масивів інформації за системою комплаєнс-контролю, що забезпечить стабільну роботу фінансової установи.

Професійними тренінгами встановлено, що ризики, пов'язані з ВК/ФТРЗ, є зростаючими у фінансовій сфері, мають свої особливості і потребують компетентного фахового забезпечення, серед якого є аудиторські послуги.

3.3. Законодавство та судова практика щодо застосування фінансового моніторингу при здійсненні платіжних послуг

Законодавче забезпечення фінансового моніторингу будується на врегулюванні різноманітних ризиків та одночасній випадковості появи тих чи інших прецедентів. Правова оцінка потребує вироблення усталених положень, які в майбутньому доцільно буде закріпити як норми законодавства про фінансовий моніторинг. Для дослідження цієї тематики проаналізовано судову практику, погляди науковців та нормативно-правові акти, що регулюють відповідні відносини.

Для дослідження судової практики ми використовуємо шаблон, відповідно до якого відмічали суб'єктів розрахункових правовідносин, права яких порушено; в чому полягало порушення; які правовідносини можуть бути об'єктом фінансового моніторингу; зміст ризику при проведенні відповідної розрахункової операції.

Розглянемо деякі судові рішення, які містять необхідну практику на досліджувану тематику.

Між недержавним банком та Товариством з обмеженою відповідальністю (далі – ТОВ) укладено договір еквайрингу. 10.10.2014 р. до недержавного банку від іноземних банків – емітентів почали надходити вхідні претензії. Для їх відхилення він повинен був надати документи на підтвердження легітимності списання грошових коштів і участі держателя платіжної картки у здійсненній операції по його платіжній картці. Такими документами мали бути, зокрема, чеки платіжного терміналу, які у відповідності до умов Договору (п. 5.8)

зберігалися у ТОВ та мали передаватися недержавному банку на його вимогу. Організацією надані чеки, але без підпису клієнтів. Згодом нею надані витребувані документи, які при наданні відповідей на претензії надіслані іноземним банкам – емітентам. У ході судового розгляду виявилося, що підписи на чеках були підробленими. Даний факт свідчив про те, що оскаржувані операції проведені за відсутності користувачів платіжних карток, що є порушенням як постанов Національного банку України (далі – НБУ), так і договору. Внаслідок неправомірних дій ТОВ недержавному банку завдано 7297308,11 грн збитків. Суд за результатом розгляду справи задовольнив касаційну скаргу банку [288].

У цій, як приклад, справі наявний операційний ризик. Окрім того, факти по справі свідчать про потребу розробки питання усунення правових ризиків у розрахункових операціях банків. Крім того, на час розгляду цієї справи діяв Закон України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» від 14.10.2014 р. №1702-VII (далі – Закон України від 14.10.2014 р. №1702-VII) [303], де виокремлювалися фінансові операції, які підлягали обов'язковому фінансовому моніторингу та сумнівні фінансові операції (ст. 15 Закону). На даний час є чинним Закон України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» від 06.12.2019 р. № 361-IX (далі – Закон України від 06.12.2019 р. № 361-IX), відповідно до якого виокремлюються порогові та підозрілі фінансові операції (ст. 20, 21) [302]. Якщо проаналізувати дану справу відповідно до чинного Закону, то фінансова операція класифікувалася як підозріла і могла бути об'єктом фінансового моніторингу (ч.1 ст. 21 Закону). Таким чином, прогалина закону щодо характеру ризику надала змогу не розповсюджувати на операції законодавство про фінансовий моніторинг.

16.06.2010 р., 30.05.2013 р. між двома недержавними банками був укладений договір про встановлення кореспондентських відносин.

У період з 08.06.2015 р. по 26.08.2015 р. банком 2 з кореспондентських рахунків банку 1, відкритих на підставі вказаних договорів, списано грошові кошти в сумі 2 176 501,86 грн. 05.06.2015 року Правлінням НБУ прийнято постанову №358/БТ «Про віднесення банку 1 до категорії неплатоспроможних». Виконавчою дирекцією Фонду гарантування вкладів фізичних осіб 05.06.2015 року прийнято рішення № 114 «Про запровадження тимчасової адміністрації у банку 1» з 08.06.2015 р. по 07.09.2015 р. включно. На час списання банком 2 грошових коштів з кореспондентських рахунків банку 1, останній був кредитором банку 2, а тому на нього поширювались обмеження, встановлені п. 1 ч. 5 ст. 36 Закону України «Про систему гарантування вкладів фізичних осіб» і, самостійне списання ним з рахунків банку 2 вартості послуг, наданих за вказаними договорами, було неправомірним [285].

На думку авторів, у цьому прикладі мета операції не співпадає з метою Закону України від 06.12.2019 р. № 361-IX, тому у такому випадку не проводиться фінансовий моніторинг. Відповідно до положень названого закону наведена операція не підпадає під критерії порогової чи підозрілої. У даній справі наявний правовий ризик, який має самостійну класифікацію та пов'язаний з несумлінним виконанням обов'язків уповноваженою особою банку. Не завжди несумлінні дії працівників банків підпадають під фінансовий моніторинг, хоча мають характер правового ризику.

Між недержавним банком та ФОП укладено договір еквайрингу. При перевірці банком наявності шахрайських транзакцій в його еквайринговій мережі в електронному звіті виявлено таку операцію, яка здійснена у платіжному терміналі торгового підприємства, що належить ФОП, внаслідок чого банку завдано збитків у розмірі 3 577,16 дол. США (за офіційним курсом НБУ на день операції – 101 054,76 грн). Суд, за результатами розгляду цієї справи задовольнив вимоги банку, оскільки за умовами договору, укладеного між сторонами не передбачено обов'язку еквайра відшкодовувати торговцю понесені збитки внаслідок визнання шахрайськими, проведених ним операцій [282].

На думку авторів, для попередження подібної ситуації необхідно в умовах договору визначити суб'єкта, який має нести відповідальність у разі здійснення шахрайських дій при проведенні операцій, які несуть додаткові ризики. Банку необхідно затвердити для власного користування додаткову типізацію підозрілих здійснюваних операцій.

На час розгляду цієї справи діяв Закон України від 14.10.2014 р №1702-VII, де виокремлювалися сумнівні фінансові операції, від таких, які підлягали обов'язковому фінансовому моніторингу (ст. 15 Закону). На даний час є чинним Закон України від 06.12.2019 р. № 361-IX, відповідно до якого виокремлюються порогові та підозрілі фінансові операції (ст. 20, 21). Якщо проаналізувати дану справу відповідно до чинного Закону, то фінансова операція класифікувалася як підозріла і могла бути об'єктом фінансового моніторингу (ч.1 ст. 21 Закону), але у даній справі банк не здійснив такої кваліфікації цієї операції. Таким чином, зміст рішення у справі підкреслює, що відсутність в банку своєчасного фінансового моніторингу з причин недостатнього визначення сумнівних операцій в банківських документах може призвести до значних збитків.

Предметом наступного спору була вимога ПрАТ про розірвання договору банківського рахунку від 29.02.2012 р., укладеного між ним та недержавним банком, про стягнення з банку грошових коштів, що знаходяться на рахунку ПрАТ 2 438 000,00 грн. пені та 200 383,56 грн. 3 % річних. 29.02.2012 р. між ПрАТ та недержавним банком був укладений договір про банківське обслуговування з використанням програмно-технічного комплексу «Банк-Клієнт». 08.07.2015 та 09.07.2015 р. ПрАТ передало через засоби програмно-технічного комплексу «Банк-Клієнт» недержавному банку на виконання електронні платіжні доручення на загальну суму 53 000 000,00 грн.

08.07.2015 р. та 09.07.2015 р. листами № 05-20/1268 та № 05-20/1291, посилаючись на п. 5.1 договору про банківське обслуговування з використанням програмно-технічного комплексу «Банк-Клієнт» від 29.02.2012 № W085, банк звернувся до ПрАТ з проханням надати йому оригінали вказаних платіжних доручень (на паперовому носії). У відповідь на це прохання йому направлені по одному примірнику

оригіналів вказаних платіжних доручень кур'єрською службою, які залишені банком без виконання, що було незаконним та суперечило умовам договору [284]. На думку автора, мета такої операції не співпадає з метою Закону України від 06.12.2019 р. № 361-IX, тому фінансовий моніторинг є неможливим. Відповідно до його положень наведена операція не підпадає під критерії порогової чи підозрілої. У даній справі наявний правовий ризик або операційний ризик пов'язаний з умисним або неумисним невиконанням обов'язків уповноваженою особою банку. Таким чином, порушення банком правил платіжних систем та договірних умов проведення операцій не ведуть до такого наслідку, як віднесення операції до такої, що підлягає фінансовому моніторингу.

17 вересня 2012 р. року з платіжної картки фізичної особи, виданої недержавним банком у м. Бангкок Королівства Таїланд знято грошові кошти у розмірі 2 417,88 доларів США (за офіційним курсом НБУ – 19 326,11 грн.), про що йому стало відомо з смс-повідомлень. У ході судового розгляду встановлено, що у цей час фізична особа перебувала на території України, сама кошти зі своєї картки не знімала та не уповноважувала будь-яких осіб вчиняти такі дії. Судом встановлено, що 17 вересня 2012 року в період часу з 21 год. 33 хв. по 21 год. 35 хв. проведено дев'ять операцій, п'ять з яких були успішними. Усі зазначені операції проведені через банкомат в м. Бангкок (Таїланд) та супроводжувались коректним вводом ПІН-коду. У ході судового розгляду суд задовільнив вимоги фізичної особи, адже банк не зміг довести обставини, які безперечно доводять, що фізична особа своїми діями чи бездіяльністю сприяла втраті, незаконному використанню ПІН коду або іншої інформації, яка дає змогу ініціювати платіжні операції [283].

На час розгляду цієї справи діяв Закон України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансуванню тероризму» від 28.11.2012 р. № 249-IV [301], де виокремлювалися фінансові операції, які підлягали обов'язковому фінансовому моніторингу та ті, що підлягають внутрішньому моніторингу (ст. 15, 16 Закону). На даний час є чинним

Закон України від 06.12.2019 р. № 361-IX, відповідно до якого виокремлюються порогові та підозрілі фінансові операції (ст. 20, 21). Якщо проаналізувати дану справу відповідно до чинного Закону, то фінансова операція класифікувалася як підозріла і могла бути об'єктом фінансового моніторингу (ч.1 ст. 21 Закону). Тобто, ця справа підкреслює необхідність додаткового локального регулювання. Як висновок необхідно відмітити, що банком не було належним чином враховано законодавство про фінансовий моніторинг при наявності для цього усіх підстав.

20 лютого 2014 року недержавний банк відкрив фізичній особі 2 карткових рахунка. 16 вересня 2014 року о 3 год. 35 хв. особі надійшло два sms-повідомлення про те, що з обох рахунків списано 10 000 грн 00 коп. та 4 000 грн 00 коп., додатково також нараховано комісію у розмірі 160 грн 00 коп. У зв'язку з тим, що списання коштів відбулось несанкціоновано, фізична особа за телефоном гарячої лінії повідомила про факт шахрайства, звернулась з вимогою заблокувати відкриті на її ім'я картки, повернути списані з поточних рахунків грошові кошти. У ході судового розгляду встановлено, що списання коштів з фізичної особи здійснено через «фітингову» систему шахраїв, яка розрахована не тільки на неуважність користувачів системи «Приват 24», а й на наявність особливостей деяких сервісів системи «Приват 24», які шахрай може використовувати для обману користувачів системи. Ураховуючи відсутність обставин, які безспірно доводять, що фізична особа своїми діями чи бездіяльністю сприяла втраті, незаконному використанню пін-коду або іншої інформації, яка дає змогу ініціювати платіжні операції, суд зобов'язав банк повернути кошти [281].

У даній справі наявний технічний ризик, який полягає у наявності особливостей деяких сервісів системи «Приват 24», які шахрай може використовувати для обману користувачів системи. На час розгляду цієї справи діяв Закон України від 14.10.2014 р №1702-VII, де виокремлювалися фінансові операції, які підлягали обов'язковому фінансовому моніторингу та сумнівні фінансові операції (ст. 15 Закону). На даний час є Закон України від 06.12.2019 р № 361-IX,

відповідно до якого виокремлюються порогові та підозрілі фінансові операції (ст. 20, 21). Якщо проаналізувати дану справу відповідно до чинного Закону, то фінансова операція класифікувалася би як підозріла і могла бути об'єктом фінансового моніторингу (ч.1 ст. 21 Закону). В той же час, окрема типова операція, що повинна бути підозрілою не врахована при моніторингу працівниками банку у зв'язку з прогалинами у локальних нормативно-правових актах. Як висновок по справі можна зазначити, що банком не віднесено до операцій, що підлягають фінансовому моніторингу певних дій з фінансовими інструментами, які чітко були правовими ризиками банківських послуг.

Між фізичною особою та недержавним банком підписано заяву про відкриття поточного рахунку, оформлення картки зі зразками підписів та відбитка печатки. Протягом 11.03.2015 р. по 20.03.2015 р. з рахунку особи поступово списувалися кошти з кредитного ліміту. Як наслідок, вона вимагала відшкодувати завдані їй збитки. Дана вимога, на думку суду, була необґрунтованою, зважаючи на наступне. У ході судового розгляду встановлено, що в акаунті Приват 24 особи до 12.03.2015 р. вхід здійснювався за логіном та статичним паролем, платіжні доручення підписувались ЕЦП клієнта. Ключ та пароль зберігався на накопичувачі і на жорсткому диску комп'ютера. Враховуючи те, що ключами та паролями доступу програмного комплексу «Приват24», як і самим комп'ютером користувалася не тільки фізична, а й треті особи, обмеження на вхід за IP-адресами не встановлювалося, користувач своїми діями (бездіяльністю) сприяв втраті, незаконному використанню інформації, яка дає змогу ініціювати платіжні операції [287].

У цій справі наявний технічний ризик. Для його усунення клієнт має стежити за безпекою даних, які дозволяють здійснювати розрахунки за допомогою електронних платіжних засобів (унеможливлювати доступ третіх осіб до пристроїв, де зберігаються такі дані), а також встановити обмеження на вхід за IP адресами. На час розгляду цієї справи діяв Закон України від 14.10.2014 р № 1702-VII від 14.10.2014 р, де виокремлювалися фінансові операції, які підлягали обов'язковому фінансовому моніторингу та сумнівні фінансові

операції (ст. 15 Закону). На даний час є чинним Закон України від 06.12.2019 р. № 361-IX, відповідно до якого виокремлюються порогові та підозрілі фінансові операції (ст. 20, 21). Якщо проаналізувати дану справу відповідно до чинного Закону, то фінансова операція класифікувалася би як підозріла і могла бути об'єктом фінансового моніторингу (ч.1 ст. 21 Закону). Отже, банком не застосовані своєчасні заходи для усунення правового та технічного ризиків, що призвело до завдання збитків клієнтам банку при користуванні його послугами.

На користь фізичної особи стягнуто з недержавного банку 1 грошові кошти в розмірі 355 250,00 доларів США. У ході примусового виконання рішення суду, що здійснювалось державним виконавцем звернуто кошти, що належать недержавному банку 1 з рахунку недержавного банку 2 шляхом направлення платіжної вимоги на суму 390 775,00 доларів США, яка отримана ним у той же день. Проте 26 листопада 2014 року недержавний банк 2 повернув платіжну вимогу без виконання. У зв'язку з цим державний виконавець був змушений вдатися до більш складної та тривалої процедури звернення стягнення на кошти боржника в національній валюті, що перебувають в інших фінансових установах, та подальшої закупівлі іноземної валюти. Під час подальшого виконавчого провадження з боржника стягнуто кошти в гривнях, на які державним виконавцем закуплено іноземну валюту в сумі 235 382,88 доларів США. Залишок нестягнутої з недержавного банку 1 грошової суми становив 119 867,12 доларів США. У подальшому, у зв'язку із ініціюванням Національним банком України та Фондом гарантування вкладів фізичних осіб відкликання банківської ліцензії та його ліквідації, виконавче провадження закінчено, і вказана сума залишилась нестягнутою. За результатами розгляду справи суд установив, що платіжна вимога повернена недержавним банком 2 без виконання без підставно [280].

На думку авторів, риси наведеної операції не співпадають з ознаками фінансової операції, що підлягає фінансовому моніторингу, тому Закон України від 06.12.2019 р. № 361-IX, не розповсюджується на таку операцію. Відповідно до його положень наведена операція не

підпадає під критерії порогової чи підозрілої. У даній справі наявний операційний ризик пов'язаний з несумлінним виконанням обов'язків уповноваженою посадовою особою банку, що виникають з вимог функціонування платіжних систем. Таким чином, операція підтверджує несумлінне виконання або навмисне невиконання службовцями банку своїх обов'язків.

ПАТ та недержавний банк уклали договір банківського рахунку інституту спільного інвестування. 26.09.2013 р. недержавним банком з депозитного рахунку ПАТ списані грошові кошти в сумі 128 000,00 грн. та перераховані на поточний рахунок ПАТ, а в подальшому – перераховані на рахунок сторонньої фізичної особи. Згодом, під час службового розслідування виявилось, що переказ коштів був несанкціонований. У ході судового розгляду проаналізовано вимоги чинного законодавства, договору та з'ясовано, що на недержавний банк покладався обов'язок перевірити зміст розрахункового документа на списання коштів. Внаслідок незабезпечення банком належного збереження коштів клієнта, йому завдано збитків в розмірі 128 000,00 грн [274].

У даній справі, на думку автора, наявні два ризики – правовий та операційний. Для усунення правового ризику необхідно на законодавчому рівні передбачити обов'язок банку у випадку надходження розрахункового документу на списання коштів з рахунку для обслуговування активів у грошовій формі здійснити перевірку відповідності такого списання вимогам чинного законодавства України, а за результатами перевірки не пізніше наступного робочого дня з дати надання йому відповідних розрахункових документів надати згоду на списання коштів з рахунку, відкритого для обслуговування активів в грошових коштах або, в той же строк надати мотивовану письмову відмову від такого списання. Щодо операційного ризику, на думку автора, у внутрішніх правилах роботи банку необхідно передбачити алгоритм поведінки працівників у випадку виникнення подібної ситуації. На час розгляду цієї справи діяв Закон України від 14.10.2014 р. №1702-VII, де виокремлювалися фінансові операції, які підлягали обов'язковому фінансовому моніторингу та сумнівні фінансові операції (ст. 15 Закону).

На даний час є чинним Закон України від 06.12.2019 р. № 361-IX, відповідно до якого виокремлюються порогові та підозрілі фінансові операції (ст. 20, 21). Якщо проаналізувати дану справу відповідно до чинного Закону, то фінансова операція класифікувалася б як підозріла і могла бути об'єктом фінансового моніторингу (ч.1 ст. 21 Закону). Таким чином, в діях банку присутнє нехтування обмеженнями для колективних активів, що потребує додаткового договірного регулювання. Як висновок, операція одночасно підпадає під фінансовий моніторинг як підозріла, а її проведення стало результатом порушення обов'язків службовцями банку.

Фізична особа 1 викрав у фізичної особи 2 близько 04.30 год. 20.12.2015 р. цінне майно, зокрема кредитну карту недержавного банку, з якої через банкомат зняв грошові кошти в сумі 7 357,10 гривень, чим спричинив потерпілому – фізичній особі 2 матеріального збитку на загальну суму 16 326,63 гривень. Він же, 12.03.2016 р. приблизно з 11.00 години до 18.00 год., знаходячись в кафе-барі спільно з фізичною особою 3, викрав у останньої банківську карту недержавного банку та мобільний телефон, в якому було вказано код на вхід на цю картку. Після цього фізична особа 1 через банкомат згаданого вище банку отримав грошові кошти двома операціями 200 та 500 гривень, які використав на власні потреби. Суд, з'ясувавши всі обставини справи та дослідивши докази, визнав винуватим Особу 1 за ч. 1 ст. 361, ч. 2 ст. 185, ч. ст. 186 КК України [100].

Злочинна спрямованість цих операцій не співпадає з метою регулювання Закону України від 06.12.2019 р. № 361-IX, тому фінансовий моніторинг є неможливим. Відповідно до його положень наведена операція не підпадає під критерії порогової чи підозрілої.

У даній справі наявний операційний ризик пов'язаний з втратою контролю над карткою банку та засобами доступу до неї та ступеня вини потерпілої фізичної особи 1. Таким чином, збитки фізичній особі завдані у зв'язку з наявністю операційного та правового ризиків при крадіжках банківських карт, при цьому відсутні достатні методи захисту доступу до коштів, а вина за збереження паролів перекладається на користувачів банківських карт.

Фізична особа 1 без наміру здійснення статутної діяльності підприємства, придбав на території м. Києва два суб'єкти господарської діяльності з метою прикриття незаконної діяльності, і вирішив зареєструвати їх на третіх осіб. З цією метою фізична особа 1 у лютому 2015 року з кола своїх знайомих підшукав фізичну особу 2 з метою реєстрації на нього ТОВ, запевнивши його, що він буде власником та директором підприємства, яке буде здійснювати статутну діяльність. Проте фактично, керівництвом займалась фізична особа 1, встановивши над ним повний контроль, отримавши у володіння установчі, реєстраційні документи та печатку підприємства поштою за адресою свого проживання.

Фізична особа 1 відкрив поточні рахунки в банківських установах, отримав ключі доступу до систем електронних платежів «Клієнт-Банк» та отримав електронний цифровий підпис для підпису та подання податкової звітності. Подібна схема здійснена фізичною особою 1 й у березні 2015 року, коли та підшукала з кола своїх знайомих малозабезпечену особу, з метою реєстрації на неї підприємства ТОВ 2. За результатами розгляду справи між прокурором та обвинуваченим укладено угоду про визнання винуватості за ч.1 ст.205 КК України. Сторони узгодили покарання у виді штрафу у розмірі 8 500 грн [99].

На думку авторів спрямованість операції не співпадає з метою регулювання Закону України від 06.12.2019 р. № 361-IX, тому фінансовий моніторинг є неможливим на етапі створення фіктивного підприємства. Але при організації діяльності ТОВ банк не міг знати, який суб'єкт господарювання та його посадові особи здійснюють операції. Відповідно до його положень наведена операція не підпадає під критерії порогової чи підозрілої. На думку автора у даній справі наявний технічний ризик. Для його подолання керівники підприємств мають убезпечити доступ до електронного цифрового підпису, ключу доступу до системи електронних платежів «Клієнт-Банк». Отже, цей приклад свідчить про наявність технічного та, як наслідок, правового ризику, при яких банком не передбачено механізму моніторингу власників рахунків та доступу до них.

Фізична особа 1, перебуваючи на посаді старшого касира недержавного банку, вчинила розтрату майна, що було їй ввірене, при наступних обставинах: начальник недержавного банку фізична особа 2, з метою заволодіння коштами клієнта банку (фізичної особи 3), що перебували на поточному рахунку, вступила в попередню злочинну змову із своєю підлеглою фізичною особою 1, надавши вказівку останній видати їй з поточного рахунку фізичної особи 3 грошові кошти в сумі 8800 доларів США, шляхом складання заяви на видачу готівки на вказану суму та проведення відповідної операції без відома останньої. З метою відображення операції по видачі готівки з каси банку з рахунку фізичної особи 3, фізична особа 1 в програмному комплексі «Flex Cube» підтвердила вчинення касової операції з видачі готівки, склала та роздрукувала заяву на видачу готівки, яку підписала від свого імені у графі «Підпис банку» та передала фізичній особі 2 для вчинення підпису в графі «Підпис отримувача». Остання у свою чергу вчинивши підпис, передала фізичній особі 1 заяву на видачу готівки для формування касових документів. Окрім того, між фізичною особою 2 та фізичною особою 4 укладено договір банківського вкладу про відкриття депозитного рахунку в сумі 8 000 євро з нарахуванням 7 % річних. По закінченні дії договору кошти автоматично перераховані на поточний рахунок фізичної особи 4. Остання звернулася до фізичної особи 2 для отримання свого депозиту в розмірі 8 000 євро та нарахованих відсотків. Однак остання з метою незаконного заволодіння коштами клієнта вмовила його укласти два нові договори банківського вкладу. Складаючи їх, фізична особа 2 один з них не зареєструвала. Згодом вона, не маючи прямого доступу до коштів, що перебувають у касі банку, вступила в попередню злочинну змову із фізичною особою 1, надавши вказівку останній провести касову операцію з видачі коштів в сумі 8 046 євро з поточного рахунку фізичної особи 4, провести вказану операцію в програмному комплексі «СБОН+». Фізична особа 2 надала незаконну вказівку економісту недержавного банку внести в програмний комплекс банку «Flex Cube» дані щодо дострокового розірвання укладених із фізичною особою 4 не повідомляючи останню, у зв'язку з чим кошти в

сумі 87 671,31 грн. автоматично перераховані на поточний рахунок фізичної особи 2 [98].

На думку авторів, спрямованість операції не співпадає з метою Закону України від 06.12.2019 р. № 361-IX. Тому фінансовий моніторинг є неможливим. Відповідно до його положень наведена операція не підпадає під критерії порогової чи підозрілої. У даній справі наявний операційний ризик пов'язаний з умисним невиконанням посадових обов'язків працівників банку. Приклад показує, що деякі операції щодо переказу коштів та депозитні операції не підпадають під дію законодавства про фінансовий моніторинг, і в цьому випадку не можуть бути відслідковані, хоча мають злочинне походження.

Фізична особа 1 зареєструвалася як фізична особа-підприємець та звернулася у філію державного банку із заявою про відкриття поточного рахунку, внаслідок чого укладено договір банківського рахунку та відкрито поточний розрахунковий рахунок. 24.02.2014 р. фізична особа 1 у приміщенні філії державного банку, уклала договір на еквайрингове обслуговування та договір оренди устаткування, згідно якого отримала електронний пристрій та прийняла у строкове тимчасове користування устаткування POS-термінал, після чого звернулась із відповідною заявою до банку про підключення до системи клієнт-банк. 04.03.2014 р. з фізичною особою 1 укладено договір на виконання розрахункових операцій системою дистанційного обслуговування «Інтернет-Клієнт-Банк». У подальшому вона, придбавши у невстановлених осіб підроблені банківські картки, з використанням банківського програмного забезпечення та орендованого POS-терміналу, заволоділа грошовими коштами, які знаходились на банківських картках, здійснивши 84 трансакції, наслідком яких стало перерахування на його поточний рахунок грошових коштів в загальній сумі 4 865 805,00 грн., що завдало державному банку шкоди в особливо великих розмірах [97].

На час розгляду цієї справи діяв Закон України від 14.10.2014 р. №1702-VII, де виокремлювалися фінансові операції, які підлягали обов'язковому фінансовому моніторингу та сумнівні фінансові операції (ст. 15 Закону). На даний час є чинним Закон України від

06.12.2019 р. № **361-IX**, відповідно до якого виокремлюються порогові та підозрілі фінансові операції (ст. 20, 21). Якщо проаналізувати дану справу відповідно до чинного Закону, то фінансова операція класифікувалася як підозріла і могла бути об'єктом фінансового моніторингу (ч.1 ст. 21 Закону).

У даній справі наявний операційний ризик, який чітко може бути відслідкований засобами фінансового моніторингу. Для його подолання, на думку авторів, банку необхідно здійснювати моніторинг підозрілої активності (у справі відбулося 84 трансакції з іноземних банківських карток на один банківський рахунок на суму більше 4 000 000). Вищенаведені операції здійснені у період чинності Закону України від 14.10.2014 р. №1702-VII. У цей період проаналізовані операції були об'єктом обов'язкового фінансового моніторингу, але з прийняттям нового Закону України від 06.12.2019 р. № 361-IX за своїми ознаками вони можуть бути класифіковані як підозрілі (ст. 21 Закону, п. 2.1.3. розділ 2 Типологічного дослідження «Актуальні методи і способи легалізації (відмивання) доходів, одержаних злочинним шляхом, та фінансування тероризму від 2012 р.) [68].

11.06.2018 р. прийнято «Положення про організацію системи управління ризиками в банках України та банківських групах», затверджене Постановою Національного банку України № 64 [270] (далі – постанова НБУ від 11.08.2018 р. № 64). У зазначеному нормативному акті виокремлено поняття операційного ризику, а саме: «операційний ризик – імовірність виникнення збитків або додаткових втрат або недоотримання запланованих доходів унаслідок недоліків або помилок в організації внутрішніх процесів, навмисних або ненавмисних дій працівників банку або інших осіб, збоїв у роботі інформаційних систем банку або внаслідок впливу зовнішніх факторів. Операційний ризик включає юридичний ризик, однак має виключати ризик репутації та стратегічний ризик». На думку авторів, з метою удосконалення даної проблематики, необхідно окремо виділити правові ризики, оскільки вони можуть мати самостійну класифікацію, наприклад, в кримінальному праві та окремий склад ознак ризиків. Окрім того наведений у визначенні юридичний ризик не охоплює всі мож-

ливі правові ризики, оскільки стосується порушень умов договору, проте не включає заборонені та злочинні дії працівників банків.

Розглянемо погляди науковців, що досліджували дану тематику. Окремі з них констатують появу проблем в управлінні ризиками платіжних систем у зв'язку з необхідністю їхнього функціонування в умовах ринкової економіки. Зокрема О. Г. Череп наголошує на появі нових факторів ризику, пов'язаних зі впровадженням сучасних технологій розрахунків на базі новітньої техніки та засобів зв'язку, що в свою чергу ускладнює внутрішню структуру системи. Конкретний вид ризику дослідником не визначається, однак, ці фактори відносяться до технічного ризику. Серед способів управління ризиками він пропонує виокремити дві групи: організаційно-технічні та фінансово-договірні способи [370].

І. Пищик та А. Дорошкевич пропонують класифікацію з чотирьох видів ризиків: правового, операційного, розрахункового та системного. Окрім того, автори наводять фактори впливу цих ризиків, а також процедури управління кожним названим видом. Більша частина статті приділяється висвітленню інституційних проблем та рішень (наприклад, функціонуванню системи АС МБР чи поєднанню валових розрахунків з нетто розрахунками). Розглядаючи питання правового ризику, дослідники аналізують білоруське законодавство та вказують на високий рівень урегульованості даного питання, про що свідчить наявність структурної правої бази з підтримки та обробки електронних платежів; повнота та обов'язковість договірних відносин; заходи безпеки, що передбачають заставні механізми, операції РЕПО, визначений час остаточних розрахунків, відсутність «нульового часу» тощо.

Окрема увага присвячена й безпеці розрахункової системи, зокрема, впровадженню криптографічного шифрування інформації, сертифікації електронного підпису, використанню засобів розмежування прав доступу, діяльності системи реагування на спроби несанкціонованого доступу, застосуванням заходів об'єктової безпеки. На думку авторів, згадані засоби усунення ризиків представляють сукупність правових засобів протидії ризикам в платіжних системах [261].

Д. Угнур пропонує класифікацію ризиків, що складається з правового ризику, ризику ліквідності, кредитного та операційного ризику, а також системного ризику. Д. Угнур також наголошує на особливостях діяльності небанківських постачальників послуг (поштові відділення, телекомунікаційні компанії, пристрої самообслуговування). Окремо вказується на необхідність запровадження «обмежувачів» роздрібних платежів (використання фінансових лімітів; ідентифікаційного коду та сертифікованого обладнання, аутентифікація користувача через інфраструктуру відкритих ключів тощо). Однак зауваження автора стосуються сфери економічних відносин, пов'язаних з платіжними послугами, й не розглядають правові ризики, а пропозиції носять більш технологічний характер, які переважно усувають уразливості операційних ризиків [361].

С. В. Діденко слушно наголошує на необхідності побудови системи ризик-менеджменту на основі оцінки якісних та кількісних характеристик ризиків, а також шляхів їх оптимізації та мінімізації. С. В. Діденко загострює свою увагу на теоретичних поняттях ризику (зокрема його зв'язку з «невизначеністю»; трактуванні ризику як самостійної величини та окремого об'єкту торгівлі) та математичних (фінансових) методах його розрахунку. Корисним також є наведення розгалуженої системи класифікації ризиків. На окрему увагу заслуговує таблиця щодо механізму легалізації незаконних доходів, яка виділяє фінансовий, операційний та бізнес-ризик, а також категорії «ризик клієнта», «ризик послуги» та «ризик країни». Втім автор не використовує термін «правовий ризик», називаючи це «ризиком легалізації», та не приділяє увагу правовим аспектам даної проблеми, звертаючи свою увагу лише на попереджувальну політику банку [141].

І. Б. Чайкін, розглядаючи питання класифікації ризиків, сформулював категорію юридичного ризику, якому надав наступне визначення: юридичний ризик – це суб'єктивно-об'єктивна обумовлена категорія, яка характеризується ймовірністю настання негативних наслідків, що виникає через порушення або недотримання вимог законів, нормативно-правових актів, угод, прийнятої практики або етичних норм, а також через можливість двозначного їх тлумачення [368].

Н. М. Внукова розглядає питання впровадження для управління ризиками фінансового моніторингу системи комплаєнс-контролю, яка закріплена в рекомендаціях Базельського комітету з питань банківського нагляду. Вчена зазначає, що комплаєнс формує основу контролю будь-якої фінансової установи, що функціонує за тими чи іншими правилами і є обов'язковою складовою системи управління, зокрема, щодо попередження ризиків фінансового моніторингу. У праці науковець виділяє функції комплаєнс-контролю, а саме аналітичну, інформаційну, попереджувальну, наводить приклади запровадження управління ризиком комплаєнс у банках ПАТ «КРЕДОБАНК», ПАТ «Креді Агріколь Банк». Водночас вона звертає увагу на те, що система комплаєнс-контролю ризиків потребує розвитку і має бути адаптована до вимог сучасної міжнародної практики. Впровадження й ефективне здійснення комплаєнс-контролю ризиків сприятиме позитивній діловій репутації, мінімізації витрат та збереженню активів банку через систему фінансового моніторингу, який ґрунтується на зарубіжному досвіді [110, с. 65]. На наш погляд, у діяльність банків доцільно впроваджувати інформаційні технології, наприклад, автоматизовані системи управління, які дозволять контролювати потоки фінансів правильність проведення транзакцій сум залишків на рахунках [27, с. 171].

С. В. Глібко пропонує впроваджувати у діяльність банків інформаційні технології, наприклад, автоматизовані системи управління, які дозволять контролювати потоки фінансів правильність проведення транзакцій сум залишків на рахунках [27, с. 171].

Крім того, розглянуто проблеми відкриття рахунків у банках та використання інновацій банками при використанні мережі Інтернет. Висновками з цих питань стали: важливого впливу зазнає послуга розрахунково-касового обслуговування від публічних зобов'язань банків, які виникають під час обслуговування клієнта на підставі законодавства щодо запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, валютного та податкового законодавства (зокрема, ст. 69 Податкового кодексу України) та касових операцій тощо [126, с. 130]. Також зроблено висновок, що одним із завдань для забезпечення інтересів платників при переказі коштів

є визначення загальних технологічних норм і стандартів щодо проведення банківських операцій та інших фінансових послуг для усунення конфліктів [125, с. 165].

Таким чином, в наукових працях виокремлюються різноманітні види ризиків, серед яких є: правовий ризик, економічний ризик, операційний ризик, розрахунковий ризик (що включає кредитний ризик та ризик ліквідності) (І. Пищик та А. Дорошкевич), системний ризик, фінансовий ризик (з його валютним, ринковим та менеджмент аспектами) (С. В. Діденко), бізнес-ризик.

Різногалузеві дослідження ризиків платіжних послуг свідчать про відсутність єдиного розуміння в правовій та економічній доктринах системи заходів, що усуває ці ризики. Завданнями у цій сфері є розроблення теоретичних моделей захисту прав та інтересів платників та прийняття відповідних нормативно-правових актів.

Що стосується відображення класифікації ризиків в нормативно-правових актах України та попередження їх настання, то в вітчизняному законодавстві цим питанням присвячений ряд норм, що розміщені у різних законах та підзаконних актах.

Нормативне визначення терміну «правовий ризик» надається в Положенні про оверсайт платіжних систем та систем розрахунків в України, затвердженого Постановою Національного банку України від 28.11.2014 р. № 755 (далі – Постанова НБУ від 28.11.2014 № 755) закріплює, що правовим ризиком є ризик відсутності правового регулювання, зміни або непередбачуваного застосування положень законодавства, що можуть призвести до виникнення збитків платіжної організації платіжної системи та/або її учасників [311].

Деякі нормативно-правові акти конкретизують даний вид ризику, адаптуючи його до цілей конкретного акту. Наприклад, термін «ризики» в Законі від 06.12.2019 р. № 361-IX говорить про небезпеку (загрозу, уразливі місця) для суб'єктів первинного фінансового моніторингу бути використаними з метою легалізації доходів, одержаних злочинним шляхом, фінансування тероризму та/або фінансування розповсюдження зброї масового знищення під час надання ними послуг відповідно до характеру їх діяльності.

Положення про здійснення банками фінансового моніторингу, затверджене Постановою Правління Національного банку України від 26.06.2015 р. № 417 запроваджує базові механізми контролю за ризиками при здійсненні фінансових операцій, а також визначає критерії такого контролю. Окремий інтерес представляють Додатки до даного Положення. Додатки 1-3, 6, 7 та 11 регулюють належну перевірку та ідентифікацію клієнтів (зокрема з використанням сучасних технологій: відеоверіфікацію). Додаток 4 присвячений встановленню кінцевих бенефіціарних власників. Додаток 9 регулює особливості обслуговування рахунків політично значущих осіб, членів їх сімей та осіб, пов'язаними з ними. Додаток 14 встановлює Порядок замороження активів в разі підозри на ФТ чи розповсюдження зброї масового знищення. Додаток 15 встановлює Порядок моніторингу фінансових операцій. Уваги заслуговують Додатки 19 та 20, що встановлюють критерії Ризику ВК/ФТ, а також Індикатори підозрілості фінансових операцій. Переважна частина запроваджених контрольних механізмів спрямована на подолання можливих правових ризиків [266].

Закон України від 06.12.2019 р. № 361-IX регулює ряд важливих положень у сфері контролю за ризиками здійснення фінансових операцій. Зокрема Закон надає визначення (та критерії) таким термінам як «ризик», «високий ризик», «належна перевірка», «підозрілі фінансові операції», «управління ризиками», «верифікація», «банк-оболонка», «фінансовий моніторинг», «ідентифікаційні дані», «кінцевий бенефіціарний власник», «національна оцінка ризиків» тощо. Окрім того нормативно-правовий акт проголошує застосування ризик-орієнтованого підходу як принципу. Інструментарій, який надається цим актом, передбачає можливість зупиняти операції та заморожувати активи, що здійснюється з метою попередження можливих правових ризиків кримінального характеру.

Постанова НБУ «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України» від 28.09.2017 р. № 95 встановлює обов'язкові мінімальні вимоги щодо забезпечення інформаційної безпеки та кіберзахисту, принципи управління інформаційною безпекою, а також вимоги до інфор-

маційних систем банку. Даний акт надає визначення ряду технічних термінів: «багатофакторна аутентифікація», «зловмисний код», «пристрої уніфікованого управління загрозами». Положення також запроваджує ризик-орієнтований підхід й визначає поняття критичних бізнес-процесів банку. Окрім того акт передбачає Принципи криптографічного захисту НБУ, заходи безпеки інформації та передумови та вимоги впровадження СУІБ у діяльності банків, а також обов'язкові сфери її застосування. Основна частина нормативних положень стосується недопущення технічних ризиків у діяльності банків [313].

На увагу також заслуговує ДСТУ ISO/IEC 27001:2015, що був затверджений Наказом від 18.12.2015 р. № 193 з метою гармонізації нормативних актів України з міжнародними актами. Всі терміни, використані в даному акті, походять з ISO/IEC 27000. Перш за все цей ДСТУ регулює технічні аспекти ризиків та способи їх попередження: визначає принципи та сферу застосування системи управління інформаційною безпекою; регулює зобов'язання вищого керівництва; планування, яке передбачає дії щодо можливих ризиків та можливостей, оцінку ризиків інформаційної безпеки, оброблення ризиків; оцінку результативності, що включає моніторинг, аналіз, внутрішній аудит; тощо. ДСТУ також містить Додаток «А», що передбачає цілі та конкретні заходи безпеки (наприклад, норми віддаленої роботи, управління ресурсами СУІБ, поводження з носіями, контроль доступу, доступ користувача, криптографію, контроль програмного забезпечення, безпеку комунікацій тощо) [148].

Постанова НБУ від 28.11.2014 р. № 755 заслуговує на увагу, оскільки приділяє значну увагу регулюванню ризиків в платіжних системах та надає багато нормативних визначень, пов'язаних з ними. Зокрема, дане Положення використовує та тлумачить терміни «депозитарний ризик», «загальний комерційний ризик», «інвестиційний ризик», «кіберризик», «кредитний ризик», «операційний ризик», «правовий ризик», «ризик ліквідності», «розрахунковий ризик», «системний ризик». Окрім того нормативно-правовий акт застосовує поняття «управління операційним ризиком», «спільний оверсайт платіжних систем», «кіберстійкість платіжної системи», «кіберзагроза» тощо. Для перевірки

виконання нормативних вимог дане Положення покладає на НБУ повноваження здійснювати моніторинг платіжних систем [311].

Методика комплексного оцінювання системно важливих платіжних систем, схвалено Постановою Правління Національного банку України від 24.09.2015 р. № 635 визначає методологію перевірки платіжних систем на предмет дотримання міжнародних стандартів нагляду (оверсайта) та законодавства України. Методика визначає ряд принципів, які стосуються правил діяльності платіжних систем, процедур та стандартів передавання інформації в платіжній системі, діяльності системи комплексного управління ризиками тощо. Зокрема названий акт регламентує управління кредитним ризиком, ризиком ліквідності, комерційним ризиком, операційним ризиком, депозитарним та інвестиційним ризиками. Серед іншого Методика передбачає критерії для визначення стану дотримання встановлених принципів, а також Додатки для самооцінювання [228].

Інструкція про безготівкові розрахунки в Україні, затверджена Постановою Правління Національного банку України від 21.01.2004 р. № 22 встановлює загальні правила, види і стандарти безготівкових розрахунків клієнтів банків в національній валюті. Акт встановлює ряд важливих вимог: наприклад, правило, за яким кошти з рахунків клієнтів можуть списуватися виключно за дорученнями власників цих рахунків; загальні правила документообігу. Інструкція також регулює безпосередні операції з рахунками, такі як «списання за дорученням», «договірне списання», «примусове списання» й окремі види розрахунків, як «розрахунки за допомогою систем дистанційного обслуговування» тощо. Окрім того НПА встановлює порядок виконання заходів щодо арешту коштів та списання коштів, отриманих від корупційних та інших злочинів. Втім текст наведеного акту жодного разу не використовує термін «ризик» [171].

Закон України «Про платіжні системи та переказ коштів» від 05.04.2001 р. № 2346-III надає визначення ряду поширених термінів, що застосовуються при взаємодії з платіжними системами. До них відноситься «платіжний інструмент» (зокрема «мобільний платіжний інструмент»), «платіжний термінал», «платіжний пристрій» тощо.

Також даний Закон визначає терміни, що стосуються нагляду за переказом коштів, такі як «оверсайт» чи «реконсиляція». Слід відмітити, що закон регулює питання ризиків в такій діяльності: наприклад, обов'язок банку включити в правила платіжної системи управління ризиками; обов'язок попереджати клієнта про випадки підвищеного ризику під час використання електронного платіжного засобу та можливість обмеження способів та місць використання тощо [320].

Окрім іншого, даним нормативно-правовим актом передбачається можливість договірного врегулювання відносин між клієнтом та банком, зокрема передбачається право укладення договору про розрахунково-касове обслуговування, що випливає зі змісту п. 1. ст. 37 Закону; ініціювання переказу при договірному списанні, що закріплюється ст. ст. 26 Закону тощо [320].

Постанова Правління Національного банку України «Про здійснення операцій з використанням електронних платіжних засобів», від 05.11.2014 р. № 705 встановлює перелік вимог, що стосуються контролю за ризиками при здійсненні відповідних операцій. Між іншим акт накладає на банк обов'язок включити до власних внутрішньобанківських правил систему управління ризиками під час здійснення платіжних операцій, включаючи порядок оцінки кредитного, операційного ризику, оцінки ризиків відмивання коштів, фінансування тероризму та фінансування розповсюдження зброї масового знищення, а також порядок урегулювання неплатоспроможності й інших випадків невиконання банком своїх зобов'язань. Розділ VI повністю присвячений викладенню загальних вимог до безпеки здійснення платіжних операцій та управління ризиками.

Наведений акт приділяє увагу як правовим ризики, так і технічним ризикам: наприклад, встановлює умови передання електронного платіжного засобу третій особі; наслідки втрати електронного платіжного засобу; наслідки витоку інформації, яка дає змогу ініціювати платіжні операції через дії чи бездіяльність клієнту тощо [316].

Таким чином, судова практика, наукові дослідження потребують наукової систематизації проблем з класифікацією ризиків та розроблення законодавства, що врегульовує усунення ризиків в фінансових операціях з коштами.