

відповідальних за проведення внутрішнього фінансового моніторингу.

Оприлюднене НБУ Положення про здійснення небанківськими фінансовими установами фінансового моніторингу 28 липня 2020 року [248] імплементує у здійснення фінансового моніторингу зміни законодавства [302].

Основні концептуальні підходи Положення – це використання РОП, саме побудова кожним СПФМ належної системи управління ризиками; поділ на посилені та спрощені заходи належної перевірки клієнтів; введення методів віддаленої ідентифікації та верифікації; адаптований перелік критеріїв ризику та індикаторів ризиковості; РОП до політично значущих осіб, членів їх сімей та пов'язаних осіб (PEPs).

Розглянута бальна методика визначення рівня ризику ВК/ФТРЗ має низку переваг: доступна у користуванні, дає достатньо достовірну оцінку, поєднує врахування кількісних та якісних показників, може оперативно вдосконалюватися. Ця бальна методика визначення рівня ризику ВК/ФТРЗ може бути використана як банком, так і іншою фінансовою установою з метою визначення ефективності системи управління ризиками ВК/ФТРЗ чи для потреб встановлення комплексного ризику конкретної фінансової операції. Також вона може бути основою розробки Карти ризиків та створення ризик-профілів клієнтів СПФМ.

2.6. Дотримання умов належної обачності щодо клієнтів з високим рівнем ризику відмивання коштів та фінансування тероризму на ринку фінансових послуг

Система фінансового моніторингу України – це структура, яка має гнучко реагувати на виклики та загрози в режимі реального часу. В умовах становлення економіки України та її інтеграції з міжнародними фінансовими системами, боротьба з ВК/ФТРЗ набуває особливої актуальності, оскільки стратегічним напрямом у боротьбі з орга-

нізованою злочинністю є підрив її економічного підґрунтя, створення та реалізація комплексної системи правових, організаційних та інших заходів щодо виявлення та ліквідації каналів відмивання кримінальних коштів [155].

ДСФМ України 21.07.2014 ухвалила Рекомендації для СПФМ щодо ризиків, пов'язаних із фінансуванням сепаратистських та терористичних заходів на території України, якими передбачається, що СПФМ повинен виявляти фінансові операції, стосовно яких є достатні підстави підозрювати, що вони пов'язані, стосуються або призначені для фінансування тероризму, інформувати про це Держфінмоніторинг України та правоохоронні органи, та посилити систему управління ризиками, а саме здійснювати організаційно-правові заходи щодо клієнтів, діяльність яких свідчить про підвищений ризик проведення ними операцій [334].

Зважаючи на євроінтеграційну стратегію Україну, важливим нормативно-правовим актом в сфері фінансового моніторингу була Третя Директива ЄС (2005 р.), яка вперше визначила заходи боротьби з фінансуванням тероризму. Найважливішим пунктом стали нові підходи до перевірки клієнтів (з англ. «customer due diligence») – «належна обачність». Цей термін порівняно новий для української системи фінансового мінторингу. Це так заний правовий аудит клієнта на предмет відповідності його діяльності вимогам законодавства і правилам фінансової установи, визначення його надійності та привабливості. Для банківського сектору due diligence є складовою процедури «compliance» [18] та передбачає комплекс заходів щодо вивчення потенційних клієнтів, їхньої діяльності, джерел походження капіталу та визначення ступеня ризику для банку у разі встановлення відносин з таким клієнтом.

У тепершній час в Україні в оновленому законодавстві враховано положення Четвертої Директиви ЄС [22], між тим у ЄС вже обговорюються зміни до нових Директив з фінансового моніторингу.

Принцип «належної обачності» передбачає заборону фінансовим установам відкривати анонімні рахунки, встановлення повної структури власності юридичних осіб до бенефіціарних власників

(включаючи компанії-трасти), визначення цілей та характеру ділових відносин, постійний моніторинг операцій клієнта, формування фінансовими установами власної системи оцінки ризиків, РОП до перевірки клієнта [123].

Саме останній передбачає дотримання умов належної обачності щодо клієнтів на підставі визначення вузьких місць, які можуть характеризувати високий рівень ризику ВК/ФТ [253].

Про заходи обачливості згадується і в Міжнародних стандартах FATF, а саме прописані правила обачливості щодо клієнтів (рис. 2.4), що розроблені на основі джерела [233].

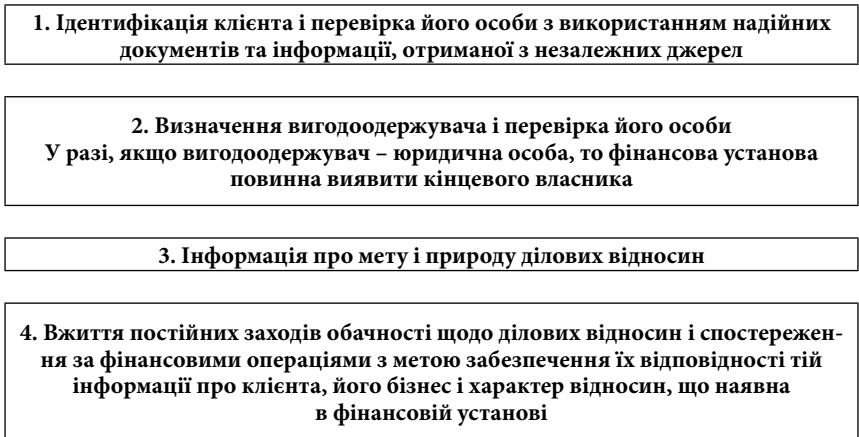


Рис. 2.4. Правила обачності щодо клієнтів для додержання фінансовими установами

Фінансові установи повинні застосовувати правила обачності, представлені на рис. 2.4, але можуть визначати міру застосування залежно від ступеня ризику, пов'язаного з типом клієнта, діловими відносинами та здійснюваними операціями. Заходи, що застосовуються, повинні відповідати рекомендаціям державних органів регулювання. До операцій з високим ризиком фінансові установи повинні використовувати більш жорсткі правила обачності.

Банки мають більш високі вимоги щодо формування системи фінансового моніторингу. Чи буде сприяти реалізації принципи високої обачності нове Положення НБУ щодо організації системи фінансового моніторингу небанківських фінансових установ покажуть результати його впровадження [248], тому оцінка і аналіз буде відбуватися у майбутньому. Окремі вимоги до фінансових установ є спрощеними порівняно з банками, наприклад: більшості установ рекомендовано мати систему автоматизації процесів із фінмоніторингу, проте обов'язковою вона є лише для платіжних систем, які здійснюють перекази коштів у режимі онлайн; оцінка ризику клієнтів відбувається за спрощеними методами, в тому числі установам надано можливість оцінювати ризик не кожного клієнта окремо, а на груповій основі, що знижує ефективність заходів з обачності щодо ризиків ВК/ФТРЗ; встановлено особливі заходи з належної перевірки клієнтів та вигодоодержувачів для страхових компаній; небанківські установи не погоджують із НБУ кандидатуру відповідального працівника за фінансовий моніторинг (до того ж відповідальному працівнику дозволяється суміщення та сумісництво за посадою).

У табл. 2.8 наведено дані про дотримання обраними для аналізу банками виконання заходів належної обачності щодо клієнтів з високим рівнем ризику ВК/ФТ на ринку фінансових послуг [250; 251; 256].

Таблиця 2.8. Дотримання обраними банками виконання заходів належної обачності щодо клієнтів з високим рівнем ризику ВК/ФТ на ринку фінансових послуг

Захід щодо протидії ВК/ФТРЗ	ПАТ КБ «ПРИВАТБАНК»	АТ «Альфа Банк»	АТ «ProCredit Bank»
Призначення відповідального співробітника з фінансового моніторингу	+ Підзвітний тільки керівнику банку	Відсутня інформація	+ Звітує перед Головою Правління банку, а також перед відповідальним співробітником ПроКредит Холдингу

Захід щодо протидії ВК/ФТРЗ	ПАТ КБ «ПРИВАТБАНК»	АТ «Альфа Банк»	АТ «ProCredit Bank»
Дотримання принципу «KYC»	+	+	+ Також має місце політика «Знай свого кореспондента»
Навчання та підвищення кваліфікації	+	+	+
Класифікація клієнтів за рівнем ризику	+ Групи клієнтів за рівнем ризику: низький, середній, високий та неприйнятно високий	+ Групи ризику: Ризик за типом клієнта; Ризик послуг, які отримує клієнт; Географічний ризик	+
Повідомлення про підозрілі операції	+	+	+
Щорічний внутрішній аудит перевірок вимог законодавства у сфері AML/CFT	+	Відсутня інформація	+
Заборона ведення анонімних рахунків банків-оболонок	+	+	+

Отже, зважаючи на табл. 2.8 та вищевикладену інформацію варто відмітити, що досліджені банки дотримуються виконання заходів належної обачності щодо клієнтів з високим рівнем ризику ВК/ФТРЗ на ринку фінансових послуг. Використовуючи у своїй діяльності РОП, фінансові установи значну увагу приділяють політиці «Знай свого клієнта», відповідно до якої вони зобов'язані встановити особу свого клієнта до проведення операцій з ним. Разом з повагою права клієнтів на конфіденційність, фінансові установи змушені дотримуватися даного принципу, щоб уникнути фінансових, репутаційних і правових ризиків.

В Україні елементом системи фінансового моніторингу є належна ідентифікація клієнтів.

За новим Законом [302], виходячи з пояснень працівників Міністерства юстиції [101], обмежуються операції без відкриття рахунку, коли фізична особа могла за певних умов не ідентифікуватися, але практично ніяких змін для операцій між власниками рахунків, коли особи ідентифіковані. Введено кількісне обмеження неідентифікованих операцій типу поповнення рахунку через термінал до 5 тис. грн., на більшу суму – тільки на власну картку за умови додаткової ідентифікації особи, переказ готівкою через термінал можливий без обмежень, якщо особа буде ідентифікована. Між тим не потрібна додаткова ідентифікація для переказів з картки на картку, чи онлайн-платежів карткою.

Настав кінець анонімності й для електронних гаманців (власники мають пройти ідентифікацію до кінця 2020 року, про криптовалюту поки неочевидно). Йдеться про запровадження РОП для здійснення моніторингу фінансових операцій, з'являються нові суб'єкти фінмоніторингу: поштові оператори, адвокати, ріелтори, бухгалтери, емітенти електронних грошей (будуть перевіряти й певною мірою відповідати за легальне походження коштів, наприклад, сторін угоди) [101].

Положенням НБУ «Про здійснення небанківськими фінансовими установами фінансового моніторингу», затвердженого постановою Правління Національного банку від 28 липня 2020 року № 107 [248] представлено Порядок дистанційної ідентифікації та верифікації клієнта, яка можлива в декількох варіаціях. Крім фізичної присутності та копії оригіналів документів для небанківських установ, як і для банків, також доступна дистанційна ідентифікація та верифікація клієнта.

Справжніми моделями верифікації є: використання BankID НБУ, кваліфікованого електронного підпису (КЕП), сеансу відеотрансляції, а також верифікація з використанням ресурсу державних онлайн-послуг «ДІЯ». Спрощеними моделями верифікації є: BankID НБУ, КЕП, зчитування даних із чипа біометричного документа, верифікація даних із бюро кредитних історій.

Побіжно Положення визначає порядок ідентифікації клієнта із залученням агента та використання інформації щодо належної перевірки клієнта, отриманої від третьої сторони.

Відтепер для укладення договору страхування або оформлення позики у фінансовій компанії чи кредитній спілці візит до відділення або особиста зустріч із представником установи непотрібна.

Відсутність належних та дієвих механізмів перевірки клієнтів може завдати суттєвої матеріальної та нематеріальної шкоди установі, особливо, коли мова йде про використання її послуг, активів чи ресурсів для неправомірних цілей, зокрема, для викрадення персональних даних, ВК/ФТРЗ.

Нині банки в усьому світі запроваджують суворі вимоги до розкриття клієнтами даних про кінцевого бенефіціара та зміст своїх операцій. Це те, що називається «знай свого клієнта» (KYC) – комплекс процедур для ідентифікації та перевірки клієнтів установи, що спрямовані на забезпечення своєчасного виявлення та ефективного запобігання можливим ризикам. Такий принцип є основою РОП банку з фінансового моніторингу [128].

Вимоги і стандарти, спрямовані на його реалізацію, встановлюються національним законодавством [302], нормативними документами регуляторів, зокрема, НБУ, міжнародних організацій, таких як FATF (принцип «Знай свого клієнта» отримав розвиток у стандартах Базельського комітету банківського нагляду «Належне ставлення банків до клієнтів»). Така вимога щодо ведення банками анкет клієнтів запроваджена ще 2003 року. Такі анкети мають містити інформацію про фінансовий стан клієнта, оцінка якого проводиться згідно з внутрішніми процедурами банку. Банки зобов'язані щоквартально здійснювати аналіз відповідності операцій клієнта його фінансовому стану та суті діяльності [255].

Основне завдання цієї політики – отримання інформації про клієнтів та джерела їх коштів, щоб упевнитися у тому, що останні не мають злочинного походження й не використовуються зі злочинною метою.

Кожна фінансова установа, відповідно до Стандартів Базельського комітету банківського нагляду «Належне ставлення банків до клієнтів» (2001 р.), розробляє власну програму ідентифікації клієнтів з метою отримання від них відповідних документів і відомостей, а

саме місця постійного перебування, професійної діяльності, джерел походження коштів, мети відкриття рахунку тощо [142].

Така процедура обов'язкова і здійснюється не лише при відкритті рахунку, а й під час проведення транзакцій (поповнення рахунку, обміну валюти, переказу коштів тощо).

Відбулись зміни з квітня 2019 для юридичних осіб-нерезидентів, в рамках програми «Знай свого клієнта» також необхідно довести, що вони не є фіктивними компаніями, («компаніями – оболонками»).

Це також стосується компаній, які є контрагентами клієнтів банку. Варто відмітити, що поступове впровадження практики КУС призвело до поступової заборони обслуговування анонімних банківських рахунків.

У табл. 2.9 подано переваги цього принципу як для клієнта, так і для фінансової установи.

Таблиця 2.9. Переваги принципу «Знай свого клієнта»

Переваги КУС для клієнта
Фінансовий консультант знайде для клієнта краще рішення для управління активами
Менеджер банку зможе запропонувати клієнту оптимальний пакет фінансових послуг відповідно до завдань
Брокер фондової біржі зможе дати інвестиційні рекомендації, враховуючи реальний фінансовий стан клієнта
Переваги КУС для фінансової установи
Ідентифікація контрагента і розуміння суті його діяльності
Визначення ступеню ризику залучення клієнта в незаконну діяльність
Визначення типу і кількості транзакцій для клієнта
Відстеження незвичайних клієнтських транзакцій
Забезпечення виконання вимог державних органів у сфері протидії ВК/ФТ; перешкодження ухиленню від сплати податків
Захист репутації фінансових установ шляхом зменшення вірогідності їх перетворення у засіб фінансового злочину
Зменшення ймовірності шахрайства

Спираючись на інформацію з табл. 2.9, видно, що сутність КУС стосується [239]: політики прийняття нових клієнтів; проведення

ідентифікації клієнтів; постійного моніторингу високоризикових рахунків; загальної системи управління ризиками.

Щодо недоліків такої практики, то для банків – це додатковий час та ресурси, які можна було б витратити, наприклад, на залучення нових клієнтів. Для клієнта це створює певні незручності, забирає час і буквально змушує шукати альтернативні способи та канали для вирішення своїх фінансових завдань.

За умови ненадання запитуваних документів клієнтом, або надання тих, що не пройшли перевірку первинного фінансового моніторингу, можна очікувати зупинку видаткових операцій, відмову у вчиненні транзакцій або здійсненні угоди, відмову від встановлення ділових відносин та їх розірвання, а також зупинення фінансової операції з подальшим повідомленням СДФМ.

У світі KYC – звичайна практика для фінансових організацій, бухгалтерських, юридичних, букмекерських контор, за якою учасники фінансових ринків протидіють шахрайству, розкраданню, відмиванню грошей і фінансуванню незаконних операцій [91].

Не менш важливим аспектом ефективної роботи внутрішньобанківської системи запобігання ВК/ФТРЗ є наявність поточних програм навчання для своїх працівників, щоб персонал фінансових установ був відповідно навчений процедурам KYC [175].

Інновацією в банківському секторі стало те, що НБУ дозволив фізичним особам дистанційно відкривати банківські рахунки та отримувати інші банківські послуги, що передбачають ідентифікацію особи. Для надання такої можливості в Україні впроваджено механізм віддаленої ідентифікації клієнтів банків через створену НБУ систему BankID [255].

Така система дозволить будь-якому клієнту, який вже пройшов процедуру KYC в одному банку та отримав національний Bank ID, використати його для відкриття рахунків у будь-якому іншому банку. При цьому відповідальність за належну ідентифікацію та вивчення клієнта в рамках міжнародних стандартів і законодавства України покладається на банк, що здійснював ці операції, а також на банк, який використовує інформацію з системи BankID [255].

Проте, запобіжні заходи КУС виходять за межі простого відкриття рахунків і ведення обліку та вимагають від банків розробки політики визначення благонадійності клієнта і програми багаторівневої ідентифікації клієнта, яка включає всебічну ретельну перевірку клієнтів та операцій підвищеного ризику, а також профілактичний моніторинг підозрілої діяльності [123].

Між тим правники з Міністерства юстиції України вважають ключовими ризиками те, чи будуть виконуватися нові вимоги до фінансового моніторингу [302] СПФМ, зокрема, банками [101].

На рис. 2.5 представлені статистичні дані щодо повідомлень про фінансові операції, отримані Держфінмоніторингом протягом 2014–2019 рр. [253].

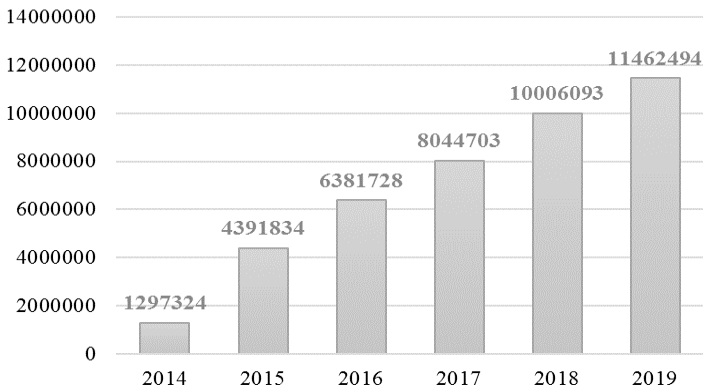


Рис. 2.5. Динаміка інформування про фінансові операції, що підлягають фінансовому моніторингу за період 2014–2019 рр.

Усього з початку експлуатації інформаційно-аналітичної системи Держфінмоніторингу отримано та оброблено 48,84 млн. повідомлень про фінансові операції, що підлягають фінансовому моніторингу, з яких понад 10 млн. та 11 млн. повідомлень отримано протягом 2018 та 2019 рр. Відповідно. За період 2018–2019 рр. цей показник зріс в 1,15 р.

Основну частину таких повідомлень надсилають здебільшого банківські установи, що наочно представлено на рис. 2.6, який розроблений на основі джерела [253].

З рис. 2.6 видно, що за весь досліджуваний період, у порівнянні з небанківськими установами, банки були більш активними в звітуванні. Так, у 2014 р. банки надіслали 97,16 % загальної кількості повідомлень про фінансові операції, у 2015 р. – 98,2 %, у 2016 р. – 98,1 %, у 2017 р. – 98,1 %, у 2018 р. та 2019 рр. – 98,7 % та 99,04 % відповідно [253].

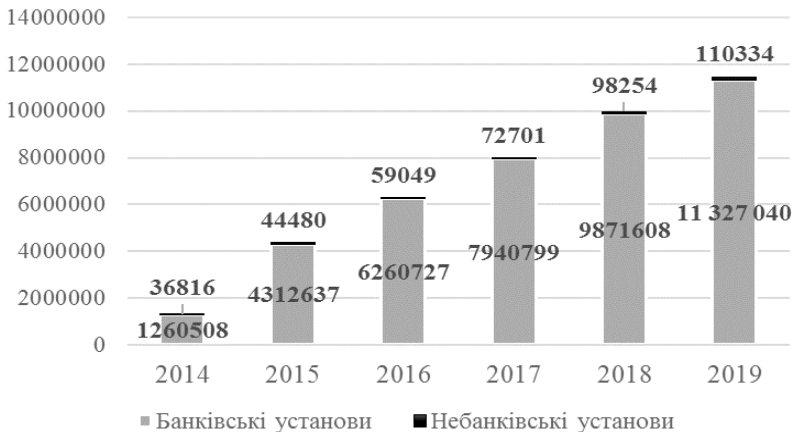


Рис. 2.6. Динаміка кількості повідомлень про фінансові операції, взятих Держфінмоніторингом на облік у 2014–2019 роках (в розрізі банківських та небанківських установ)

Серед небанківських установ найбільш активними у поданні повідомлень є професійні учасники фондового ринку. Питома вага таких повідомлень у загальному обсязі взятих на облік повідомлень про фінансові операції, що надійшли до Держфінмоніторингу від небанківського сектору, трохи менше 50 %.

Статистику кількості повідомлень від небанківського сектору надано у табл. 2.10 [253].

Таблиця 2.10. Загальна кількість повідомлень про фінансові операції небанківського сектору Держфінмоніторингу протягом 2018–2019 рр.

Тип установи	2018		2019	
	Кількість повідомлень, од.	Питома вага, %	Кількість повідомлень, од.	Питома вага, %
Страхові установи	40 021	40,76	44 577	40,40
Інші суб'єкти господарювання, що надають фінансові послуги	6 810	6,94	12 783	11,59
Професійні учасники фондового ринку	45 805	46,65	51 318	46,51
Суб'єкти господарювання, які проводять лотереї	600	0,61	648	0,59
Нотаріуси	21	0,02	11	0,01
Інші СПФМ	4 927	5,02	997	0,90

Згідно з табл. 2.10, найбільше повідомлень серед небанківських установ надсилають професійні учасники фондового ринку та страхові установи (в сумі майже 90 %). Важливо відзначити, що серед СПФМ, які подавали інформацію, вже є і нотаріуси, також розширений ринок інших учасників, і він може збільшуватися щодо наданих повідомлень.