VIII. ФИНАНСЫ, ДЕНЕЖНОЕ ОБРАЩЕНИЕ И КРЕДИТ. ПРОБЛЕМЫ АНАЛИЗА ФИНАНСОВО-ХОЗЯЙСТВЕННОЙ ДЕЯТЕЛЬНОСТИ. БУХГАЛТЕРСКИЙ УЧЁТ И СТАТИСТИКА

УДК 336.02

D.F. Zakirova

FORMATION OF PROMISING DIRECTIONS FOR IMPROVING THE SYSTEM OF FINANCIAL MONITORING ORGANIZATION IN CREDIT INSTITUTIONS

In the modern world, permeated by complex economic ties and the rapid development of technology, the problem of money laundering and terrorist financing (hereinafter referred to as ML/FT) is becoming increasingly threatening. The state is faced with the urgent task of developing effective mechanisms to counter these negative phenomena, while it is extremely important to find a balance between ensuring securities and preserving the economic freedom of citizens. On the one hand, the fight against ML/FT requires the creation of bangs and an effective system of government regulation. On the other hand, excessive tightening of control and excessive government interference in economic activity can lead to an increase in the administrative burden on business, a decrease in the country's investment attractiveness, restriction of freedom of entrepreneurship and even an increase in the shadow sector of the economy.

The complexity of the task is aggravated by a number of factors, among which are the globalization and digitalization of the financial system, the growth of transnational crime, and the lack of effectiveness of international cooperation. At the same time, given that most of the crimes under ML/FT occur with the active participation of credit and financial institutions, the main direction of countering emerging trends is the organization of financial monitoring in banks.

Keywords: money laundering, national AML/CFT system, banks, biometrics, financial monitoring, customer identification.

Д.Ф. Закирова[1]

ФОРМИРОВАНИЕ ПЕРСПЕКТИВНЫХ НАПРАВЛЕНИЙ СОВЕРШЕНСТВОВАНИЯ СИСТЕМЫ ОРГАНИЗАЦИИ ФИНАНСОВОГО МОНИТОРИНГА В КРЕДИТНЫХ ОРГАНИЗАЦИЯХ

В современном мире, пронизанном сложными экономическими связями и стремительным развитием технологий, проблема отмывания доходов, полученных преступным путём, и финансирования терроризма (далее – ОД/ФТ) приобретает всё более угрожающие масштабы. Перед государством остро стоит задача разработки эффективных механизмов противодействия этим негативным явлениям, при этом крайне важно найти баланс между обеспечением безопасности и сохранением экономической свободы граждан. С одной стороны, борьба с ОД/ФТ требует создания чёткой и действенной системы государственного регулирования. С другой стороны, чрезмерное ужесточение контроля и избыточное вмешательство государства в экономическую деятельность могут привести к увеличению административной нагрузки на бизнес, снижению инвестиционной привлекательности страны, ограничению свободы предпринимательства и даже росту теневого сектора экономики.

Сложность задачи усугубляется рядом факторов, среди которых следует отметить глобализацию и цифровизацию финансовой системы, ростом транснациональной преступности, недостаточной эффективностью международного сотрудничества. При этом, учитывая, что большая часть преступлений по ОД/ФТ происходят при активном участии кредитно-финансовых учреждений, главным направлением противодействия складывающимся тенденциям является организация финансового мониторинга в банках.

[1] Закирова Д.Ф., доцент кафедры рекламы и связи с общественностью, кандидат экономических наук, доцент; ФГБОУ ВО "Российский государственный педагогический университет имени А.И. Герцена", г. Санкт-Петербург

Zakirova D.F., Associate Professor of the Department of Advertising and Public Relations, PhD in Economics, Associate Professor; Federal State Budgetary Educational Institution of Higher Education "Russian State Pedagogical University named after A.I. Herzen", Saint Petersburg

E-mail: dilyara159@mail.ru

Ключевые слова: отмывание денежных средств, национальная система ПОД/ФТ, банки, биометрия, финансовый мониторинг, идентификация клиентов.

DOI: 10.36807/2411-7269-2024-4-39-125-135

Банковский сектор представляется самой законодательно зарегулированной частью национальной системы ПОД/ФТ. Однако преступные элементы регулярно стараются использовать его финансовые учреждения для вовлечения в процессы ОД/ФТ, что может быть обусловлено тем, что банковский сектор является самой большой частью финансового рынка, который способен предоставлять широкий спектр услуг. Данные обстоятельства создают условия для того, чтобы именно банковский сектор испытывал постоянный высокий уровень угрозы и, учитывая, что российский банковский рынок, по сути, включается в состав мировых финансовых рынков, негативные эффекты, являющиеся последствиями несоблюдения противолегализационного законодательства, оказывают влияние на общую стабильность всей мировой банковской системы. Данные обстоятельства, особенно в условиях активного развития цифровой экономики, наличия внешнеэкономических финансовых ограничений в отношении РФ со стороны отдельных зарубежных стран обусловливают необходимость поиска новых профилактических мер противодействия.

В научно-практической литературе, посвящённой вопросам ПОД/ФТ, большое количество трудов уделяют внимание оценке юридической стороны проблемы. В частности, Кошелев К.А. [1] анализирует причины отсутствия на текущий момент в Российской Федерации закона, регулирующего обращение цифровых активов, Казбаева С.А.Ы, Исмагилов А.Е.А.ЛЫ. [2] анализируют эффективность законотворческого процесса в сфере ПОД/ФТ. Жариков Ю.С. [3] определяет специфические признаки имущества, отличающие его от законно приобретённой собственности. Гриненко А.В., Коляда А.В., Хорьяков С.Н. [4] проводят углублённое исследование различных аспектов ПОД/ФТ. Они исследуют как уголовные, так и уголовно-процессуальные и криминалистические особенности таких действий. Ряд исследователей посвящают свои исследования вопросам взаимодействия данного вида преступления с финансированием терроризма [5]–[7], легализации параллельного импорта в Российской Федерации [8], механизмам и способам легализации незаконно полученных денежных средств с использованием различных финансовых институтов (криптовалютные биржи, платёжные системы, краудфаундинговые платформы), которые считаются нетрадиционными в отношении ОД/ФТ [9]. Исследования Р.Д.А. Галали [10] и Ю.В. Евдокимовой и О.В. Шинкаревой [11] проводят сравнительный анализ существующих методик оценки рисков привлечения финансово-кредитных учреждений к ОД/ФТ, выделяя их сильные и слабые стороны. Исследователи [12]–[20] также уделяют внимание вопросам организационного плана, связанным с совершенствованием процедур идентификации клиентов, мониторинга операций, обучения персонала и реагирования на подозрительные транзакции.

Однако, на наш взгляд, в настоящее время необходимо не однобокое рассмотрение проблемы, а комплексный подход к исследованию перспективных аспектов совершенствования инструментов финансового мониторинга в финансово-кредитных учреждениях, которые будут способствовать повышению эффективности борьбы с проникновением в них преступных доходов.

Анализ национальной системы ПОД/ФТ выявляет ряд слабых мест, которые преступники активно используют для придания законного вида своим незаконно полученным средствам. Рассмотрим основные риски и уязвимости, которым подвержена российская система ПОД/ФТ, уделяя особое внимание банковской сфере[1]:

1 использование номинальных юридических лиц ("фирм-однодневок". "Фирмы-однодневки" регистрируются на подставных лиц и используются для проведения фиктивных сделок, обналичивания средств, ухода от налогов и, как следствие, отмывания доходов;

2 использование нелегальной внешнеэкономической деятельности. Схемы включают в себя занижение/завышение стоимости товаров при импорте/экспорте, фиктивные экспортно-импортные операции, использование поддельных документов и т.д.

[1] Национальная оценка рисков финансирования терроризма. Публичный отчёт 2022. [Электронный ресурс]. – URL: https://www.fedsfm.ru/content/files/отчеты%20нор/ национальная%20оценка%20рисков-фт.pdf.

3 использование юридических лиц-нерезидентов и трастов, что обусловлено сложной системой владения и низким уровнем прозрачности для выявления бенефициарных владельцев и отслеживания движения финансовых потоков;

4 использование инструментов обналичивания, что связано с анонимностью и отсутствием электронного следа наличных денежных средств;

5 использование электронных платёжных средств и виртуальных денег (типа биткоинов и пр.), что обусловлено анонимностью, высокой скоростью транзакций и отсутствием жёсткого регулирования. Согласно действующему законодательству (ст. 174 и 174.1 УК РФ[1]), преобразование цифровых активов (криптовалют и пр.), полученных в результате незаконной деятельности, в фиатные деньги (рубли, доллары и т.д.) с целью сокрытия их происхождения рассматривается как уголовно наказуемое деяние.

В своей деятельности ЦБ РФ активно использует понятие "сомнительных операций", которое является одним из ключевых категорий в выявлении и пресечении ПОД/ФТ. Под сомнительными ЦБ РФ понимает операции (сделки), которые выглядят необычными или подозрительными. ЦБ РФ понимает необычные или подозрительные операции, в отношении которых в процессе реализации внутренних мер контроля у уполномоченных сотрудников банка могут возникать подозрения, что они проводятся с целью ОД/ФТ. В таких случаях финансово-кредитные учреждения обязаны действовать в строгом соответствии с законодательством, прежде всего, Федеральным законом от 07 августа 2001 года № 115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма"[2] (далее – Федеральный закон № 115-ФЗ), в частности оно обязано:

1) приостановить операцию до выяснения обстоятельств;

2) направить соответствующую информацию в Росфинмониторинг в случае подтверждения подозрений;

3) отказать в проведении операции, если у сотрудников банка есть основания полагать, что она связана с ОД/ФТ.

Это необходимо, чтобы государственные органы могли своевременно выявлять и предотвращать преступные действия, связанные с финансами. В соответствии с Указанием Банка России от 15 июля 2021 года № 5861-У[3] финансово-кредитные учреждения формируют электронный документ в виде формализованного электронного сообщения, в котором указывают код вида операции. Данные коды вида операции состоят из четырёх числовых символов, где первые две цифры обозначают отношение к группе операций, а последующие две цифры непосредственно конкретизируют саму операцию. Наибольший интерес представляет код группы операций, который содержит лишь один код по конкретной операции, а именно 6001. Данный код означает, что у сотрудников банка возникли вопросы к происхождению денежных средств или к цели проведения операции и в соответствии с Федеральным законом № 115-ФЗ банк обязан направить соответствующую информацию в Росфинмониторинг вне зависимости от того, подпадает ли конкретная операция под обязательный контроль, предусмотренный статьёй 6 данного нормативно-правового акта.

В то же время, сам ЦБ РФ классифицирует сомнительные операции в зависимости от их содержания по следующим категориям (Рис. 1):

- транзитные операции повышенного риска;
- обналичивание денежных средств;
- вывод денежных средств за границу.

[1] Уголовный кодекс РФ от 13.06.1996 № 63-ФЗ (ред. от 12.06.2024. [Электронный ресурс]. – URL: www.consultant.ru.

[2] Федеральный закон от 07.08.2001 N 115-ФЗ (ред. от 29.05.2024) "О противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма" [Электронный ресурс]. – URL: www.consultant.ru.

[3] Указание Банка России от 15.07.2021 N 5861-У (ред. от 15.07.2021) "О порядке представления кредитными организациями в уполномоченный орган сведений и информации в соответствии со статьями 7 и 7.5 Федерального закона "О противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма" [Электронный ресурс]. – URL: www.consultant.ru.

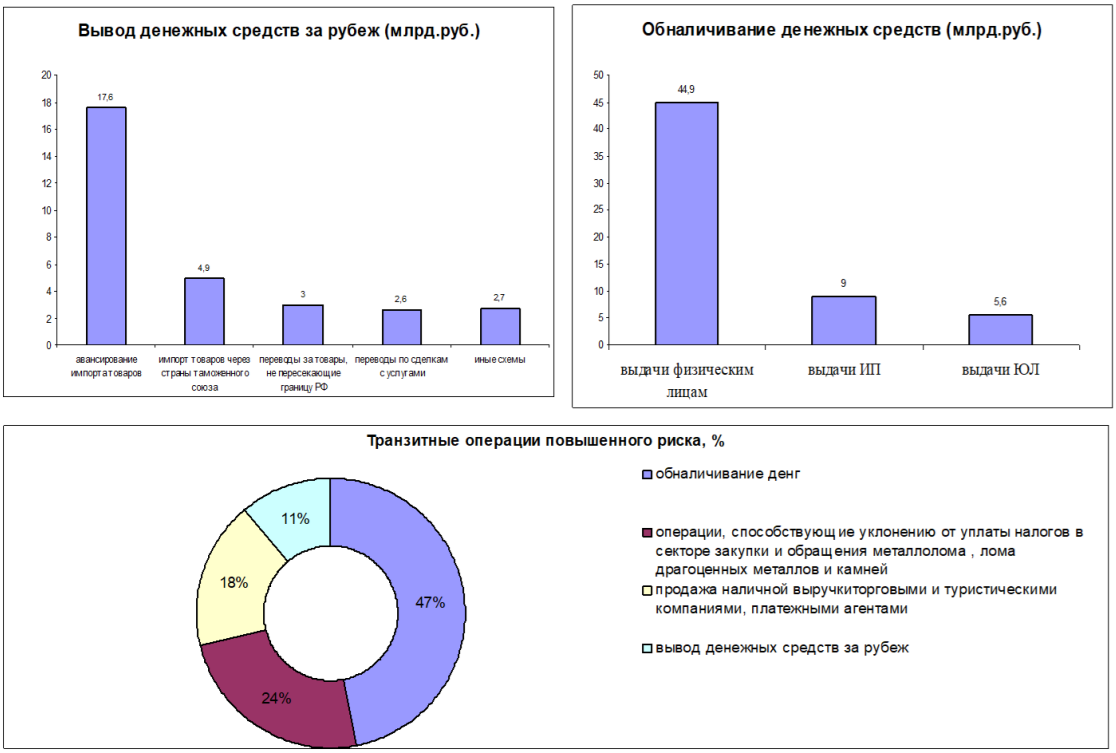

Рисунок 1 – Структура сомнительных операций в банковском секторе за 2023 г.

По данным регулятора (Рис. 1), в 2023 г. основную часть (47%) всех транзитных операций повышенного риска составляли операции, направленные на обналичивание денежных средств через счета физических лиц, включая использование платёжных карт. Это неудивительно, ведь банковские счета и карты обеспечивают анонимность и мобильность, делая их привлекательным инструментом для теневых схем. Тем не менее, обнадёживает тот факт, что объёмы операций с признаками незаконного обналичивания в российском банковском секторе сократились на 6%. Более того, объёмы сомнительных транзитных операций повышенного риска снизились ещё значительнее – на 21%[1]. Такая положительная динамика связана с рядом факторов, в числе которых усиление контроля со стороны регулятора, повышение финансовой грамотности населения, а также активное внедрение цифровых технологий. Запуск цифровой платформы ЦБ РФ "Знай своего клиента" с 1 июля 2022 г. стал важным шагом в борьбе с ОД/ФТ. Несмотря на снижение объёмов, структура операций по обналичиванию денежных средств в 2023 г. в целом сохранилась. Основной канал: выдача наличных со счетов физических лиц, включая платёжные карты (76%). Для вывода денежных средств за рубеж в 2023 г. наиболее часто применялись следующие схемы:

а) авансовые платежи за импортируемые товары (57%): заключаются фиктивные контракты на поставку товаров, которые фактически не ввозятся в страну, а деньги оседают на счетах оффшорных фирм;

б) импорт товаров через страны таможенного союза (16%): товары ввозятся по заниженной стоимости или под видом другой продукции, что позволяет уклоняться от уплаты таможенных пошлин и НДС.

Важно отметить, что потребность в теневых финансовых услугах формируется в определённых отраслях экономики. В 2023 г., как и в предыдущие годы, лидерами по привлечению теневого капитала стали: строительный сектор (32%), торговля (27%), сфера услуг (26%) (Рис. 2). Эти отрасли продолжают активно использовать нелегальные финансовые схемы для достижения своих целей.

[1] Объёмы подозрительных операций в 2023 г. сократились на 12% [Электронный ресурс]. – URL: https://businesspravo.ru/PressReleasebusinesspravo/PressReleaseShow.asp?id=769835.

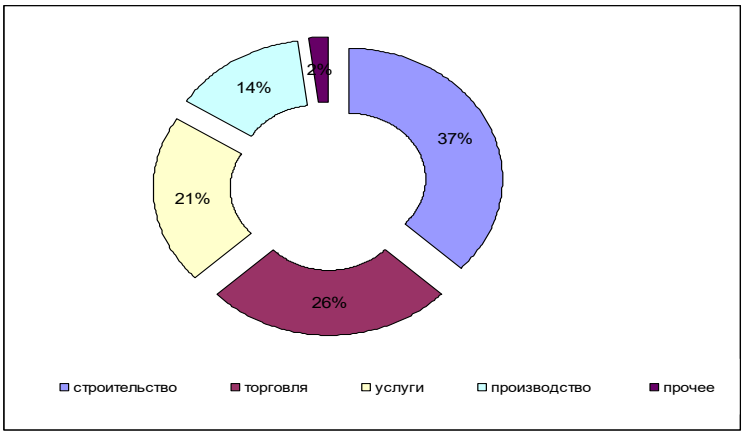

Рисунок 2 – Отрасли экономики, сформировавшие спрос на теневые финансовые услуги в 2023 г.

По мнению ЦБ РФ, транзитные операции повышенного риска считаются одними из наиболее острых угроз для финансовой стабильности России. Эти операции представляют собой передачу денежных средств на счета контролируемых организаций с последующим выводом этих средств в наличную валюту или за пределы страны. Важно отметить, что в документах, сопровождающих эти операции, часто происходит изменение целей исходящих и входящих платежей, что затрудняет отслеживание их легальности и целевого использования. Например, в основании для зачисления средств может стоять пометка, что сумма рассчитана с учётом НДС, а в основаниях списания – без учёта НДС. Этот процесс известен как "ломка НДС".

Большая часть денежных средств в таких операциях подвергается обналичиванию, т.е. переводу безналичных средств в наличные. В отличие от банковских переводов, которые оставляют цифровой след, движение наличных денег отследить гораздо сложнее. Это создаёт благоприятную среду для совершения преступлений и злоупотреблений, делая наличные "валютой выбора" для теневого сектора. Сам процесс перевода денежных средств из безналичной в наличную форму является легальным, однако он становится инструментом для незаконных операций, когда речь идёт о значительных суммах, несоразмерных с обычной деятельностью юридического или физического лица. Это вызывает подозрения у контролирующих органов и служит основанием для проведения дополнительных проверок.

Вместе с тем, денежная масса М2 в национальном определении на 01.01.2024 г. составляет 98,385 трлн руб., при этом, несмотря на то что в составе денежной массы доля наличных денег (агрегат М0) на 01.01.2024. достигла примерно 17,42%, а её удельный вес в структуре прироста денежной массы М2 невелик, в количественном измерении рост наличных денег в обращении имеет тенденцию к ежегодному существенному увеличению (Рис. 3).

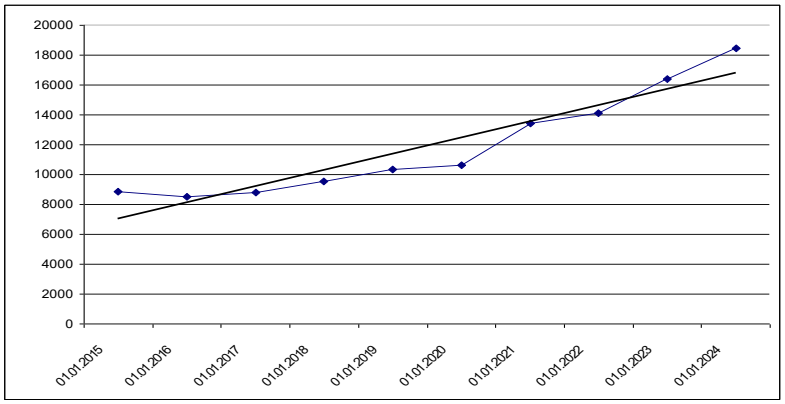

Рисунок 3 – Количество наличных денежных средств, находящихся в обращении в Российской Федерации за 2015–2023 гг., млрд руб.[1]

[1] Структура наличной денежной массы в обращении [Электронный ресурс]. – URL: https://www.cbr.ru/statistics/cash_circulation/20210101/.

Структура сомнительных операций согласно классификации ЦБ РФ включает в себя прохождение денежных средств через несколько этапов и смену юрисдикций, среди которых можно выделить следующие:

а) аккумулирование средств: преступные доходы, полученные от незаконной деятельности, накапливаются на счетах подставных лиц в одной или нескольких странах;

б) вывод капитала: накопленные средства переводятся за границу, часто с использованием сложных цепочек транзакций, оффшорных зон, подставных компаний и фиктивных сделок;

в) смена юрисдикции и легализация. Оказавшись в другой юрисдикции, часто с более мягким законодательством в области ПОД/ФТ или недостаточно эффективно работающей системой контроля, преступники придают своим доходам легитимный вид посредством инвестиций в ценные бумаги, предметы роскоши, создания новых компаний, фиктивных кредитов и других схем.

Смена юрисдикции затрудняет расследование правоохранительным органам разных стран, так как требует международного сотрудничества, которое оказывается недостаточно эффективным в силу отсутствия такой тесной взаимной интеграции национальных систем, как это происходит на национальном уровне. В результате, обмен информацией между различными юрисдикциями не всегда возможен оперативно и качественно.

Мошенники часто прибегают к различным сомнительным методам, чтобы скрыть истинную природу своих операций. Одним из таких методов является маскировка операций под расчёты с зарубежными контрагентами. Это позволяет незаконно вывести деньги за границу, избегая при этом подозрений со стороны контролирующих органов. Несмотря на определённые успехи в борьбе с нелегальным вывозом капитала, полностью его искоренить пока не удалось. Причины такого положения кроются в многочисленных лазейках, которые позволяют увести деньги за границу, зачастую с использованием сложных схем и подставных лиц. Для решения этой проблемы требуется всесторонний подход. Во-первых, необходимо усилить контроль за лицами, которые не могут документально подтвердить законное происхождение своих капиталов. Это включает в себя более тщательную проверку финансовых операций и активов, а также ужесточение наказаний за финансовые преступления. Во-вторых, нужна реформа правоохранительной и судебной систем, чтобы они могли более эффективно преследовать и наказывать нарушителей. В-третьих, важно создать благоприятный бизнес-климат, который бы снижал мотивацию вывода капитала за границу (налоговые льготы, упрощение процедур ведения бизнеса и другие меры, направленные на поддержку предпринимательства). Кроме того, международное сотрудничество в области ПОД/ФТ должно быть усилено (создание международных платформ для обмена информацией, проведение совместных расследований и т.п.).

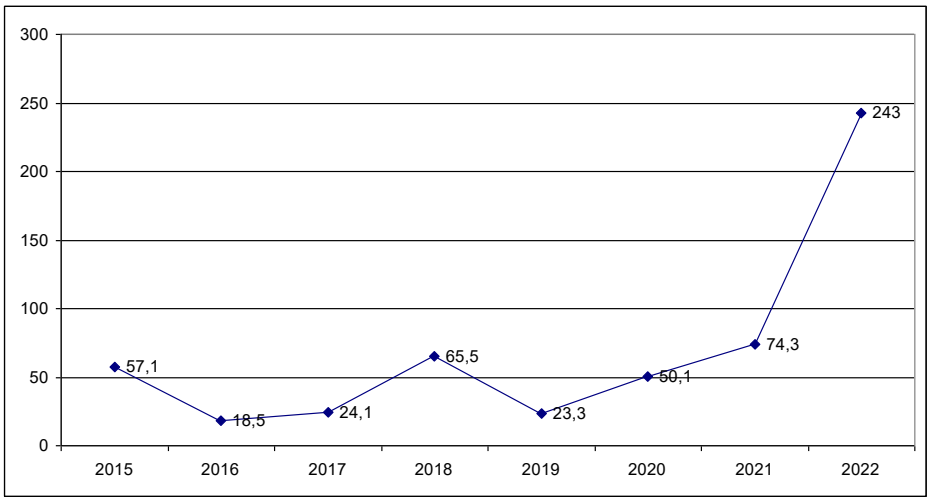

Рисунок 4 – Динамика вывоза капитала частным сектором за 2015–2022 гг.

Вместе с тем, сальдо финансовых операций частного сектора в 2022 г. составило $243 млрд ($74,3 млрд в 2021 г.), а рост чистого оттока за год обусловлен "наращиванием вложений резидентов в иностранные активы" (Рис. 4).

Одно из направлений вывода денежных средств за рубеж порождается необходимостью осуществления расчётов за нелегальный или полулегальный импорт товаров. Следует пояснить, что все грузы, пересекающие границу России, подвергаются тщательному таможенному контролю. Центральным элементом этой процедуры является определение стоимости товара, указанной в документах, предоставляемых импортёром. Эта стоимость не просто номинальная цифра, а ключевой фактор для расчёта таможенных пошлин и налогов, которые предстоит оплатить. Однако, чтобы минимизировать эти расходы многие импортёры прибегают к искусственному занижению стоимости товаров, что является нарушением законодательства. Зачастую именно таким путём в Россию попадают различные товары народного потребления из Китая или скоропортящиеся товары из стран ближнего зарубежья. В случае контрабанды всю стоимость приобретаемого товара необходимо переводить с использованием схем незаконного вывода денег, поскольку весь товар изначально попал на территорию России незаконно.

В таком случае импортёры сначала осуществляют продажу наличной выручки, после этого происходит вывод денежных средств безналичным путём различными способами, в том числе посредством криптовалют как наиболее удобным инструментом при нелегальных расчётах.

Операции по выводу денежных средств за границу носят более завуалированный характер и по большому счёту основаны на проведении фиктивных (притворных) сделок, в первую очередь, по оказанию услуг или приобретению товара, в которых часто задействованы операции по купле/продаже ценных бумаг.

Важную роль в подобных операциях играют компании, зарегистрированные на территории стран Содружества независимых государств, входящих в Таможенный союз. При осуществлении поставок товаров в пределах Таможенного союза, таможенного контроля на границе не осуществляется, т.е. отсутствует возможность проследить через таможенную базу, осуществлялась эта поставка или нет, при том, что документальное сопровождение сделки осуществляется в соответствии со всеми нормами. В счёт оплаты подобных фиктивных поставок, которые в действительности не осуществляются, производятся взаиморасчёты с использованием ценных бумаг, которые в дальнейшем могут быть реализованы на фондовом рынке в другой юрисдикции, таким образом, из сделки исключается денежная составляющая.

Анализ национальной оценки рисков в деятельности кредитных организаций по ПОД/ФТ выявил, что, несмотря на высокую эффективность принимаемых Банком России мер с целью минимизации рисков вовлечения кредитных организаций в процесс ОД/ФТ, развитие современных цифровых технологий во всех сферах банковского дела приводит к возникновению новых уязвимых мест в банковской системе как фундаментальной составляющей российской системы ПОД/ФТ.

Принципиальной особенностью появляющихся уязвимостей становится низкая эффективность существующих традиционных методов финансового мониторинга, вследствие комбинирования использования злоумышленниками уже выявленных существующих уязвимостей с непрерывно развивающимися цифровыми технологиями и новыми способами предоставления банковских услуг.

В современном мире, где взаимодействие всё чаще происходит онлайн, традиционные методы проверки личности клиентов, основанные на личном контакте, становятся всё более сложными и неэффективными. Возникает потребность в безопасных и автономных системах цифровой идентификации, способных обеспечить безопасное и эффективное взаимодействие без физического присутствия. Цифровая идентификация, как и любая другая форма проверки, несёт в себе определённые риски, однако, при использовании надёжных систем и строгих мер безопасности, эти риски могут быть сведены к минимуму.

Цифровая идентификация личности – это процесс, который позволяет подтвердить личность в цифровом мире. Он включает в себя два ключевых элемента и третий необязательный:

1) проверка личности и её регистрации (обязательно). Проверка личности предполагает:

- сбор идентификационных данных с помощью онлайн форм или сканирования документов (имя, фамилия, дата рождения, место рождения, пол, адрес, номер телефона, электронная почта и т.п.);

- верификация данных, т.е. проверка достоверности предоставленной информации путём сопоставления её с официальными базами данных (например, базами данных государственных органов);

- создание уникального профиля клиента в системе, содержащего проверенные данные.

В зависимости от уровня технологического развития, серьёзности потенциальных угроз и масштабов коммерческого внедрения системы цифровой идентификации могут предполагать включение следующих элементов:

- биофизических данных личности, которые являются статичными на протяжении всей жизни человека. К ним, например, относятся:

а) отпечатки пальцев: узор папиллярных линий на кончиках пальцев является уникальным для каждого человека;

б) радужная оболочка (цвет, структура, расположение кровеносных сосудов). Распознавание радужной оболочки в аэропортах, банках и иных учреждениях, где требуется высокая степень безопасности;

в) голосовые отпечатки (уникальный тембр, тональность голоса, характерные нюансы произношения);

г) распознавание лица по его геометрическим особенностям: расстояние между глазами, форма носа, контур губ, сравниваются с базой данных;

- биомеханических данных, в частности механика нажатия клавиш, поскольку стиль набора текста, скорость, сила и длительность нажатия, паузы между нажатиями являются уникальными для каждого человека;

- поведенческих данных, которые определяются особенностями взаимодействия человека с окружающим миром: пути передвижения человека, траектории движения глаз, способ взаимодействия человека с различными устройствами, такими как, например, смартфон, совокупность данных о местоположении человека, стиль написания писем, используемая лексика и т.п. являются уникальными для каждого человека.

2) аутентификация и контроль жизненного цикла удостоверений (обязательно), что предполагает подтверждение личности клиента при каждом доступе к системе или совершении транзакции. Аутентификация личности может осуществляться с помощью:

- пин-кода или пароля: ввод уникального пароля или пин-кода, известного только клиенту;

- одноразового пароля (OTP): получение кода подтверждения на телефон или электронную почту;

- биометрических данных: сканирование отпечатка пальца, распознавание лица или сканирование радужной оболочки глаза;

- программного обеспечения, которым управляет абонент или криптографические методы защиты.

Чем больше параметров задействовано в процесс аутентификации, тем более надёжной является данная система.

3) механизмы переносимости и взаимодействия (необязательно).

Данный элемент позволяет передавать информацию о подтверждённой личности между различными организациями и государственными учреждениями без повторной идентификации. Для реализации переносимости необходимы совместимые системы и процессы цифровой идентификации.

В современной России уже функционирует платформа для удалённой идентификации. Она основана на единой системе идентификации и аутентификации (далее – ЕСИА) и единой биометрической системе, которая позволяет физическим лицам получать услуги дистанционно, минуя необходимость личного посещения офиса соответствующей организации. Процесс удалённой идентификации осуществляется уполномоченными банками, которые обладают правом регистрировать пользователей в ЕСИА и единой биометрической системе. В их число входят финансово-кредитные учреждения, являющиеся участниками системы страхования вкладов и не находящиеся под мерами по предупреждению банкротства. Чтобы воспользоваться преимуществами удалённой идентификации, физическому лицу необходимо пройти первичную регистрацию биометрических данных в одном из уполномоченных банков. Данный процесс включает следующие этапы:

1) личное посещение банка с документами, удостоверяющими личность (паспорт), для подтверждения своей идентичности;

2) регистрация в ЕСИА;
3) сбор биометрических данных;
4) передача данных в единую биометрическую систему.

После завершения этой процедуры гражданин РФ может использовать удалённую идентификацию для получения различных банковских услуг, таких как открытие счёта, оформление кредита, инвестирование и многое другое.

Система удалённой идентификации позволяет банкам привлекать новых клиентов, которым удобно пользоваться дистанционными услугами. Однако помимо преимуществ система удалённой идентификации также несёт в себе ряд вызовов для банков:

а) необходимость адаптации бизнес-модели посредством пересмотра своих бизнес-процессов и технологической инфраструктуры с целью обеспечения бесперебойной работы удалённой идентификации;

б) усиление конкуренции, обусловленной упрощением процедуры открытия счетов, возможностью смены банков или открытия счетов в нескольких банках.

В то же время, цифровая идентификация открывает новые возможности для сотрудничества. Банки смогут обмениваться данными о клиентах с другими участниками финансового рынка, такими как страховые компании, инвестиционные фонды и платёжные системы. По мере развития цифровой идентификации и наполнения ЕСИА, а также единой биометрической системы, спектр её применения будет расширяться. К сбору биометрических данных смогут подключаться некредитные финансовые организации, а также государственные учреждения, такие как МФЦ.

Внедрение цифровой идентификации сопряжено с определёнными рисками, которые необходимо учитывать. Одним из самых актуальных на данный момент рисков в национальной системе ПОД/ФТ (как впрочем и в подавляющем большинстве систем ПОД/ФТ) является использование номинальных юридических лиц – резидентов ("фирм-однодневок"). В текущий момент, банки осуществляют обмен информацией со своими клиентами посредством использования систем дистанционного банковского обслуживания, где в качестве идентификатора используются различной степени защищённости физические носители ключевой информации. Интеграция сервисов ЕСИА в системы дистанционного банковского обслуживания кредитных организаций позволит использовать собранную в ЕБС информацию в качестве подтверждения подлинности личности клиента, представителя клиента, выгодоприобретателя или бенефициарного владельца. Существующие схемы обналичивания денежных средств с использованием подставных лиц перестанут быть актуальными ввиду невозможности использования третьими лицами персонифицированных финансовых инструментов без присутствия их владельца, не вызывая подозрения у кредитной организации.

Таким образом, цифровая идентификация с использованием биометрии несёт в себе огромный потенциал и де-факто может в будущем выступить в качестве системы идентификации общего назначения, что впоследствии позволит гражданам получать государственные услуги, совершать все виды банковских операций, заключать договоры и совершать другие юридически значимые действия онлайн. Внедрение цифровой идентификации, являющейся ключевым фактором в борьбе с ОД/ФТ и распространением оружия массового уничтожения, обретает особую актуальность в контексте современных угроз, и именно кредитные организации, на наш взгляд, должны сыграть в реализации этого процесса ведущую роль.

В силу ужесточения требований российского законодательства в сфере ПОД/ФТ/ФРОМУ, а также подходов регулятора при применении мер воздействия в случае их исполнения ненадлежащим образом, кредитные организации вынуждены прилагать всё большие усилия для минимизации своих рисков в этой области. Нарушение требований противолегализационного законодательства ведёт к применению по отношению к банкам таких мер надзорного реагирования как штраф, приостановление деятельности, а при установлении фактов неоднократного нарушения требования Федерального закона № 115-ФЗ в течение одного года банк и вовсе может лишиться своей лицензии на осуществление банковских операций.

В свете этих угроз банки оказываются перед необходимостью тратить всё большую часть своих ресурсов на выявления актуальных угроз в используемых стандартизированных бизнес-процессах.

Проведённый анализ национальной оценки рисков отмывания доходов и финансирования терроризма представляет для кредитных организаций возможность принимать необходимые управленческие решения в отношении возникающих угроз, опера-

тивно выявлять уязвимые места с целью их минимизации, и в целом позволяет повысить эффективность организованной системы финансового мониторинга в банке.

После ужесточения ЦБ РФ подходов к оценке степени участия банков в осуществлении сомнительных операций и организации комплексного методического сопровождения финансового мониторинга в крупных банках, удалось снизить риски вовлечения банков в проведение сомнительных операций. Согласно данным анализа, в последние годы наблюдается положительная тенденция к снижению объёмов проведения сомнительных операций в Российской Федерации, при единовременной трансформации вновь организуемых схем проведения сомнительных операций.

В связи с вышеизложенным, в статье была рассмотрена и обоснована возможность внедрения в национальную систему ПОД/ФТ перспективных с точки зрения финансового мониторинга инструментов цифровой идентификации. Идентификация в цифровой среде нивелирует влияние субъективного фактора при аутентификации клиента. Внедрение систем многофакторной аутентификации, основанных на биометрических данных и надёжных алгоритмах шифрования, делает практически невозможным несанкционированный доступ к учётным записям. Это повышает уверенность в том, что человек, пытающийся получить доступ к своим средствам, действительно является тем, за кого себя выдаёт.

При использовании процедуры цифровой идентификации на основании биометрических данных клиента, кредитные организации, руководствуясь подходами с точки зрения должной осмотрительности, а также реализуя в своей деятельности принцип "знай своего клиента", смогут исключить факт использования подставных лиц для вовлечения финансового учреждения в процесс легализации ОД/ФТ, что позволит вывести финансовый мониторинг в банке на качественно новый уровень.

Список использованных источников

1. Koshelev K.A. Legislative Impediments to cripto assets in the Russian Federation // XXXIII International Plehanov Readings. – 2020. – С. 60-65.

2. Kazbaeva A.G., Ismasgulov K.E. Analysis of the efficiency of legislation oncountering the legalization (money-laundering) of proceeds from crime and financing of terrorism // Bulletin of Institute of legislation information of the Republic Kazahstan. – 2020. – № 3(70). – С. 181-188.

3. Жариков Ю.С. Проблемы уголовной ответственности за легализацию преступных доходов // Актуальные вопросы публично-правового регулирования экономических отношений. – М., 2020. – С. 92-97.

4. Гриненко А.В., Коляда А.В., Хорьяков С.Н. Противодействие легализации (отмыванию) доходов, полученных преступным путём: уголовно-правовые, уголовно-процессуальные и криминалистические аспекты: монография. – М., 2022. – 184 с.

5. Albekova M.G. Problems of anti-money laundering and countering the financing of terrorism // Актуальные научные исследования в современном мире. – 2021. – № 12-13(80). – С. 258-260.

6. Колбасин Е.А. Доходы, полученные преступным путём, как предмет легализации // Традиции и новации в системе современного российского права: материалы Международного конгресса молодых учёных. – М., 2024. – С. 466-468.

7. Власов В.А., Шаповалов С.А. Противодействие легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма: вопросы финансового контроля и правоприменительной практики // Аграрное и земельное право. – 2021. – № 12(204). – С. 69-71.

8. Ivegesh O.A. Legalisation of parallel import in the Russian Faderation // Works on Intellectual property. – 2023. – № 2. – P. 53-62.

9. Радюк Д.И. Петрухина А.В. Кунцевич В.П. Легализация незаконных доходов через нетрадиционные финансовые институты // Economics. – 2020. – № 4(47). – С. 53-56.

10. Галали Р.Д.А. Риски вовлечения банков в легализацию преступных доходов и финансирование терроризма: подходы к анализу и оценке // Финансовые исследования. – 2020. – № 2(67). – С. 86-97.

11. Евдокимова Ю.В., Шинкарева О.В., Евдокимова А.А. Анализ рисков легализации незаконных доходов в Российской Федерации // Вестник Екатерининского института. – 2023. – № 2(62). – С. 1621.

12. Страхов И.А. Осуществление контроля за соблюдением правил внутреннего контроля противодействия легализации доходов, полученных преступным путём, и финансированию терроризма // Вестник евразийской науки. – 2021. – Т. 13. – № 6. – С. 66-75.
13. Карпова Е.Н. Особенности организации внутреннего контроля в целях противодействия легализации преступных доходов в лизинговых компаниях // Научные исследования и разработки. Экономика фирмы. – 2019. – Т. 8. – № 3. – С. 67-74.
14. Meshkov A. Biometrics as a tool to combat money laundering and terrorist financing // Dictum-Factum: from research to policy-making. – 2020. – № 1. – С. 143-147.
15. Гарышинова А.Р. Роль банковской системы РФ по противодействию легализации доходов, полученных преступным путём // Актуальные проблемы современной экономики. – 2022. – № 7. – С. 48-54.
16. Крочак В.С. Становление системы противодействия легализации доходов, полученных преступным путём // Научный лидер. – 2022. – № 31(76). – С. 64-68.
17. Дудинский И.И. Разработка мер противодействия совершению финансовых операций в целях легализации доходов, полученных преступным путём // Интернаука. – 2022. – № 1-3(224). – С. 68-70.
18. Александров Н.Д. Международное сотрудничество Росфинмониторинга в сфере противодействия легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма // Инновации. Наука. Образование. – 2022. – № 50. – С. 1160-1164.
19. Васильченко А.А. К вопросу о совершенствовании противодействия легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма // Право и образование. – 2022. – № 3. – С. 66-74.
20. Штанько О.И. Совершенствование деятельности коммерческого банка по противодействию легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма // Российское общество и государство на современном этапе: сборник научных трудов. – Владимир, 2022. – С. 260-265.