economics/2012/09/01/paint-threshold

[131] https://www.finews.com/news/english-news/23238-swiss-freeports-move-to-crack-down-on-art,-loot

[132] *Вразливості до відмивання грошей зон вільної торгівлі*: http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20vulnerabilities%20of%20Free%20Trade%20Zones.pdf

[133] http://www.taxjustice.net/wp-content/uploads/2013/04/TJN-141124-CRS-AIE-End-of-Banking-Secrecy.pdf

Фінансування тероризму

Вільні порти мають кілька обмежень, які заважають місцевій владі здійснювати розслідування щодо майна, яке зберігається у їхніх приміщеннях.

Нещодавня справа, яка ілюструє *алгоритм дій*:

У грудні 2016 року влада Швейцарії конфіскувала культурні реліквії, які були викрадені з Сирії, Лівії та Ємену і зберігалися у вільних портах Женеви, де знаходяться склади, де речі можуть зберігатися без накладення податків. Мародери привезли конфісковані предмети до Швейцарії через Катар. Три предмети були з древнього міста Пальміра (Сирія), місця всесвітньої спадщини ЮНЕСКО, систематично знищуваного джихадистами ІСІЛ (Даеш), які захопили його у травні 2015 року.

Висновки: Тому рівень загрози фінансування тероризму, пов'язаної з вільними портами, вважається значним (рівень 3).

Відмивання коштів

Злочинці, які базуються в ЄС, покладаються переважно на виробників, які базуються за кордоном, а потім організовують ввезення, транспортування, зберігання та розповсюдження підроблених товарів в ЄС. Однак деякі також є активними виробниками підроблених товарів в ЄС. Такому виробництву сприяє використання підроблених етикеток та упаковки, що ввозяться з-за меж ЄС та часто організовуються ОЗГ; є ознаки того, що така злочинність зростає.

ОЗГ, які беруть участь у шахрайстві з акцизами, значною мірою покладаються на використання легальних бізнес-структур. Це передбачає:

- створення підставних компаній;
- змову з ключовими працівниками митних органів та митних складів; та
- співпрацю з транспортними компаніями і дистриб'юторами.

Нещодавні справи, що ілюструють *алгоритм дій*:

1. У 2015 році компанія Panama Papers повідомила, що Девід Нахмад, відомий приватний колекціонер предметів мистецтва, був кінцевим власником картини Модільяні *«Чоловік з тростиною, що сидить»*. Нахмад придбав витвір мистецтва на аукціоні Крісті у 1996 році приблизно за 25 мільйонів доларів США через свій Міжнародний мистецький центр (IAC) у Панамі та зберігав його у Женевському вільному порту.

   Картина привернула увагу громадськості, коли онук Оскара Штіттінера, єврейського торговця антикваріатом, заявив, що нацисти вкрали її під час окупації Парижа у 1939 році. Органи влади Швейцарії спочатку конфіскували її, а пізніше повернули назад Нахмаду, коли позивач не зміг довести право власності, оскільки опис витвору мистецтва, який використовувався для підтвердження позову, був надто розпливчастим.

2. У звіті FATF у жовтні 2013 року про відмивання коштів та фінансування тероризму шляхом торгівлі алмазами повідомляється, що злочинці використовують алмази в якості валюти для того, щоб їх операції було складніше відстежувати.[134]

   У звіті наводиться приклад справи про шахрайство з алмазами на суму 800 мільйонів євро, що мала місце у Женевському вільному порту у 2005 році. Кур'єрська компанія, що базується в Антверпені, використовувала вільний порт для контрабанди дорогоцінного каміння, яке вона згодом продавала на чорному ринку Антверпена через офшорні компанії-оболонки.

Висновки: Рівень загрози відмивання коштів, пов'язаної з вільними портами, вважається значним (рівень 3).

Вразливість

Фінансування тероризму

Оцінка вразливості до фінансування тероризму, пов'язаної з вільними портами, свідчить про таке:

a) схильність до ризику

Вільні порти забезпечують секретність. Завдяки своєму пільговому режиму вони нагадують офшорні фінансові центри, які пропонують високу ступінь безпеки та свободу дій і дозволяють здійснювати операції, не привертаючи уваги регуляторів або органів прямого оподаткування. Хоча декларація вартості і є необхідною для товарів, які зберігаються у вільному порту чи на митному складі, це зазвичай має форму самодекларації власником або представником і у більшості випадків не перевіряється.

Товари, що перебувають у вільних портах або на митному складі, технічно є «транзитними», хоча у більшості вільних портів такого типу немає обмежень за часом. Товари можуть увійти у вільний порт, перебувати там протягом невизначеного терміну (при цьому набираючи вартість) та продаватися необмежену кількість разів без сплати жодного податку.

Крім конфіденційності, висока вартість грошових операцій, необізнаність правоохоронних органів з цінностями та портативний характер витворів мистецтва роблять ринок мистецтв зручним способом для здійснення незаконної діяльності з використанням вільних портів. Оскільки інші методи відмивання коштів піддаються більш пильному контролю, вважається, що контрабандисти, наркоторговці і торговці зброєю дедалі частіше звертаються до ринку предметів мистецтва.

b) обізнаність про ризики

Станом на 10 січня 2020 року оператори вільних портів та інші суб'єкти на ринку предметів мистецтва, такі як аукціонні будинки та галереї, стануть «зобов'язаними нефінансовими суб'єктами» відповідно до П'ятої директиви про боротьбу з відмиванням грошей. Виступаючи в якості «воротарів» ПВК, їм доведеться повідомляти про підозрілі операції підрозділам фінансової розвідки та здійснювати дослідження належної перевірки клієнтів для ідентифікації кінцевого бенефіціарного власника товарів, що зберігаються.

Після справи Був'є,[135] національні органи влади в односторонньому порядку вирішили застосувати вимоги щодо протидії відмиванню коштів у Люксембурзькому вільному порту, але операторам мав бути наданий пільговий період в один рік для оновлення своїх документів та узгодження своїх процедур з новими вимогами. Це свідчить про те, що обізнаність про ризики

[134] http://www.fatf-gafi.org/media/fatf/documents/reports/ML-TF-through-trade-in-diamonds.pdf
[135] https://www.newyorker.com/magazine/2016/02/08/the-bouvier-affair

все-таки зростає і що реалізація нових заходів може вимагати значної роботи з боку ліцензійних операторів, щоб адаптувати свою практику таким чином, аби вони могли визначати кінцевих бенефіціарних власників товарів, завезених їх клієнтами.

c) законодавча база і засоби контролю

Оскільки вони підпадають під дію положень щодо ПВК на рівні ЄС та на національному рівні, вільні порти більше регулюються в ЄС, ніж в інших країнах.

Основною сферою, в якій домовленості вільних портів дуже різняться, є їх політика щодо розкриття інформації – місцеві положення у деяких країнах є більш обтяжливими, ніж в інших.

Висновки: У разі анонімного використання, вільні порти є вразливими до фінансування тероризму. Рівень обізнаності в цьому секторі зростає, але все ще є недостатнім. Тому рівень вразливості до фінансування тероризму, пов'язаної з вільними портами, вважається значним (рівень 3).

Відмивання коштів

Вразливість до відмивання коштів не оцінюється окремо, вона оцінюється а на основі описаних вище притаманних факторів. Тим не менш, велика кількість випадків корупції, ухилення від сплати податків, злочинної діяльності та відмивання коштів, виявлених та врегульованих правоохоронними органами, вимагає спеціального розгляду.

Висновки: Вільні порти є вразливими до відмивання коштів у разі анонімного використання. Хоча рівень обізнаності сектора про ризик відмивання коштів здається вищим, ніж для фінансування тероризму, його структура та здатність забезпечити спеціальні ресурси і навчання є недостатніми. Тому рівень вразливості до відмивання коштів, пов'язаної з вільними портами, вважається дуже значним (рівень 4).

Пом'якшувальні заходи:

Існує можливість вдосконалити процедуру регулювання вільних портів ЄС.

Щоб уникнути плутанини, Комісія повинна усунути такі термінологічні невідповідності в П'ятій директиві про боротьбу з відмиванням грошей та Митному кодексі Союзу:

- П'ята директива про боротьбу з відмиванням грошей містить прямі посилання на вільні порти, але Митний кодекс Союзу охоплює їх лише як тип вільної зони; та
- у Митному кодексі Союзу процедура вільної зони має майже ті самі правові умови, що і митні склади. Це порушує питання про те, чи підпадають митні процедури та митні склади під сферу дії Директиви про боротьбу з відмиванням грошей. Оскільки ринок митних складів є значно більшим, ніж ринок вільних портів, це питання має бути роз'яснене до транспозиції П'ятої директиви про боротьбу з відмиванням грошей (січень 2020 року).

Держави-члени повинні:

- здійснювати регулярні незалежні аудиторські перевірки в області ПВК для функцій нормативно-правового дотримання узгодженими операторами вільних зон (УОВЗ), і забезпечувати належне та послідовне виконання процедур ПВК і контролю, які вже закріплені у законодавстві;
- гарантувати, що УОВЗ регулярно обмінюватимуться інформацією з відповідними органами з питань ПВК щодо кінцевих бенефіціарних власників та змін у праві власності на активи вільних портів;
- встановити розумне, відповідне обмеження за часом для зберігання товарів у вільних портах; та
- заохочувати європейський ринок предметів мистецтва, як одного з головних клієнтів вільних портів, здійснювати саморегулювання та підвищувати свою прозорість, особливо з огляду на те, що операції на ринку предметів мистецтва все ще характеризуються високим ризиком відмивання коштів через їх непрозорість та суб'єктивність оцінювання активів.

ГРОМАДЯНСТВО/ВИД НА ПРОЖИВАННЯ

1. Програми надання громадянства через інвестиції та схеми надання інвесторам виду на проживання

Продукт
«Золоті візи» та «золоті паспорти»

Сектор
Громадянство/вид на проживання

Загальний опис сектора та відповідного продукту/діяльності

Останніми часом спостерігається зростаюча тенденція у схемах надання інвесторам громадянства та виду на проживання. Вони спрямовані на залучення інвестицій у певну країну шляхом надання інвесторам громадянства або права на проживання. Такі схеми викликають занепокоєння в частині притаманних ризиків, зокрема щодо безпеки, відмивання коштів, ухилення від сплати податків[136] та корупції.

Схеми надання інвесторам громадянства часто називають «програмами надання громадянства через інвестиції», «громадянство на продаж» або «золоті паспорти». Вони дозволяють іноземцям бути натуралізованими як громадяни країни взамін на інвестиції за умови їх відповідності певним критеріям. Схеми надання інвесторам громадянства відрізняються від схем надання інвесторам виду на проживання («золота віза»), спрямованих на залучення інвестицій в обмін на вид на проживання у відповідній країні.

[136] Можливими зловживаннями є, наприклад, ухилення від сплати податків шляхом зловживання подвійним видом на проживання та ухилення від сплати податків – створення компанії без фізичної присутності, щоб скористатися податковими пільгами та низькими вимогами держави-члена, що пропонує схему надання інвесторам громадянства/виду на проживання.

Незважаючи на те, що в основі цих програм лежить законне економічне збагачення та диверсифікація для приймаючої країни,[137] повідомляється про випадки їх зловживання.

Як і при отриманні будь-якого другого громадянства, до переваг можна віднести легкість подорожування, право на проживання та ведення бізнесу. Це також може бути засобом переміщення активів за межі своєї країни походження, особливо у разі проживання у нестабільному політичному чи економічному середовищі або у разі незаконного одержання капіталу. Ці схеми можуть також використовуватися для уникнення притягнення до кримінальної відповідальності чи покарання у своїх країнах походження. Багато країн, які мають програми надання інвесторам громадянства є офшорними фінансовими центрами, чиї структури забезпечують безпеку, секретність та податкові пільги. Вони також можуть пропонувати людям більшу свободу дій у здійсненні операцій з глобальними фінансовими центрами, враховуючи (набутий) статус учасника як місцевий, який, таким чином, підпорядковується менш суворому контролю.

Опис сектора у межах ЄС

В ЄС три держави-члени (Болгарія, Кіпр та Мальта) використовують **схеми надання інвесторам громадянства**, коли громадянство надається за менш жорстких умов, ніж за звичайних режимів натуралізації, зокрема без чинного попереднього проживання у відповідній країні.[138] Такі схеми мають наслідки для Європейського Союзу в цілому, оскільки кожна особа, яка має громадянство держави-члена, одночасно є громадянином ЄС. Дійсно, незважаючи на те, що це національні схеми, вони свідомо продаються на ринку і часто явно рекламуються як засіб набуття громадянства ЄС, разом з усіма пов'язаними з ними правами та привілеями, зокрема, правом на вільне пересування.

Схеми надання інвесторам виду на проживання існують у 20 державах-членах ЄС:[139] Болгарії, Чехії, Естонії, Ірландії, Греції, Іспанії, Франції, Хорватії, Італії, Кіпрі, Латвії, Литві, Люксембургу, Мальті, Нідерландах, Польщі, Португалії, Румунії, Словаччині та Об'єднаному Королівстві. Ризики, притаманні таким схемам, схожі на ризики, характерні для схем надання інвесторам громадянства. Більше того, ці схеми мають вплив на інші держави-члени, оскільки чинний дозвіл на проживання надає громадянам третіх країн певні права на вільне пересування, зокрема у Шенгенській зоні.

Європейський Парламент у своїй Резолюції від 16 січня 2014 року[140] висловив занепокоєння тим, що національні схеми, пов'язані з «прямим або непрямим продажем» громадянства ЄС, підірвали саму його концепцію. Він закликав Комісію оцінити різні національні схеми надання громадянства у світлі європейських цінностей, а також сутності і духу законодавства та практики ЄС.

У своєму звіті про громадянство 2017 року[141] Комісія опублікувала звіт про національні схеми

[137] Перша програма надання інвесторам громадянства була створена у Сент-Кітс і Невісі у 1984 році як засіб відновлення економіки. Її успіх спонукав багато інших країн слідувати цьому прикладу.
[138] Інвестори зобов'язані інвестувати від 800 тисяч до 2 мільйонів євро.
[139] Два переліки збігаються, оскільки три країни - Болгарія, Кіпр та Мальта - торгують обома.
[140] Постанова Європейського Парламенту від 16 січня 2014 року про громадянство ЄС для продажу (2013/2995(RSP)): http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0038&language=EN&ring=P7-RC-2014-0015
[141] Звіт Комісії до Європейського Парламенту, Ради, Європейського економічного та соціального комітету та Комітету регіонів *«Зміцнення прав громадян у Союзі демократичних змін: Звіт про громадянство ЄС 2017 року* (COM(2017) 030 final). Доступний за посиланням: https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=51132

надання інвесторам громадянства ЄС. У звіті описано заходи Комісії у цій галузі та вивчено діюче національне законодавство і практики, з наданням рекомендацій державам-членам. Для підготовки звіту Комісія доручила вивчити законодавство та практику щодо схем надання громадянства та виду на проживання у всіх відповідних державах-членах[142] та організувала консультації з державами-членами. Звіт також враховує інші відповідні джерела, включаючи останні публікації на цю тему,[143] та був опублікований у січні 2019 року.[144]

Після публікації звіту Комісія створила групу експертів із держав-членів для вивчення конкретних ризиків, пов'язаних зі схемами надання інвесторам громадянства, а також для врегулювання аспектів прозорості та належного управління щодо впровадження як схем надання інвесторам громадянства, так і схем надання інвесторам виду на проживання. Очікується, що до кінця 2019 року група експертів розробить загальний набір перевірок безпеки для схем надання інвесторам громадянства, включаючи конкретні процеси управління ризиками з урахуванням питань безпеки, відмивання коштів, ухилення від сплати податків та корупційних ризиків.

Загроза

Громадяни третіх країн можуть інвестувати у державу-члена на законних підставах[145], але можуть також переслідувати нелегітимні цілі, такі як ухилення від розслідування правопорядку та притягнення до кримінальної відповідальності у своїй країні або захист своїх активів від заходів заморожування та конфіскації. Отже, схеми надання інвесторам громадянства та виду на проживання створюють низку ризиків для країн-членів та для ЄС в цілому: зокрема, ризики для безпеки, включаючи можливість проникнення з боку організованих злочинних груп, які не входять до складу ЄС, а також ризики відмивання коштів, корупції та ухилення від сплати податків. Такі ризики посилюються прикордонними правами, пов'язаними з громадянством або видом на проживання у державі-члені ЄС.

Також спостерігається занепокоєність відсутністю прозорості та управління схемами. Як схеми надання громадянства, так і схеми надання виду на проживання підлягають суворому державному контролю у разі звинувачень у зловживанні та корупції, пов'язаних з ними у деяких державах-членах.[146] Більше того, процедура перевірки заявників часто передається приватним компаніям, якщо існує постійний ризик конфлікту інтересів та корупції. Підвищення прозорості та створення належних механізмів управління ризиками, систем контролю та механізмів нагляду можуть допомогти максимально пом'якшити деякі з цих проблем.

---

[142] Дослідження фактів. Milieu Law and Policy Consulting, *Фактичний аналіз схем для інвесторів держав-членів, що надають громадянство або вид на проживання громадянам третіх країн, які здійснюють інвестиції зазначеній державі-члені*, Брюссель 2018.

[143] Див., зокрема, Європейська парламентська служба досліджень, *Схеми надання інвесторам громадянства та виду на проживання в ЄС: Стан справ, проблеми та наслідки*, жовтень 2018 року. http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2018)627128
Transparency International/Global Witness, *Європейська втеча – у примарному світі «золотих віз»*, жовтень 2018, https://www.transparency.org/whatwedo/publication/golden_visas

[144] Звіт Комісії до Європейського Парламенту, Ради, Європейського економічно-соціального комітету та Комітету регіонів, *Схеми надання інвесторам громадянства та права на проживання* (COM (2019) 12 final. https://ec.europa.eu/info/sites/info/files/com_2019_12_final_report.pdf

[145] Відповідно до статті 63 ДФЄС, принцип вільного переміщення капіталу застосовується між державами-членами та між державами-членами і третіми країнами. Стаття 65 дозволяє обмежувати вільне переміщення капіталу, зокрема, з причин, пов'язаних з державною політикою, громадською безпекою чи оподаткуванням.

[146] Наприклад, у 2009 році австрійський політик заявив потенційному російському інвестору, що він може одержати громадянство Австрії в обмін на інвестицію у розмірі 5 мільйонів євро та здійснення пожертвування для його партії. Докладний виклад звітів про зловживання або неправильне використання схем міститься у дослідженні, згаданому у виносці 5.

Існує низка способів, за допомогою яких можна зловживати схемами надання громадянства або виду на проживання в ЄС для цілей оподаткування. Фізичні особи можуть декларувати місце проживання в одній із цих юрисдикцій, проте їх реальне податкове місце проживання може знаходитися в іншій юрисдикції (подвійне зловживання видом на проживання). Відповідно до договорів обміну інформацією між юрисдикціями інформація для цілей оподаткування може надсилатися до неправильної юрисдикції місця проживання. Що стосується ухилення від сплати податків, управління бізнес-структурами може бути встановлено у юрисдикціях зі схемами надання громадянства чи виду на проживання в ЄС, які мають низькі вимоги до виду на проживання, що не відповідають міжнародним нормам протидії ухиленню від сплати податків, наприклад, не потребують суттєвої комерційної діяльності, та/або в яких бізнес-структура може користуватися податковими режимами, які сприяють агресивному податковому плануванню.

Крім того, конкуренція між державами-членами за клієнтів, які бажають набути громадянство або вид на проживання за допомогою інвестиційних схем, ризикує викликати «перегони за низхідною» в частині стандартів належної перевірки та прозорості.

Фінансування тероризму

Оцінка загрози фінансування тероризму, пов'язаної із золотими візами/паспортами, визначила такі проблеми, які викликають занепокоєння:

- **Перевірки безпеки**: Законодавством ЄС передбачені певні зобов'язання щодо безпеки, які необхідно виконати перед тим, як видавати візу чи дозвіл на проживання іноземним інвесторам. Однак бракує наявної інформації щодо практичної реалізації та свободи дій в частині того, як держави-члени підходять до питань безпеки.

- **Вимоги до фізичного місця проживання:** Дозволи на проживання, отримані за рахунок інвестицій, з обмеженою або необов'язковою фізичною присутністю інвестора у відповідній державі-члені, можуть впливати на застосування статусу довгострокового проживання в ЄС та пов'язаних з цим прав, і можуть навіть забезпечити швидке відстеження національного, а отже європейського громадянства.

- **Відсутність прозорості:** У звіті наголошується на недостатній прозорості та нагляді за схемами, зокрема, в частині моніторингу, а також на відсутності статистики щодо того, скільки людей отримують дозвіл на проживання за допомогою таких схем.

Висновки: У цьому контексті, рівень загрози фінансування тероризму, пов'язаної із золотими візами/паспортами, вважається значним/дуже значним (рівень 3/4).

Відмивання коштів

<u>Приклади юрисдикцій, які залучили заможних людей, що причетні до відмивання коштів:</u>

Останнім часом Кіпр став фінансовим притулком для українських та російських олігархів та осередком операцій з відмивання коштів. Частково це пояснюється його програмою надання громадянства через інвестиції: заможні іноземці можуть стати громадянами менше ніж за 6 місяців в обмін на здійснення інвестицій у розмірі 2 мільйонів євро. Майже половина з 2 000 паспортів, виданих за схемою за останні 2 роки, були придбані росіянами. Такі інвестиції можуть легітимізувати відмиті кошти, а кіпрське громадянство може полегшити переказ грошей у країну та на європейський фінансовий ринок. Кіпр також користується популярністю, оскільки є країною податкових пільг.

Мальтійське громадянство так само популярне серед заможних росіян. Громадяни Саудівської Аравії також інвестують у цю схему: наприклад, Уелід аль-Ібрагім, голова Центру радіомовлення на Близькому Сході. Аль-Ібрагім був заарештований у листопаді 2017 року у ході програми корупційної чистки.[147]

Для відмивання коштів також використовуються паспорти Карибських островів. Фізична особа, пов'язана зі скандалом азербайджанського ландромату, була громадянином Пакистану, який також мав громадянство Сент-Кітсу і Невісу; цілком імовірно, що метою одержання цього громадянства було приховування активів.

Золоті візи також використовуються для уникнення санкцій

Після введення економічних санкцій з боку ЄС та США, заборон на отримання віз та замороження активів Росії після вторгнення в Україну та незаконної анексії Криму в 2014 році, спостерігається зростання російських заяв на участь у програмах надання громадянства через інвестиції; це спричинило ризик ухилення від санкцій на додаток до можливого відмивання незаконних коштів.

Громадянам Північної Кореї раніше також вдалося отримати альтернативні паспорти, які вони потім використовували для ведення діяльності за межами Північної Кореї – за допомогою паспортів Кірібаті та Сейшельських островів були ідентифіковані двоє північнокорейців, які працювали у Гонконгу та Японії. Хоча обидві країни нібито скасували цю схему, вважається, що їх паспорти були видані після стверджуваної дати скасування.

Нарешті, програма надання інвесторам громадянства Коморських островів отримала негативні відгуки у пресі: на початку січня 2018 року уряд Коморських островів скасував 170 паспортів, які були нібито неналежним чином видані іноземцям, у тому числі багатьом іранцям, під час перебування на посаді попереднього уряду. Влада Коморських островів встановила, що принаймні двоє іноземних власників паспортів Коморських островів, за твердженнями органів влади США, порушили санкції проти Ірану (хоча у жодному разі само по собі громадянство Коморських островів не впливає на ухилення).

Таким чином, основним ризиком цих схем є **схильність до ризику відмивання коштів**. Існує чіткий і визначений ризик того, що певним клієнтам могли бути приписані нижчі рівні ризику (залежно від їх національності), ніж гарантовано. Це могло вплинути на рівень здійснюваної належної перевірки клієнтів та/або моніторингу операцій. Це може призвести до очищення операцій, які, хоча і є доброчесними, повинні були пройти більш ретельний контроль з огляну на основні обставини.

[147] Див., загалом: www.transparency.org/whatwedo/publication/golden_visas
Також:
https://www.maltatoday.com.mt/news/national/83539/russian_nationals_dominate_list_of_global_rich_who_are_now_maltese#.XSxUtCBS-Uk
http://www.independent.com.mt/articles/2018-12-30/local-news/Turkish-billionaires-and-Russian-industry-moguls-meet-Malta-s-new-citizens-6736201441

Висновки: У світлі вищеописаного сценарію, рівень загрози відмивання коштів, пов'язаної із золотими візами/паспортами, вважається значним/дуже значним (рівень 3/4).

Вразливість

Фінансування тероризму

Оцінка вразливості до фінансування тероризму, пов'язаної із золотими візами/паспортами, визначила такі проблеми, які викликають занепокоєння:

a) схильність до ризику

Двома основними проблемами, які оцінюються європейськими установами, є безпека та прозорість і інформація. Що стосується безпеки, було встановлено, що перевірки, які здійснюються щодо заявників, не є достатньо надійними, і що власні централізовані інформаційні системи ЄС, такі як Шенгенська інформаційна система, не використовуються так систематично, як це має бути. Що стосується прозорості та інформації, бракує чіткої інформації про те, як працюють схеми, у тому числі щодо кількості отриманих, наданих чи відхилених заявок та походження заявників. Крім того, держави-члени не обмінюються інформацією щодо заявників таких схем, а також не інформують один одного про відхилених заявників.

b) обізнаність про ризики

Задіяні національні органи влади, здається, не обізнані про проблеми, пов'язані з цими схемами, або, у найгіршому випадку, охоче беруть на себе притаманні ризики схем в обмін на очікувані інвестиції.[148]

Нещодавні скандали, про які повідомлялося в ЗМІ, свідчать про те, що деякі країни ЄС не встановили стандартної процедури проведення розширених перевірок заявників, членів їх родин та походження їх коштів.

c) законодавча база і засоби контролю

Перевірки безпеки: Законодавством ЄС передбачені певні зобов'язання щодо безпеки, які необхідно виконати перед тим, як видавати візу чи дозвіл на проживання іноземним інвесторам. Однак бракує наявної інформації щодо практичної реалізації та свободи дій в частині того, як держави-члени підходять до питань безпеки.

Вимоги до фізичного місця проживання: Дозволи на проживання, отримані за рахунок інвестицій, з обмеженою або необов'язковою фізичною присутністю інвестора у відповідній державі-члені, можуть впливати на застосування статусу довгострокового проживання в ЄС та пов'язаних з цим прав, а також можуть навіть забезпечити швидке відстеження національного, а отже європейського громадянства.

[148] Робочий документ МВФ, WP/15/93, Надто багато хорошого?: Розумне управління вхідними потоками за програмами надання громадянства: Сінь Сю, Ахмед Ель-Ашрам та Джудіт Голд https://www.imf.org/external/pubs/ft/wp/2015/wp1593.pdf

Висновки: У цьому контексті, рівень вразливості до фінансування тероризму, пов'язаної із золотими візами/паспортами, вважається значним/дуже значним (рівень 3/4).

Відмивання коштів

Оцінка вразливості до відмивання коштів спирається на ті самі фактори, які описані вище, і не розглядається окремо. Тим не менш, необхідно враховувати її високу вразливість, у світлі високого рівня корупції, ухилення від сплати податків, злочинної діяльності та відмивання коштів, виявлених та досліджених правоохоронними органами.

Висновки: У цьому контексті, рівень вразливості до відмивання коштів, пов'язаної із золотими візами/паспортами, вважається дуже значним (рівень 4).

Пом'якшувальні заходи:

Описані схеми є спільними для ЄС, оскільки кожна особа, яка набуває громадянство однієї держави-члена, одночасно набуває **громадянство в ЄС**. Рішення однієї держави-члена про надання громадянства взамін на інвестиції автоматично надає права стосовно інших держав-членів, зокрема право вільного переміщення та доступу до внутрішнього ринку ЄС для здійснення економічної діяльності, а також право голосу та бути обраним на європейських та місцевих виборах. На практиці ці схеми часто рекламуються як засіб набуття громадянства ЄС разом із усіма пов'язаними з цим правами та привілеями.

Крім основних етичних міркувань щодо продажу громадянства та тривожного згадування про те, що деякі держави-члени отримують прибуток від продажу спільного європейського активу, існує чітка і характерна низка ризиків, пов'язаних із цими схемами.

Для Комісії:

Комісія здійснюватиме **моніторинг більш широких питань дотримання законодавства ЄС**, порушених схемами надання інвесторам громадянства та виду на проживання, та вживатиме необхідних заходів. З цієї причини державам-членам необхідно, зокрема, забезпечити:

- систематичне виконання всіх обов'язкових прикордонних перевірок та перевірок безпеки;
- належне виконання вимог Директиви про надання довгострокового дозволу на проживання та Директиви про возз'єднання родини;
- оцінку коштів, сплачених заявниками за отримання громадянства та виду на проживання в обмін на інвестиції, згідно з **правилами ЄС щодо протидії відмиванню коштів**;
- **Директива 2018/822/ЄС**[149], яка вимагає від посередників надання інформації про підзвітні транскордонні податкові домовленості їх національним органам влади,[150]

[149] Директива Ради (ЄС) 2018/822 від 25 травня 2018 року про внесення змін до Директиви 2011/16/ЄС стосовно обов'язкового автоматичного обміну інформацією у сфері оподаткування щодо підзвітних транскордонних схем; OB L 139, 05.06.2018, с. 1-13.

[150] Адміністративна співпраця у (прямому) оподаткування в ЄС: https://ec.europa.eu/taxation_customs/business/tax-cooperation-control/administrative-cooperation/enhanced-administrative-cooperation-field-direct-taxation_en.

набирає чинності з 2020 року;

- Комісія має намір стежити за заходами, яких вживають держави-члени для вирішення питань прозорості та управління такими схемами. Вона створила **групу експертів з держав-членів** для підвищення прозорості, управління та безпеки схем. Зокрема, така група має наступні завдання:

  - створення системи обміну інформацією та консультацій щодо кількості отриманих заявок, країн походження та кількості дозволів на громадянство та проживання, наданих/відхилених державами-членами фізичним особам на основі інвестицій;

  - розробка загального набору перевірок безпеки для схем надання інвесторам громадянства, включаючи конкретні процеси управління ризиками, до кінця 2019 року.

Нарешті, стосовно третіх країн, які встановлюють подібні схеми, що можуть мати наслідки для безпеки для ЄС, Комісія має намір відслідковувати схеми надання інвесторам громадянства у країнах-кандидатах та потенційних кандидатах у рамках процесу вступу до ЄС. Вона також буде відстежувати вплив таких схем у безвізових країнах ЄС у рамках механізму призупинення дії віз.

Для держав-членів:

Держави-члени повинні забезпечити прозорість та належне управління у реалізації схем для врегулювання, зокрема, ризиків проникнення в економіку ЄС з боку організованих злочинних груп, які не є членами ЄС, а також ризиків відмивання коштів, корупції та ухилення від сплати податків. Дії держав-членів повинні включати:

- щорічне звітування, які оприлюднюються;
- переконання в тому, що звіти містять дані про кількість отриманих заяв, країни походження та кількість наданих та відхилених дозволів на громадянства та вид на проживання, разом з інформацією про особу та країну походження новоприйнятих мешканців та громадян;
- надання дезагрегованої статистики щодо схем надання інвесторам виду на проживання, щоб можна було визначити підставу для набуття виду на проживання або ідентифікувати обрану опцію інвестування;
- впровадження процесу управління ризиками, включаючи відповідну ідентифікацію, класифікацію та пом'якшення ризиків, під координуванням призначеного національного органу. Моніторинг реалізації плану;
- здійснення щорічних аудиторських перевірок для оцінки реалізації плану управління ризиками;
- у контексті **ухилення від сплати податків та ризиків ухилення від сплати податків**, у законодавчій базі ЄС є інструменти для адміністративного співробітництва (Директива 2011/16/ЄС[151]), зокрема, спонтанний обмін інформацією, що дозволить, наприклад, компетентним органам держави-члена зі схемами надання громадянства/виду на проживання через інвестиції повідомити державу-члена проживання фізичної особи, яка користується такою схемою.

[151] https://ec.europa.eu/taxation_customs/business/tax-cooperation-control/administrative-cooperation/enhanced-administrative-cooperation-field-direct-taxation_en

Держави-члени також повинні уточнити та оприлюднити критерії для оцінки заяв та перевірок безпеки, що здійснюються в рамках схеми, а також забезпечити регулярний *подальший* моніторинг відповідності цим критеріям, зокрема, в частині інвестицій, здійснюваних заявником. Вони також повинні запровадити процедуру відкликання дозволів, якщо критерії більше не виконуватимуться.

І останнє, але не менш важливе, держави-члени повинні також запропонувати повну прозорість процесів, яка має бути забезпечена у разі передачі права на управління цими схемами приватним компаніям, аж до включення інформації про бенефіціарне право власності таких компаній. За жодних обставин такі приватні компанії не повинні залучатися до фактичної перевірки інформації та документів, наданих заявниками: ці перевірки повинні залишатися під контролем відповідальних державних органів, а не приватних суб'єктів.

ДОДАТОК 2 – ЗАКОНОДАВЧА БАЗА ЄС ЩОДО БОРОТЬБИ З ВІДМИВАННЯМ КОШТІВ ТА ПРОТИДІЇ ФІНАНСУВАННЮ ТЕРОРИЗМУ

Законодавство ЄС про фінансові послуги та нагляд, що має значення для сфери ПВК/ФТ, на основі статті 53 та статті 114 ДФЄС:

- Директива (ЄС) 2015/2366 про надання платіжних послуг на внутрішньому ринку, що вносить зміни до Директив 2002/65/ЄС, 2009/110/ЄС та 2013/36/ЄС і Регламенту (ЄС) № 1093/2010 та скасовує Директиву 2007/64/ЄС.
- Директива 2009/110/ЄС щодо започаткування та здійснення діяльності установами – емітентами електронних грошей та пруденційний нагляд за ними, що вносить зміни до Директив 2005/60/ЄС та 2006/48/ЄС, та скасовує Директиву 2000/46/ЄС.
- Директива 2014/65/ЄС про ринки фінансових інструментів та про внесення змін до Директиви 2002/92/ЄС та Директиви 2011/61/ЄС.
- Директива 2013/36/ЄС про доступ до діяльності кредитних установ і пруденційний нагляд за кредитними установами та інвестиційними фірмами, що вносить зміни до Директиви 2002/87/ЄС та скасовує Директиви 2006/48/ЄС та 2006/49/ЄС.

Додаткове законодавство ЄС було прийнято у сфері ПВК/ФТ на основі статті 114 ДФЄС та статті 33 стосовно контролю над переміщенням готівкових коштів на зовнішньому кордоні ЄС:

- Регламент (ЄС) 2018/1672 про контроль ввезення в ЄС та вивезення з ЄС готівкових коштів і про скасування Регламенту (ЄС) № 1889/2005 (новий Регламент про контроль готівкових коштів).

Додаткові превентивні положення:

- Директива (ЄС) 2018/1673 про боротьбу з відмиванням грошей за кримінальним правом.
- Регламент (ЄС) 2019/880 про впровадження та імпорт культурних товарів.[152]

Інші сфери, що стосуються ПВК/ФТ, підпадають під дію законодавства ЄС, прийнятого у сфері протидії фінансуванню тероризму на основі статті 215, статті 75 та статті 352 ДФЄС – запровадження цільових фінансових санкцій:

- Регламент Ради (ЄС) № 2580/2001 про встановлення спеціальних обмежувальних заходів по відношенню до окремих осіб та організацій в цілях боротьби з тероризмом.
- Регламент Ради (ЄС) № 881/2002 про вжиття обмежувальних заходів, спрямованих проти певних осіб та організацій, пов'язаних з Усамою бен Ладеном, Аль-Каїдою і Талібаном, який скасовує Регламент Ради (ЄС) № 467/2001 про заборону експорту певних товарів та послуг до Афганістану, посилення заборони на польоти та продовження заморожування коштів та інших фінансових ресурсів стосовно Талібану в Афганістані.
- Регламент Ради (ЄС) № 267/2012 щодо обмежувальних заходів проти Ірану, який скасовує Регламент (ЄС) № 961/2010.

Законодавство ЄС, прийняте у сфері ПВК/ФТ на основі положень ДФЄС у сфері свободи, безпеки та правосуддя

- Рішення Ради 2000/642/ЈНА відносно домовленостей про співпрацю між підрозділами фінансової розвідки держав-членів у плані обміну інформацією.
- Рішення Ради 2007/845/ЈНА щодо співпраці між офісами з повернення активів держав-членів у сфері розшуку та виявлення доходів від злочинів або іншого майна, пов'язаного зі злочинами.
- Рамкове рішення Ради 2001/500/ЈНА про відмивання грошей, ідентифікацію, відстеження, замороження, арешт та конфіскацію знарядь злочинів та доходів від них.
- Директива (ЄС) 2017/541 про боротьбу з тероризмом, яка замінює Рамкове рішення Ради 2002/475/ЈНА та вносить зміни до Рішення Ради 2005/671/ЈНА.
- Рамкове рішення Ради 2005/212/ЈНА про конфіскацію доходів, знарядь та майна, пов'язаних із злочинами.
- Рамкове рішення Ради 2003/577/ЈНА про виконання у Європейському Союзі ордерів на арешт майна або доказів.
- Рамкове рішення Ради 2006/783/ЈНА про застосування принципів взаємного визнання постанов про конфіскацію.

[152] Регламент (ЄС) 2019/880 Європейського Парламенту та Ради від 17 квітня 2019 року про впровадження та імпорт культурних товарів; PE/82/2018/REV/1; OB L 151, 07.06.2019, с. 1-14.

- Директива 2014/41/ЄС про Європейський слідчий ордер у кримінальних справах.
- Директива 2014/42/ЄС про замороження і конфіскацію засобів здійснення злочинів і доходів, одержаних злочинним шляхом, у Європейському Союзі.

ДОДАТОК 3 – ГЛОСАРІЙ

Акроніми та абревіатури, пов'язані з протидією відмивання коштів	
Акронім	**Значення**
ACH	Автоматизована розрахункова палата
AML/CFT (ПВК/ФТ)	Протидія відмиванню коштів/фінансуванню тероризму
AMLID	Міжнародна база даних з питань протидії відмиванню коштів
APG	Азіатсько-тихоокеанська група з питань відмивання коштів
API	Уповноважені платіжні установи
APT	Траст для захисту активів
ARS	Альтернативна система переказу грошових коштів
ATM	Банкомат
BO	Бенефіціарний власник
BSA	Закон про банківську таємницю
CCR	Регламент про контроль готівки
CCTV	Система телевізійного спостереження
CDD	Належна перевірка клієнтів
CIP	Програма ідентифікації клієнтів
CTR	Звіт про валютні операції
DNFBPs (УНФПП)	Встановлені нефінансові підприємства і професії
EAG	Євразійська група з протидії легалізації злочинних доходів і фінансуванню тероризму
EBA	Європейська служба банківського нагляду http://www.eba.europa.eu/
ECB (ЄЦБ)	Європейський центральний банк
ECEF	Електронна папка продовження розгляду
EDD	Розширена належна перевірка клієнтів
EFT	Електронний переказ коштів

EGMLTF	Експертна група з питань відмивання коштів та фінансуванням тероризму (E02914)
Egmont Group (Егмонтська група)	Егмонтська група підрозділів фінансової розвідки (неофіційна міжнародна мережа підрозділів фінансової розвідки)
EIOPA	Європейська організація страхування та пенсійного забезпечення https://eiopa.europa.eu/
ESAs	Три Європейські органи нагляду (EBA, EIOPA та ESMA)
ESAAMLG	Група боротьби з відмиванням коштів у Східній та Південній Африці
ESMA	Європейське управління з цінних паперів та ринків https://www.esma.europa.eu/
FATF	Група з розробки фінансових заходів боротьби з відмиванням грошей www.fatf-gafi.org FATF була заснована у 1989 році Групою семи промислових держав для сприяння встановленню національних та глобальних заходів боротьби з відмиванням коштів. Це міжнародний орган, який розробляє політику, а також встановлює стандарти боротьби з відмиванням коштів та заходи протидії фінансуванню тероризму в усьому світі. Її Рекомендації не мають сили закону. До її складу входять тридцять п'ять країн та дві міжнародні організації. У 2012 році FATF переглянула свої Рекомендації 40 + 9 та скоротила їх до 40. http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html FATF розробляє щорічні типологічні звіти, в яких відображаються поточні тенденції та методи відмивання коштів та фінансування тероризму.
FI	Фінансова установа
FinCEN	Мережа з питань боротьби з фінансовими злочинами
FinTech	Фінансові послуги на основі та за підтримки технологій
FIU (ПФР)	Підрозділи фінансової розвідки
FSRB	Регіональний орган по типу Групи з розробки фінансових заходів боротьби з відмиванням грошей
FTF	Іноземні бойовики-терористи
GAFILAT	Група з розробки фінансових заходів боротьби з відмиванням грошей у країнах Латинської Америки

GDP (ВВП)	Валовий внутрішній продукт
IA	Оцінка впливу
IBC	Міжнародна комерційна компанія
IVTS	Неформальна система переказу коштів
KYC	«Знай свого клієнта»
KYE	«Знай свого працівника»
LEA	Правоохоронний орган
MER	Звіт про взаємну оцінку
ML (ВК)	Відмивання коштів
MENAFATF	Група з розробки фінансових заходів боротьби з відмиванням грошей на Ближньому Сході та у Північній Африці
MLAT	Договір про взаємну правову допомогу
MLRO	Службовець, відповідальний за звітування щодо операцій по відмиванню коштів
MONEYVAL	Спеціальний експертний комітет для оцінки заходів боротьби з відмиванням грошей Ради Європи https://www.coe.int/en/web/moneyval Іменований раніше PC-R-EV, комітет був створений у 1997 році Комітетом Міністрів Ради Європи для проведення самооцінки та взаємної оцінки заходів протидії відмиванню коштів, що застосовуються у країнах Ради Європи, які не є членами FATF. MONEYVAL – це підкомітет Європейського комітету з проблем злочинності Ради Європи (CDPC).
MOU	Меморандум про взаєморозуміння
MSB	Підприємства, які надають розрахунково-касові послуги
MVTS	Послуги переказу грошових коштів
NPO	Некомерційні організації
NRA	Національна оцінка ризиків
OCG (ОЗГ)	Організована злочинна група
OECD (ОЕСР)	Організація економічного співробітництва та розвитку http://www.oecd.org/

	Міжнародна організація, яка допомагає урядам у вирішенні питань економічного розвитку у світовій економіці. OECP має секретаріат FATF у Парижі.
OFC	Офшорний фінансовий центр
PEP	Впливова політична особа
PIC	Приватна інвестиційна компанія
PSD	Директива про надання платіжних послуг
RBA	Підхід на основі ризиків
ROE	Звіт про результати розгляду
SAR	Звіт про підозрілу діяльність
SNRA	Наднаціональна оцінка ризиків
SPSP	Невеликі провайдери платіжних послуг
STR	Звіти про підозрілі операції
TBML	Відмивання коштів на основі торговельної діяльності
TCSPs	Особи, які надають послуги з управління фондами та компаніями
TF (ФТ)	Фінансування тероризму
TI	Transparency International https://www.transparency.org/ Недержавна організація, яка базується в Берліні і метою якої є підвищення відповідальності уряду та стримування як міжнародної, так і національної корупції. Заснована у 1993 році, TI працює приблизно у 100 країнах. Вона щодня публікує «корупційні новини» на своєму веб-сайті та зберігає архів новин та статей, пов'язаних з корупцією. Її система онлайн досліджень та інформації з питань корупції, або CORIS, є найбільш комплексною глобальною базою даних про корупцію. TI найвідоміша за свій щорічний Індекс сприйняття корупції (CPI), який забезпечує рейтинг країн за рівнями корупції серед державних чиновників; Індекс хабарників (BPI), який забезпечує рейтинг провідних країн-експортерів за їх схильністю до хабарництва. Щорічний глобальний звіт про корупцію TI поєднує індекси CPI та BPI і забезпечує рейтинг кожної країни за її загальним рівнем корупції. Переліки допомагають фінансовим установам визначити ризик, пов'язаний з певною юрисдикцією.
UBO	Кінцевий бенефіціарний власник

UCITS	Організація колективного інвестування у переказні цінні папери
UTR	Звіт про нестандартні операції

ДОДАТОК 4 – ПЕРЛІК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1/ Документація Комісії

Лютий 2016 – Повідомлення Комісії до Європейського Парламенту та Ради щодо Плану дій щодо посилення боротьби з фінансуванням тероризму. https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52016DC0050

Березень 2016 — Робочий документ персоналу Комісії про рух капіталу та свободу платежів (SWD(2016) 105).
https://ec.europa.eu/.../documents/2019-capital-market-monitoring-analysis_en.pdf

Липень 2016 — Оцінка впливу, яка додається до Пропозиції щодо Директиви Європейського Парламенту та Ради про внесення змін до Директиви (ЄС) 2015/849 про запобігання використанню фінансової системи для відмивання коштів або фінансування тероризму та про внесення змін до Директиви 2009/101/ЄС.
http://eur-lex.europa.eu/legal- content/EN/TXT/PDF/?uri=CELEX:52016SC0223&from=EN

Листопад 2016 — Початкова оцінка впливу — Імпорт культурних товарів. http://ec.europa.eu/smart-regulation/roadmaps/docs/2017_taxud_004_cultural_goods_synthesis_en.pdf

Грудень 2016 — Оцінка впливу, яка додається до Пропозиції щодо Регламенту Європейського Парламенту та Ради про контроль ввезення в ЄС або вивезення з ЄС готівкових коштів, яка скасовує Регламент (ЄС) № 1889/2005.
http://eur-lex.europa.eu/legal- content/EN/TXT/PDF/?uri=CELEX:52016SC0470&from=EN

Січень 2017 – Початкова оцінка впливу — Пропозиція щодо ініціативи ЄС стосовно обмежень на готівкові платежі.
http://ec.europa.eu/smart- regulation/roadmaps/docs/plan_2016_028_cash_restrictions_en.pdf

Січень 2017 – Зміцнення прав громадян у Союзі демократичних змін ЄС.
Звіт про громадянство 2017
https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52017DC0030

Червень 2017 – Робочий документ персоналу Комісії щодо поліпшення співпраці між підрозділами фінансової розвідки ЄС
https://ec.europa.eu/newsroom/document.cfm?doc_id=45318

Грудень 2017 – Ідентифікація ринкових та регуляторних перешкод для транскордонного розвитку «краудфандингу» в ЄС
https://ec.europa.eu/info/publications/171216-crowdfunding-regulatory-obstacles- crossborder-development_en

Березень 2018 – Пропозиція Комісії щодо регламенту про європейських провайдерів послуг «краудфандингу».
https://ec.europa.eu/info/publications/180308-proposal-crowdfunding_en

Березень 2018 – План дій FinTech: Для більш конкурентоспроможного та інноваційного європейського фінансового сектора.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0109

Січень 2019 – Схеми надання інвесторам громадянства та виду на проживання у Європейському Союзі. https://ec.europa.eu/info/sites/info/files/com_2019_12_final_report.pdf

Березень 2019 – Повідомлення Комісії до Європейського Парламенту, Європейської Ради, Ради та Європейського центрального банку про поглиблення економічного валютного союзу Європи: Підведення підсумків через чотири роки після публікації Доповіді п'яти президентів. https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-migration/20190306_com-2019-126-report_en.pdf

2/ Документація Європейського Парламенту

2018 – Комітет EP/ECON: Наглядовий підхід до боротьби з відмиванням коштів: аналіз презентації Спільної робочої групи
http://www.europarl.europa.eu/RegData/etudes/IDAN/2018/624424/IPOL_IDA(2018)62 4424_EN.pdf

2018 – Комітет EP/ECON: Відмивання коштів – Нещодавні справи з точки зору банківського нагляду ЄС
http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_IDA(2018) 614496

2018 – Комітет EP/ECON: Віртуальні валюти. Monetary Dialogue, липень 2018
http://www.europarl.europa.eu/cmsdata/149902/KIEL_FINAL%20publication.pdf

2018 – Комітет EP/ECON: Віртуальні валюти в Євросистемі: майбутні виклики. Monetary Dialogue, липень 2018
http://www.europarl.europa.eu/cmsdata/150541/DIW_FINAL%20publication.pdf

2018 – Комітет EP/TERR: Віртуальні валюти та фінансування тероризму: оцінка ризиків та оцінка відповідей
http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)6 04970_EN.pdf

2018 – Схеми надання інвесторам громадянства та виду на проживання в ЄС: Стан справ, питання та наслідки
www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2018)627128

3/ Звіти Євростату

Статистика приватних переказів, Statistics explained, Eurostat - 2017.
http://ec.europa.eu/eurostat/statistics-explained/index.php/Personal_remittances_statistics

Посібник щодо складання статистичних даних про незаконну економічну діяльність на національних рахунках та у платіжному балансі – редакція 2018 року.
https://ec.europa.eu/eurostat/documents/3859598/8714610/KS-05-17-202-EN- N.pdf/eaf638df-17dc-47a1-9ab7-fe68476100ec

4/ Звіти Європолу

Звіт Європолу: Чому готівка досі править?, 2015.
https://www.europol.europa.eu/publications-documents/why-cash-still-king-strategic- report-use-of-cash-criminal-groups-facilitator-for-money-laundering

Європол 2016, Оцінка загрози організованої злочинності у мережі Інтернет (IOCTA) 2016.
https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime- threat-assessment-iocta-2016

Оцінка загрози серйозної та організованої злочинності в Європейському Союзі (ЄС) (SOCTA), 2017.
https://www.europol.europa.eu/activities-services/main-reports/european-union-serious- and-organised-crime-threat-assessment-2017

Група фінансової розвідки Європолу, Звіт «*Від підозри до дії*», 2017.
https://www.europol.europa.eu/publications-documents/suspicion-to-action-converting- financial-intelligence-greater-operational-impact

5/ Інші органи на рівні Союзу

Звіти щодо платіжної статистики ЄЦБ.

Робочий документ ЄЦБ за 2014 рік про використання готівки споживачами.
https://www.ecb.europa.eu/pub/pdf/scpwps/ecbwp1685.pdf

Січень 2017 – Спільна думка ESA щодо ризиків відмивання коштів та фінансування тероризму, які впливають на фінансовий сектор Союзу.
http://www.eba.europa.eu/documents/10180/1759750/ESAS+Joint+Opinion+on+the+risks+of+money+laundering+and+terrorist+financing+affecting+the+Union%E2%80%99s+financial+sector+%28JC-2017-07%29.pdf

2017 – Спільні настанови європейських органів нагляду, Настанови щодо нагляду на основі ризиків.
https://esas-joint- committee.europa.eu/Publications/Guidelines/Joint%20Guidelines%20on%20risk-based%20supervision_EN%20%28ESAs%202016%2072%29.pdf

2019 – Звіт EBA з порадами для Європейської Комісії щодо криптовалют
https://eba.europa.eu/documents/10180/2545547/EBA+Report+on+crypto+assets.pdf

2019 – Рекомендації ESMA інституціям Європейського Союзу щодо початкової пропозиції монет та криптовалют
https://www.esma.europa.eu/press-news/esma-news/crypto-assets-need-common-eu- wide-approach-ensure-investor-protection

6/ Звіти FATF та Moneyval:

2009 – Ризики відмивання коштів та фінансування тероризму у секторі цінних паперів, FATF.
http://www.fatf- gafi.org/media/fatf/documents/reports/ML%20and%20TF%20in%20the%20Securities%20Sector.pdf

2013 – Роль системи «хавала» та інших подібних провайдерів послуг у відмиванні коштів та фінансуванні тероризму, FATF.
http://www.fatf-gafi.org/media/fatf/documents/reports/Role-of-hawala-and-similar-in- ml-tf.pdf

2013 (спільний звіт з Егмонтською групою) – Відмивання коштів та фінансування тероризму шляхом торгівлі алмазами, FATF.
http://www.fatf-gafi.org/media/fatf/documents/reports/ML-TF-through-trade-in- diamonds.pdf

2013 – Відмивання коштів та фінансування тероризму – Вразливості спеціалістів з юридичних питань, FATF.
http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20and%20TF%20vulnerabilities%20legal%20professionals.pdf

2013 – Використання азартних ігор онлайн для відмивання коштів та фінансування тероризму (Moneyval).
https://www.coe.int/t/dghl/monitoring/moneyval/Activities/MONEYVAL(2013)9_Onlin egambling.pdf

2015 – Типологічні звіти про відмивання доходів від організованої злочинності, Moneyval.
http://www.coe.int/t/dghl/monitoring/moneyval/Activities/MONEYVAL(2015)20_typologies_launderingtheproceedsoforganisedcrime.pdf

2015 – Фінансування терористичної організації Ісламська держава в Іраку та Леванті (ISIL), FATF.
http://www.fatf-gafi.org/media/fatf/documents/reports/Financing-of-the-terrorist- organisation-ISIL.pdf

2018 – Фінансування вербування для терористичних цілей
http://www.fatf-gafi.org/publications/methodsandtrends/documents/financing- recruitment-terrorist-purposes.html

2018 – Зобов'язання Великої двадцятки щодо впровадження стандартів FATF та підтримки роботи з криптовалютами.
http://www.fatf-gafi.org/media/fatf/documents/reports/FATF-Report-G20-FM-CBG- July-2018.pdf

2018 – Щорічний звіт Moneyval за 2017 рік
https://rm.coe.int/moneyval-annual-report-2017-eng/16808af3c2

2019 – Підхід на основі ризиків для осіб, які надають послуги з управління довірчими фондами та компаніями
http://www.fatf-gafi.org/publications/fatfrecommendations/documents/rba-trust- company-service-providers.html

2019 – Настанови щодо підходу на основі ризиків для спеціалістів з питань бухгалтерського обліку
http://www.fatf-gafi.org/publications/fatfrecommendations/documents/rba-accounting- profession.html

2019 – Підхід на основі ризиків для спеціалістів з юридичних питань
http://www.fatf-gafi.org/publications/fatfrecommendations/documents/rba-legal- professionals.html

2019 – Настанови щодо підходу на основі ризиків для віртуальних активів та провайдерів послуг з обслуговування віртуальних активів.
http://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba- virtual-assets.html

7/ Інші зовнішні інформаційні джерела

Оцінка ризику відмивання коштів в Європі — Заключний звіт проекту IARM — 31 травня 2017 р.
http://www.transcrime.it/iarm/wp-content/uploads/sites/5/2017/05/ProjectIARM-FinalReport.pdf

Transparency International/Global Witness, Європейська втеча 2018 – У примарному світі золотих віз.
www.transparency.org/whatwedo/publication/golden_visas

8/ Конфіденційна інформація

Інформація була отримана від Європолу (конфіденційна).

9/ Усні та письмові внески наступних зацікавлених сторін

У липні 2018 року Комісія провела консультації з державами-членами у формі анкети з додатками стосовно:

- національних пом'якшувальних заходів;
- шаблонів для фінансових і процесуальних даних про ВК/ФТ; та
- нових ризиків.

До кінця 2018 року Комісія отримала 23 відповіді. Згодом з країнами-членами були проведені консультації на спеціальних засіданнях Експертної групи з питань відмивання коштів та фінансування тероризму, які відбулися 10 грудня 2018 року та 11 лютого 2019 року.

У листопаді-грудні 2018 року Комісія провела чотири семінари із зацікавленими особами приватного сектора: один з представниками фінансових установ, два з «встановленими нефінансовими підприємствами і професіями» (DNFBPs) і один з громадянським суспільством (некомерційні організації) та науковцями. Другий етап цього раунду засідань відбувся у січні 2019 року. Усний внесок приватного сектора був доповнений 15 письмовими відповідями.

Національні асоціації були представлені через свою відповідну європейську федерацію:

- Accountancy Europe
- Приватний фонд Antwerp World Diamond Centre
- Асоціація фінансових ринків Європи
- BEUC — Європейська асоціація споживачів
- Громадська організація Europe
- Confédération Fiscale Européenne
- COFACE Family Europe
- Рада нотаріусів Європейського Союзу
- Cultural Action Europe
- Асоціація електронних грошей
- Європейська асоціація кооперативних банків
- Європейська асоціація державних банків
- Європейська асоціація агентів нерухомості
- Європейський комітет банківського сектора
- Європейська банківська федерація
- Європейські адвокати (Рада адвокатських об'єднань та юридичних товариств Європи, CCBE)
- Європейська асоціація казино
- Європейська федерація будівельних компаній
- Європейська федерація ювелірів (EFJ)

- Центр європейських фондів
- Європейська фандрайзингова асоціація (EFA)
- Європейська асоціація азартних ігор та розваг
- Європейська асоціація азартних ігор та букмекерства
- Європейські лотереї
- Європейська асоціація грошей
- Європейський тоталізатор
- Європейська федерація платіжних установ
- Колектив з питань безпеки людини
- Insurance Europe
- Міжнародний комітет Червоного Хреста
- Спільний дослідницький центр транснаціональної злочинності (TRANSCRIME)
- Асоціація юристів Англії та Уельсу
- Leaseurope
- Mastercard
- Moneygram Europe
- Громадська організація Voice
- Фонд «Відкрите товариство»
- PayPal
- Асоціація віртуальних азартних ігор
- STEP
- SWIFT
- Università Catolica del Sacro Cuore
- Taxadvisers Europe
- Transparency International EU
- Асоціація фінансових ринків Європи (AFME)
- Рада адвокатів та адвокатських об’єднань Європи
- Trust Europe Affairs (віртуальні валюти)
- Voice
- Visa
- Western Union Europe