Федеральное государственное образовательное бюджетное учреждение
высшего образования
«Финансовый университет при Правительстве Российской Федерации»

На правах рукописи

Казанцев Дмитрий Андреевич

ТРАНСФОРМАЦИЯ МЕХАНИЗМА МОНИТОРИНГА ПРОТИВОДЕЙСТВИЯ ЛЕГАЛИЗАЦИИ (ОТМЫВАНИЮ) ДОХОДОВ, ПОЛУЧЕННЫХ ПРЕСТУПНЫМ ПУТЕМ, И ФИНАНСИРОВАНИЮ ТЕРРОРИЗМА В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ЭКОНОМИКИ

5.2.3. Региональная и отраслевая экономика:
экономическая безопасность

ДИССЕРТАЦИЯ
на соискание ученой степени
кандидата экономических наук

Научный руководитель Капустина Надежда Валерьевна,
доктор экономических наук, профессор

Москва – 2024

Оглавление

Введение

Актуальность темы исследования. Цифровизация человеческой жизнедеятельности практически во всех ее аспектах становится одним из главных факторов экономического развития постиндустриального общества. Более того, в современных научных исследованиях цифровые преобразования (в том числе расширенное внедрение киберфизических систем, использование технологий искусственного интеллекта, робототехники, 3D-печати, биоинженерии) выделяются в качестве базиса новой четвертой промышленной революции [12; 262]. Внедрение данных технологий позволит, в первую очередь, повысить производительность труда каждого человека в отдельности и экономики в целом. Человеку в эпоху Интернета и ЭВМ уже не надо затрачивать значительные усилия на поиск информации, ее механический анализ (например, для обнаружения нужных фраз и терминов), проведение математических расчетов. Во многом человек уже привык полагаться на вычислительные устройства. Четвертая промышленная революция является продолжением вышеуказанной тенденции и может в перспективе позволить человеку отказаться от ряда более комплексных, но рутинных в исполнении действий (в том числе, написания шаблонных ответов на запросы, вынесения решений по стандартным вопросам, управления транспортным средствам и многим другим), а вычислительным устройствам в ряде областей встать в один ряд с ним.

Несомненно, как и все нововведения, внедрение цифровых технологий в человеческую жизнедеятельность обладает положительными и отрицательными сторонами. Среди первых можно назвать снижение нагрузки на ряд правоприменительных органов в результате внедрения технологий искусственного интеллекта, уменьшение аварийности на дорогах в результате использования беспилотных транспортных средств, сокращение стоимости производства в результате применения технологий 3D-печати в промышленном масштабе, повышение качества оказываемых услуг благодаря анализу значительных объемов данных с применением технологий Big Data и так далее.

Однако, отмечаем, что не менее внушителен и список негативных сторон цифровизации экономики: риск роста безработицы среди наименее социально защищенных слоев общества в результате вытеснения киберфизическими системами работников, занимающихся трудом низкой и средней квалификации, риск расширения масштабов утечек персональных данных, влекущий за собой рост числа экономических преступлений, повышение критичности кибернетических атак в результате повсеместного внедрения цифровых устройств, снижение уровня конкуренции (при этом, как внутригосударственного, так и международного) в результате вытеснения более продвинутыми в вопросе управления «большими данными» игроками менее развитых конкурентов с рынка, а также снижение возможностей государственного контроля в результате расширения горизонтальных связей между субъектами социально-экономических отношений и использования технологий, позволяющих скрыть транзакционные цепочки передачи денежных средств (в том числе, технологий Blockchain и искусственного интеллекта). Именно последний аспект и оказывает наиболее значительное влияние на эффективность функционирования механизма мониторинга противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (далее – ПОД/ФТ).

Механизм мониторинга ПОД/ФТ является важной частью национальной системы обеспечения экономической безопасности государства. В соответствии со Стратегией экономической безопасности Российской Федерации на период до 2030 года с эффективностью противодействия легализации преступных доходов непосредственно связано устойчивое развитие национальной финансовой системы [43]. Деятельность механизма мониторинга ПОД/ФТ оказывает существенное влияние на минимизацию уровня экономической преступности в стране и способствует снижению террористической активности [54]. От функционирования механизма мониторинга ПОД/ФТ зависит деловая активность в государстве, инвестиционная привлекательность экономики страны, эффективность расходования бюджетных средств и устойчивость кредитно-финансовой сферы.

Работоспособность механизма мониторинга ПОД/ФТ несомненно зависит от многих социально-экономических и правовых факторов, среди которых: правовая культура общества, в целом, и менеджеров организаций, осуществляющих операции с денежными средствами и иным имуществом, в частности, уровень преступности в государстве и масштабы «теневой экономики», развитость законодательства и правоприменительной практики в сфере ПОД/ФТ, а также уровень экономического развития страны. Однако, не меньшее влияние на функционирование механизма мониторинга ПОД/ФТ оказывает наличие устойчивых схем легализации доходов, полученных преступным путем, и финансирования терроризма, позволяющих сокрыть факт их совершения, и обеспечивающих деперсонифицированность их участников (для чего, помимо прочего, применяются и технологии цифровой экономики), а также наличие у контрольно-надзорных и правоохранительных органов методов и технологий, позволяющих выявлять такие схемы и лиц, участвующих в них. В числе таких технологий можно назвать технологии искусственного интеллекта, блокчейн, Big Data, непосредственно связанные с цифровизацией экономики.

Стоит отметить, что все вышеперечисленные технологии обладают дуалистической природой с точки зрения ПОД/ФТ. С одной стороны, их можно применять в целях сокрытия цепочек отмывания денежных средств и финансирования терроризма. Так, по данным аналитического сервиса Chainalysis только за 2023 год от криптовалютных адресов, связанных с осуществлением незаконной деятельности, было получено 24,2 трлн долларов, что составило 0,34% от общей суммы криптовалютных транзакций в 2023 году (однако, аналитики предупреждают, что данная цифра может вырасти по мере получения дополнительной информации о связи тех или иных криптовалютных адресов с криминалом [274]).

С другой стороны, данные же технологии можно использовать и в целях выявления схем легализации доходов и финансирования терроризма. Так, для отслеживания операций с криптовалютой используются технологии искусственного интеллекта, а технология блокчейн нашла свое применение в

области обмена результатами идентификации клиентов [64]. Актуальность применения технологий цифровой экономики в механизме мониторинга ПОД/ФТ, обусловливается, в первую очередь, теми рисками в сфере ПОД/ФТ, которые создает эксплуатация данных же технологий в преступных целях.

Увеличивающаяся сложность выявления классическими аналитическими методами схем легализации денежных средств, полученных преступным путем, и финансирования терроризма, осуществляемых с использованием цифровых технологий, а также потенциал усиления аналитических возможностей субъектов первичного финансового мониторинга и органа государственного финансового мониторинга – Росфинмониторинга – в результате применения цифровых технологий обусловливают актуальность темы кандидатского исследования.

Степень разработанности темы исследования. Развитию механизма ПОД/ФТ (и, в том числе, механизма мониторинга ПОД/ФТ) в условиях цифровизации экономики уделяется значительное внимание, как в научной среде, так и на государственном уровне. Так, противодействие легализации преступных доходов, осуществляемой с использованием инфокоммуникационных технологий, фигурирует в числе задач государственной политики в рамках Стратегии национальной безопасности Российской Федерации [41] и Стратегии экономической безопасности Российской Федерации на период до 2030 года [43]. Особое внимание совершенствованию механизма ПОД/ФТ уделяется в Концепции развития национальной системы противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма [106].

Общая проблематика ПОД/ФТ в целом и механизма мониторинга ПОД/ФТ в частности рассматривалась в работах В.И. Авдийского, В.М. Безденежных, .Г. Братко, И.Е. Волуевича, В.И. Глотова, В.А. Дадалко, О.В. Зимина, В.А. Зубкова, А.Я. Капустина, Ю.В. Лафитской, А.Ф. Милюкова, Г.Ю. Негляда, С.К. Осипова, М.М. Прошунина, Н.Г. Синявского, В.И. Третьякова, А.М. Цирина, Ю.А. Чиханчина, Н.В. Юсупова и других.

Трансформация механизма мониторинга противодействия отмыванию доходов, полученных преступным путем, и финансированию терроризма

анализировалась в трудах И.М. Аничкина, А.Д. Грачева, В.Н. Едроновой, С.В. Ефимова, Ф.К. Иванова, Н.В. Капустиной, Г.О. Крылова, С.Б. Лапиной, И.А. Лебедева, И.Н. Лоскутова, О.П. Овчинникова, В.И. Прасолова, М.М. Прошунина, В.М. Селезнева, С.С. Фешиной, З.И. Хисамовой и других авторов.

Цель исследования – подготовка предложений по совершенствованию механизма мониторинга противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма на основе результатов исследования трансформации механизма мониторинга ПОД/ФТ, в том числе в условиях цифровизации экономики.

С учетом поставленной цели необходимо решить следующие **задачи** исследования:

– выработка теоретического подхода к определению сущности механизма мониторинга противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

– формулирование роли и места противодействия легализации доходов, полученных преступным путем, и финансирования терроризма в системе обеспечения экономической безопасности государства;

– анализ трансформации российского механизма мониторинга противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, в том числе в условиях цифровизации экономики;

– определение уровня влияния цифровизации экономики на эффективность функционирования механизма мониторинга противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

– разработка рекомендаций по совершенствованию механизма мониторинга противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма в условиях цифровизации экономики.

Объект исследования – процесс трансформации механизма мониторинга противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

Предмет исследования – механизм мониторинга противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма в условиях цифровизации экономики.

Область исследования соответствует п. 13.8. «Проблемы экономической безопасности, связанные с криминальной деятельностью, распространением теневой экономики и финансированием экстремистских организаций» и п. 13.12. «Разработка и применение методов, механизмов и инструментов повышения экономической безопасности» Паспорта научной специальности 5.2.3. Региональная и отраслевая экономика: экономическая безопасность (экономические науки).

Научная новизна исследования состоит в расширении экономико-теоретической базы механизма мониторинга ПОД/ФТ, а также в формировании рекомендаций по совершенствованию механизма мониторинга ПОД/ФТ в условиях цифровизации экономики.

Научная гипотеза исследования. Функционирование механизма мониторинга ПОД/ФТ в условиях цифровизации экономики требует выработки экономической интерпретации процессного взаимодействия его участников, а также разработки многоуровневой (наднациональный, национальный и микроуровень организации) модели функционирования механизма мониторинга ПОД/ФТ в условиях цифровизации экономики. С учетом развития экономических процессов и формирования взаимосвязанных между собой условий, определяющих необходимость совершенствования механизма мониторинга ПОД/ФТ, использование преимуществ технологий и иных нововведений цифровой экономики в целях повышения эффективности механизма мониторинга ПОД/ФТ, а также минимизация негативного воздействия на механизм мониторинга ПОД/ФТ, связанного с противоправным применением данных технологий и нововведений,

позволит наиболее эффективно обеспечивать экономическую безопасность государства.

Теоретическая значимость работы заключается в расширении научных знаний о сущности и направлениях развития механизма мониторинга противодействия отмыванию доходов, полученных преступным путем, и финансированию терроризма.

Практическая значимость работы состоит в возможности использования авторской модели модернизации механизма мониторинга противодействия отмыванию (легализации) доходов, полученных преступным путем, и финансированию терроризма в целях модернизации существующего механизма мониторинга ПОД/ФТ с учетом рисков и преимуществ цифровизации экономики.

Также в деятельности Росфинмониторинга, кредитных организаций и некредитных финансовых организациях могут использоваться сформированные признаки подозрительности операций с цифровыми валютами и цифровыми финансовыми активами.

Результаты исследования могут использоваться образовательными учреждениями в рамках учебного процесса при подготовке учебно-методических материалов и проведении занятий по дисциплине «Финансовые расследования и противодействие легализации незаконных доходов».

Методология и методы исследования. Методологическую основу исследования составили: научные труды российских и зарубежных ученых и специалистов в сфере ПОД/ФТ по вопросам генезиса и трансформации механизма мониторинга ПОД/ФТ, международные конвенции и директивы, разработки и результаты деятельности международных организаций, рекомендации Группы разработки финансовых мер по борьбе с отмыванием денег – Financial Action Task Force (FATF), российское законодательство и иные нормативные правовые акты в области ПОД/ФТ.

При проведении исследования применялись следующие методы: системно-исторического анализа, группировки и классификации, сопоставления и

сравнения, анализа и синтеза, моделирования, научного обобщения, индукции и дедукции.

Информационную базу исследования составили нормативные и информационно-аналитические материалы Федеральной службы по финансовому мониторингу (Росфинмониторинга) и Банка России, аналитической компании Chainalysis, публикации в периодической печати, посвященные вопросам экономической безопасности и тематике ПОД/ФТ, монографии, материалы научно-практических конференций и семинаров, информационно-аналитические ресурсы сети Интернет.

Положения, выносимые на защиту:

а) Сформулирован авторский подход к определению механизма мониторинга ПОД/ФТ, как составной части механизма ПОД/ФТ, в рамках которой на основании анализа информации о проводимых финансовых операциях и заключаемых сделках осуществляется выявление операций, имеющих признаки легализация (отмывания) доходов, полученных преступным путем, или финансирования терроризма, результаты чего передаются в правоохранительные и иные государственные органы в целях принятия ими мер, направленных на противодействие легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (С. 34–42). Представленный подход потребовал выработки авторского определения отмывания доходов, полученных преступным путем, в контексте его экономической сущности, как комбинации результирующего и операционного подходов (С. 22–24), на основании составленной авторской классификации подходов к определению понятия отмывания преступных доходов в соответствии с их ведущей компонентой, в отличие от представленных в научных источниках научно-отраслевых подходов к классификации (С. 20–22).

б) Научно обоснована многоуровневая (наднациональный, национальный (включая региональный) и микроуровень) модель функционирования механизма мониторинга ПОД/ФТ в условиях цифровизации экономики в контексте информационного взаимодействия участников механизма мониторинга ПОД/ФТ (С. 46–53), что позволило исследовать механизм мониторинга ПОД/ФТ с позиции

его динамичных изменений (трансформации) и выделить организационно-технологические факторы трансформации механизма мониторинга ПОД/ФТ в условиях цифровизации экономики (С. 53–57).

в) Установлена взаимосвязь цифровизации экономики и трансформации механизма мониторинга ПОД/ФТ, а также корреляционным методом доказана зависимость между цифровизацией механизма мониторинга ПОД/ФТ и снижением финансового потока, связанного с ОД/ФТ, что с учетом систематизации внедряемых в механизм мониторинга ПОД/ФТ технологий и иных нововведений цифровой экономики по группам организационно-технологических факторов трансформации механизма мониторинга ПОД/ФТ в условиях цифровизации экономики будет способствовать выработке превентивных мер по упреждающему развитию механизма мониторинга ПОД/ФТ в условиях постоянного возникновения новых факторов развития экономических процессов в условиях цифровизации экономики и их воздействия на механизм мониторинга ПОД/ФТ (С. 127–144; С. 186–193).

г) Обоснован комплексный подход к развитию механизма мониторинга противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма в условиях динамичного развития цифровой экономики, базирующийся на частичном слиянии микроуровня и национального уровня механизма мониторинга ПОД/ФТ за счет разработки и внедрения в информационные системы субъектов противодействия отмыванию преступных доходов и финансированию терроризма программных модулей единой автоматизированной системой противодействия отмыванию доходов, полученных преступным путем, и финансированию терроризма. Данный подход позволит повысить эффективность процедур мониторинга ПОД/ФТ, а также снизить аналитическую и надзорную нагрузку на субъектов микроуровня механизма мониторинга ПОД/ФТ, за счет осуществления части процедур мониторинга ПОД/ФТ (в том числе выявления операций, подлежащих обязательному контролю, направления ответов на запросы Росфинмониторинга и ряда других) единой

автоматизированной системой противодействия отмыванию доходов, полученных преступным путем, и финансированию терроризма (С. 205–231).

д) Предложены рекомендации по совершенствованию механизма мониторинга ПОД/ФТ в условиях цифровизации экономики, обоснованные разработанной в работе классификацией рисков эффективного функционирования механизма мониторинга ПОД/ФТ и преимуществ цифровизации экономики в контексте повышения эффективности механизма мониторинга ПОД/ФТ (С. 177–185), направленные на дополнение перечней признаков подозрительности финансовых операций с цифровыми валютами и цифровыми финансовыми активами, которые могут быть применены в целях развития единой автоматизированной системы противодействия отмыванию доходов, полученных преступным путем, и финансированию терроризма, а также могут быть внесены в существующие нормативно-правовые акты в сфере противодействия отмыванию доходов, полученных преступным путем, и финансированию терроризма (С. 225–228; С. 313–314), что позволит минимизировать риски ОД/ФТ, связанные с использованием цифровых валют и цифровых финансовых активов в противоправных целях.

Степень достоверности, апробация и внедрение результатов исследования. Достоверность обеспечивается использованием методов научного познания в исследовании, достоверных статистических данных, научных трудов отечественных и зарубежных ученых, полнотой анализа и практической проверкой результатов исследования.

Основные положения и итоги исследования представлены на следующих научно-практических конференциях: на XVIII Международной научно-практической конференции «Корпоративная социальная ответственность и этика бизнеса» (Москва, Финансовый университет, 19-20 мая 2022 г.); на III Всероссийской научно-практической конференции с международным участием «Право, экономика и управление: теория и практика» (г. Чебоксары, Чувашский государственный институт культуры и искусств, 23 июня 2022 г.); на III Международной научно-практической конференции «Экономика. Наука. Инноватика» (г. Донецк, Донецкий Национальный Технический Университет,

23 марта 2023 г.); на LX Международной научно-практической конференции «Научный форум: Инновационная наука» (Москва, ООО «МЦНО», 29 мая 2023 г.); на IV Международной научно-практической конференции «Современные экономические проблемы развития и эксплуатации транспортной инфраструктуры» (Москва, Российский университет транспорта, 21-22 ноября 2023 г.).

Результаты исследования нашли отражение в практической деятельности ООО «ГК «Иннотех». В процессе диссертационного исследования Казанцевым Д.А. составлена классификация рисков и преимуществ цифровизации экономики в контексте противодействия отмыванию преступных доходов и финансированию терроризма. Применение авторского подхода на практике позволяет повысить качество аналитической работы, связанной с оценкой новых вызовов и угроз в сфере отмывания доходов, полученных преступным путем, финансирования терроризма, с последующей выработкой противодействия им. Кроме того, сформированные автором признаки подозрительности операций с цифровыми валютами применяются в ходе оценки с использованием программного обеспечения «Инчейн» финансовых операций, осуществляемых посредством цифровых валют. Использование предложений автора в продукте «Инчейн» позволило повысить эффективность работы, направленной на выявление операций, связанных с отмыванием преступных доходов и финансированием терроризма, совершаемых с использованием цифровых валют, улучшить аналитическую работу по выявлению и минимизации рисков легализации доходов, полученных преступным путем, и финансирования терроризма, связанных с использованием злоумышленниками цифровых технологий, а также способствовало принятию мер по своевременному выявлению и устранению причин и условий, приводящих к совершению указанных правонарушений.

Признаки подозрительности операций с цифровыми валютами применяются в деятельности АНО Экспертно-правовой центр «Финансовые расследования и судебные экспертизы» в рамках осуществления процедур внутреннего контроля, что позволило повысить эффективность работы по выявлению подозрительных

операций, а также способствовало принятию мер по своевременному обнаружению и устранению причин и условий, которые могли использоваться злоумышленниками в целях осуществления противозаконных финансовых операций.

Материалы исследования использовались Департаментом экономической безопасности и управления рисками Факультета экономики и бизнеса Финансового университета в преподавании учебной дисциплины «Организация финансовой разведки на основе риск-ориентированного подхода» по образовательной программе бакалавриата 38.03.01 «Экономика», профиль «Финансовая разведка».

Апробация и внедрение результатов исследования подтверждены соответствующими документами.

Публикации. Основные положения и результаты исследования отражены в 9 работах общим объемом 6,04 п.л. (авторский объем 5,27 п.л.), в том числе 6 работ общим объемом 5,12 п.л. (авторский объем 4,45 п.л.) опубликованы в рецензируемых научных изданиях, определенных ВАК при Минобрнауки России.

Структура и объем диссертации обусловлены целью, задачами и логикой исследования. Диссертация состоит из введения, трех глав, заключения, списка литературы, включающего 306 наименований, и шести приложений. Текст диссертации изложен на 314 страницах, содержит 8 таблиц и 72 рисунка.

Глава 1

Сущность механизма мониторинга противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма

1.1 Анализ генезиса легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма как объекта воздействия механизма мониторинга противодействия отмыванию доходов, полученных преступным путем, и финансированию терроризма[1]

«Природа отмывания преступных доходов кроется в самой сущности преступной деятельности, а точнее той ее части, которая предполагает получение прибыли в результате совершения уголовно наказуемых деяний. В данном типе преступлений (зачастую предполагающими то или иное планирование и подготовку) конечной целью является добыча денежных средств или иного имущества, порой независимо от обнаружения факта совершения преступления и выявления лиц, причастных к криминальной деятельности. Соответственно, центральным аспектом такой преступной деятельности является возможность использования полученного в результате преступления или производного от него имущества. Для достижения данной цели, сокрытия самого факта совершения преступления, сокрытия лиц, причастных к нему, или (в случае совершения преступления в той или иной форме соучастия, а также когда меры уголовной ответственности не превышают допустимые для преступника пределы и есть возможность воспользоваться добытым преступным путем после отбывания наказания) сокрытия местонахождения преступных доходов применяются разнообразные схемы легализации (отмывания) преступных доходов» [230, с. 56].

Понятие «отмывание доходов» (далее – ОД) получило широкое распространение в США в 1980-х годах и первоначально не имело нормативного

1) Текст подготовлен на основе публикаций автора [227; 236].

закрепления, а использовалось в судебных процессах. Одна из первых трактовок термина была дана в 1984 году Президентской комиссией США по организованной преступности, согласно которой «отмывание денег – процесс, позволяющий скрыть существование, незаконное происхождение или незаконное использование денег, путем маскировки доходов так, чтобы они казались законными» (цитируется по [3, с. 13]).

Первым международным актом в сфере противодействия отмыванию доходов, полученных преступным путем, является Конвенция Организации Объединенных Наций о борьбе против незаконного оборота наркотических средств и психотропных веществ (далее – соответственно ООН, Венская конвенция) о борьбе против незаконного оборота наркотических средств и психотропных веществ, принятая в 1988 г., в которой хоть и отсутствует сам термин «отмывание доходов», однако содержится перечень действий, которые в совокупности соответствуют современному пониманию легализации преступных доходов [3]. Также в 1988 г. Базельский комитет по банковскому надзору принимает Декларацию о предотвращении преступного использования банковской системы в целях отмывания денежных средств, в которой уже содержится термин «отмывание денег», описываемое как «деятельность преступников и их пособников по использованию финансовой системы для:

– осуществления платежей и переводов денежных средств, полученных преступным путем, с одного счета на другой;

– сокрытия источника происхождения и бенефициарного владельца денежных средств;

– хранения банкнот в банковских сейфах» (цитируется по [6, с. 18]).

В 2000 г. Генеральная Ассамблея ООН приняла Конвенцию против транснациональной организованной преступности (далее – Палермская конвенция) [10]. В данной конвенции употребляется термин «отмывание доходов», полное определение которого приводится в ст.6 Палермской конвенции, согласно которому под отмыванием доходов понимается:

– «конверсия или перевод имущества, если известно, что такое имущество представляет собой доходы от преступлений, в целях сокрытия или утаивания преступного источника этого имущества или оказания помощи любому лицу, участвующему в совершении основного правонарушения, с тем чтобы оно могло уклониться от ответственности за свои деяния;

– сокрытие или утаивание подлинного характера имущества, источника его возникновения, местонахождения, способа распоряжения, перемещения, прав на имущество или его принадлежность, если известно, что такое имущество представляет собой доходы от преступлений;

– приобретение, владение или использование имущества, если в момент его получения известно, что такое имущество представляет собой доходы от преступлений;

– участие в преступлении, причастность к нему или вступление в сговор с целью совершения любого из преступлений, признанных таковыми в соответствии с указанной статьей, покушения на его совершение, а также пособничество, подстрекательство, содействие или дача советов при его совершении» [10, с. 20].

«В российском правовом пространстве термин «отмывание доходов» закрепляется в сочетании с синонимичным, но более формальным понятием «легализация доходов». Так, в Федеральном законе № 115-ФЗ от 07.08.2001 «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (далее – Закон № 115-ФЗ) под легализацией (отмыванием) доходов понимается придание правомерного вида владению, пользованию или распоряжению денежными средствами или иным имуществом, полученными в результате совершения преступления [34]. Аналогичная трактовка содержится в ст. 174, 174.1 Уголовного кодекса Российской Федерации, за тем исключением, что в них раскрывается суть действий по приданию правомерного вида владению, пользованию или распоряжению денежными средствами или иным имуществом, которые происходят в форме финансовых операций или иных сделок [37]. В российском законодательстве термин «отмывание доходов» является инкорпорированным из международных

актов, тогда как понятие «легализация» представляет собой российское нововведение, включенное в текст нормативных актов с целью придать более формализованный вид терминологии. Однако, стоит отметить, что оба понятия подвергаются критике в научной среде. Так, Прошунин М.М. отмечает бытовой характер термина «отмывание доходов», а Тангаров В.С. и вовсе относит его к жаргонизмам [256; 267]. Анализируя понятие «легализация преступных доходов», ряд авторов также приходят к выводу о его неполной релевантности. В частности, Алешин К.Н. считает более целесообразным использование термина «отмывание доходов», так как в процессе «отмывания» имуществу придается лишь правомерный вид, однако ни само оно, ни действия, связанные с данным имуществом, правомерными от этого не становятся» [230, с. 56–57].

В научных источниках определение понятия отмывания (легализации) преступных доходов содержится преимущественно в работах уголовно-правового характера. «В.А. Никулин рассматривает легализацию преступных доходов, как окончательное придание законной формы материальным ценностям, полученным преступным путем [267]. Тогда как Ю.В. Коротков определяет отмывание (легализацию) незаконных доходов, как умышленное сокрытие происхождения доходов посредством искажения информации об их истинном характере [267]. Характерно различие между вышеприведенными определениями. В первом легализация доходов рассматривается как конечный результат некого процесса, в результате которого преступные доходы обретают правомерный вид. Во второй трактовке термин легализации (отмывания) преступных доходов приобретает характер самого этого процесса с учетом наличия в данном процессе юридической категории умысла. Аналогичное второй трактовке определение дает и В.М. Шумилов, который под отмыванием преступных доходов понимает процесс преобразования нелегально полученных денег в легальные [13]. Кроме результирующей и процессной интерпретаций понятия отмывания (легализации) доходов, полученных преступным путем, в научных работах также можно выделить операционную. Так, немецкий ученый Х.Х. Кернер дает следующее определение термину отмывания преступных доходов: операции, осуществляемые

с целью на первой стадии утаить или скрыть наличие, происхождение или целевое назначение вещественных ценностей, проистекающих из преступления, с тем, чтобы на второй стадии приступить к извлечению из них регулярных доходов» [7; 230, с. 57].

«Более комплексное определение понятия отмывания незаконных доходов содержится у М.М. Прошунина [256]. Прошунин выделяет четыре аспекта отмывания доходов, среди которых материальный, процедурный, экономический и правовой. Под материальным аспектом Прошунин понимает последовательность действий по размещению незаконно полученного имущества в финансовой системе, проведение операций с данным имуществом по его расслоению (перемешиванию) и интегрирование незаконных доходов в национальную экономику. Под процедурным аспектом Прошунин подразумевает процесс маскировки изначального происхождения и истинных владельцев имущества, полученного преступным путем. В рамках правовой составляющей отмывания доходов автор отмечает придание правомерного вида владению, пользованию и распоряжению имуществом. В экономическом смысле легализация преступных доходов заключается, согласно мнению Прошунина, в переходе денежных средств или иного имущества, полученного преступным путем из теневой экономики в легальную экономику» [230, с. 57].

С учетом вышеприведенного составлена классификация подходов к определению понятия отмывания преступных доходов, представленная на рисунке 1.

Классификации подходов к определению понятия отмывания преступных доходов разнятся в зависимости от подхода того или иного автора. Концепция четырех аспектов отмывания доходов, изложенная М.М. Прошуниным, приведена выше. А.Ф. Милюков выделяет три подхода к легализации преступных доходов: экономический, уголовно-правовой и гражданско-правовой. В рамках экономического подхода отмывание доходов, полученных преступным путем, представляет собой «процесс предъявления спроса со стороны криминальных доходов на возможность потребления и сбережения в легальной экономике»

[247, с. 86]. С позиции уголовно-правового подхода, согласно А.Ф. Милюкову, отмывание преступных доходов представляет собой придание преступно полученных доходам легального статуса. Тогда как с позиции гражданско-правового подхода отмывание доходов «рассматривается как несколько финансовых операций, совершаемых в определенной последовательности, и по отдельности являющихся абсолютно законными и не представляющих никакой общественной опасности» [247, с. 87]. При этом, стоит отметить, что классификацию подходов А.Ф. Милюкова также можно отнести к комплексному подходу, с учетом разделения правового аспекта ОД на два подхода: уголовно-правовой и гражданско-правовой, а также исключением материального и процедурного аспектов.

Источник: составлено автором.

Рисунок 1 – Классификация подходов к определению понятия отмывания преступных доходов

Вышеприведенные концепции (являющиеся также, по сути, авторскими формулировками) тяготеют к научно-отраслевому принципу дифференциации подходов. Научно-отраслевое разделение трактовок понятия отмывания доходов актуально, как способ разграничения объекта исследования между экономическими и юридическими науками, а также как возможность более

всестороннего изучения явления отмывания (легализации) преступных доходов путем его рассмотрения с позиций разных научных отраслей.

Сформулированная в данном исследовании классификация подходов сводится к выделению центрального компонента того или иного подхода к ОД. Так, результирующие подходы преимущественно свойственны уголовно-правовым научным исследованиям и акцентируют внимание на придании правомерного вида преступно полученным денежным средствам и иным доходам, как наиболее важной черте отмывания доходов. Процессные и операционные подходы различаются условно путем восприятия процесса ОД в качестве непрерывного (в случае процессного подхода) или набора дискретных операций (в случае операционного подхода), однако, основное внимание в таких определениях уделяется самой деятельной составляющей процесса отмывания доходов, полученных преступным путем.

Отдельно выделяется комплексный подход к определению ОД. Именно комплексный подход позволяет наиболее разносторонне подойти к процессу анализа отмывания доходов, как явления, и соответственно, к противодействию данному явлению. При этом, комплексный подход необязательно должен быть связан с мультиотраслевым изучением явления. Комплексный подход применительно к сформулированной в данном исследовании классификации позволяет остаться в рамках изучения понятия отмывания доходов исключительно в рамках экономических наук.

В соответствии с позицией, представленной в исследовании, экономическая сущность отмывания (легализации) преступных доходов «заключается в комбинации результирующей составляющей отмывания доходов (перевод доходов, полученных преступным путем, из теневого сектора экономики в легальный, создание условий для использования преступных доходов в рамках экономической системы) и процедурной составляющей (осуществление финансовых операций, гражданско-правовых сделок и иных действий, направленных на размещение полученных преступных доходов в финансовой системе, их расслоение, а затем интеграцию)» [230, с. 57–58].

Таким образом, вышеприведенное определение, не тяготея к дисциплинарной сегрегации, также относится к комплексному подходу в рамках сформированной в данной работе классификации подходов к определению понятия отмывания преступных доходов, что представлено на рисунке 2.

Источник: составлено автором.

Рисунок 2 – Классификация подходов к определению понятия отмывания преступных доходов, включая авторскую трактовку

В связи с этим, сложно согласиться с классификацией подходов, предложенной Прошуниным М.М., согласно которой экономический аспект ОД ограничивается лишь диффузией преступных капиталов из теневой экономики в легальную, без учета форм реализации данного процесса, выраженных им в процедурном и материальном аспектах. Рассмотрение ОД в рамках данного исследования в качестве комплексного явления, сочетающего результирующую и операционную составляющие (с учетом того, что «экономическая сущность отмывания доходов, полученных преступным путем, сводится к правовому результату – приданию правомерного вида данным преступным доходам» [230, с. 58]) важно еще потому, что позволяет также комплексно подойти к противодействию ОД и, соответственно, механизму противодействия отмыванию доходов, полученных преступным путем, и финансированию терроризма,

осуществляя борьбу с конечным результатом ОД – переходом денежных средств и иного имущества из теневого оборота в легальную экономику, с учетом форм и методов реализации данного процесса.

«При рассмотрении процедурных аспектов отмывания (легализации) неправомерных доходов стоит отметить, что преступные доходы в процессе придания им правомерного вида проходят несколько этапов легализации. В научной литературе зачастую приводится трехфазная модель отмывания доходов, разработанная экспертами FATF (Financial Action Task Force on Money Laundering – Группа разработки финансовых мер борьбы с отмыванием денег) [3; 6; 256]. Данная модель предполагает последовательное прохождение трех фаз: размещение (placement), расслоение (layering), интеграцию (integration). Однако на практике данные фазы могут проходиться в любой последовательности, налагаться друг на друга или отсутствовать» [230, с. 58].

«Под размещением понимается такой этап процесса отмывания доходов, в рамках которого преступно полученные денежные средства поступают в легальную финансовую систему того или иного государства. Данный этап может осуществляться путем депонирования наличных денежных средств на банковский счет, приобретения ценных бумаг, преобразования цифровой валюты в фиатную валюту и т.д. Размещение преступных доходов является самым уязвимым для осуществляющего отмывание доходов лица этапом, поэтому при размещении преступных денежных средств преступники отдают предпочтение либо контролируемым финансовым учреждениям, либо таким финансовым организациям, которые не будут задавать лишних вопросов о происхождении денежных средств. Возможны также иные варианты размещения преступных доходов, при которых наличные денежные средства разбиваются на небольшие суммы (так чтобы они не превышали порогов контроля, установленных законодательством) при внесении их на счета в различные банки от имени различных клиентов, а также маскируются в законной выручке предприятий, деятельность которых связана с значительным оборотом наличных денежных средств» [230, с. 58].

«Под расслоением понимается совершение финансовых операций, гражданско-правовых сделок, иных действий с целью отдаления преступных доходов от источника их происхождения, нивелирования связи между обращающимися в легальной финансовой системе денежными средствами, а также иным имуществом и их преступным началом. При осуществлении расслоения преступных доходов активно применяются трансграничные финансовые операции при помощи банков (предоставляющих возможность проведения финансовых операций) и компаний (предоставляющих основания проведения финансовых операций), расположенных в офшорных юрисдикциях. Льготные налоговые режимы, предоставляемые офшорными юрисдикциями нерезидентам, и обеспечение со стороны таких юрисдикций конфиденциальности информации о владельцах банковских счетов создают условия, благоприятствующие использованию данных юрисдикций в процессе отмывания преступных доходов» [230, с. 58].

«В процессе анализа фазы расслоения доходов, полученных преступным путем, в научных источниках отмечается, что после завершения данной фазы распутать цепочку финансовых операций и определить источник возникновения средств может быть затруднительно [3].

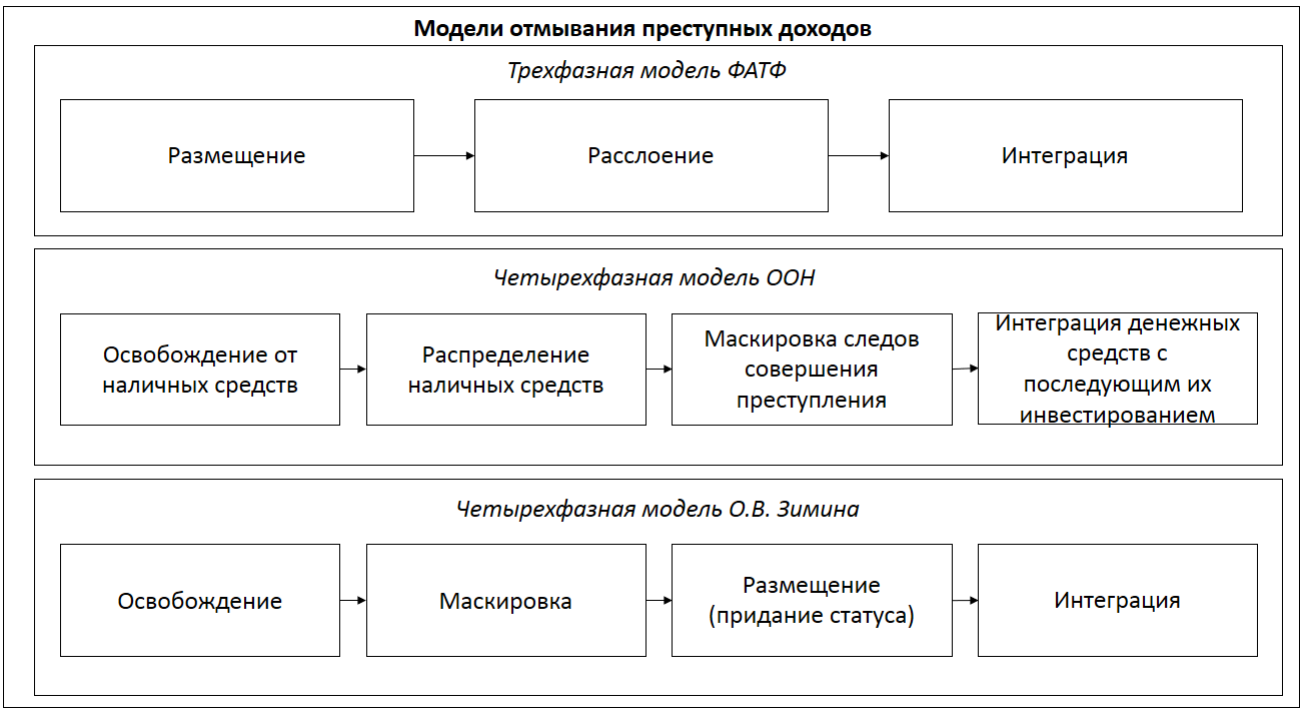
В рамках третьей фазы – интеграции – отмытые денежные средства консолидируются из разрозненных на предыдущих стадиях активов и инвестируются в легальную экономику, в том числе путем приобретения недвижимости, ценных бумаг, произведений искусства, предметов роскоши и т.д. При выборе активов для приобретения приоритет отдается тем государствам и отраслям, в которых преступники имеют определенные гарантии сохранения контроля за вложенными средствами (например, пользуются политическим, экономическим или иным влиянием). Часть средств возвращается в страну расположения преступной организации. В научных источниках отмечается, что для организованных преступных группировок характерно приобретение или создание предприятий, которые могут в дальнейшем использоваться при осуществлении преступной деятельности или в целях отмывания доходов» [6; 230, с. 58].

«Существует также четырехфазная модель легализации преступных доходов, используемая экспертами ООН [3]. В рамках данной модели первой фазой является освобождение от наличных средств и перечисление их на счета подставных лиц. Во второй фазе происходит распределение наличных денежных средств посредством приобретения ценных бумаг, а также с использованием пунктов обмена валюты, казино, ночных клубов. В третьей фазе маскируются следы совершения преступления, скрывается преступный источник происхождения имущества. Заключительной фазой является интеграция денежных средств с последующим инвестированием их в отрасли экономики с высоким уровнем доходности.

Четырехстадийную модель отмывания доходов, полученных преступным путем, предлагает использовать О.В. Зимин [227]. Он выделяет четыре стадии процесса отмывания преступных доходов: освобождение, маскировка, размещение (придание статуса) и интеграция. Под освобождением ученый понимает такие действия лица, получившего преступный доход, в ходе которых оно вводит преступные доходы в легальный коммерческий оборот. Под маскировкой подразумевается стадии легализации, выражающаяся в сокрытии преступности происхождения доходов, их источника, а также владельца. В ходе стадии размещения, по мнению Зимина, совершаются экономические и хозяйственные операции с целью исключения возможности установления взаимосвязи между полученными доходами и их источником, владельцем. На заключительной стадии – интеграции – происходит аккумулирование денежных средств и иного имущества у владельца, позволяющее последнему свободно их использовать в экономическом обороте» [230, с. 58–59]. Концепции моделей ОД в сравнительном обзоре представлены на рисунке 3.

Как следует из вышеприведенного сравнения различия между моделями выражаются в разделении некоторыми экспертами стадий размещения и расслоения преступных доходов на две стадии. При этом, в случае с экспертами ООН разделяется именно стадия размещения (хотя стоит отметить, что распределение наличных средств, как стадия, может происходить одновременно с

освобождением от наличных средств, выделение ее в качестве отдельной стадии скорее связано с отличием процедурной реализации, чем с принципиально иным функциональным назначением). Тогда, как О.В. Зимин разделяет именно стадию расслоения на стадию сокрытия преступного происхождения доходов и стадию сокрытия фактов связи между денежными средствами и их владельцем [230]. По нашему мнению, такое разделение также является искусственным, так как данные стадии фактически могут выполняться в рамках одного действия (например, за счет использования программ-миксеров в криптовалютах, позволяющих, как сокрыть преступный характер доходов в конечном их виде, так и связь с их владельцем). По мнению автора, наиболее актуальной концепцией стадий ОД является общепризнанная трехфазная модель FATF (далее будет применяться вариант наименования в русской транслитерации – ФАТФ, как получивший широкое распространение).



Источник: составлено автором на основании материалов [3; 227].
Рисунок 3 – Модели отмывания преступных доходов

«Интерес также представляет позиция некоторых зарубежных ученых, которые выделяют две стадии процесса отмывания доходов: отмывание денег (money laundering) и возвращение их в оборот (recycling). Стоит отметить, что ряд ученых, в частности Прошунин М.М., считает данный подход несостоятельным

[256]. По его мнению, отмывание денег невозможно без их возвращения в оборот. Также он считает, что не выдерживает критики и четырехстадийная модель, так как стадия маскировки является лишь составной частью стадии размещения. В силу этого ученый считает состоятельной лишь трехфазную модель отмывания преступных доходов» [230, с. 59].

С процессом отмывания преступных доходов имеет тесную связь и процесс финансирования терроризма. Данная взаимосвязь обусловлена тем, что ряд источников финансирования терроризма имеет незаконный характер и потому могут потребовать предварительного отмывания [6]. Кроме того, лица, участвующие в финансировании террористической деятельности, зачастую заинтересованы в сокрытии данного факта, а также каналов спонсирования, в силу чего в них применяются схожие с легализацией преступных доходов методы и средства. Также научные источники указывают на то, что схожесть техник финансирования терроризма и отмывания доходов, полученных преступным путем, может быть обусловлена возможностью вовлечения в процесс финансирования терроризма финансовых посредников, оказывающих услуги по легализации доходов (так называемых, «профессиональных отмывателей»), которые могут быть и не осведомлены о назначении легализуемых денежных средств [3].

«Понятие финансирования терроризма на международном уровне закреплено в рамках Международной конвенции о борьбе с финансированием терроризма, принятой ООН в 1999 г. [22]. Согласно данной конвенции, финансированием терроризма признается предоставление любым лицом любыми методами, прямо или косвенно, незаконно и умышленно, средств или осуществление их сбора с намерением, чтобы они использовались, или при осознании того, что они будут использоваться, полностью или частично, для совершения:

а) какого-либо деяния, представляющего собой преступление согласно сфере применения одного из договоров, перечисленных в приложении, и содержащемуся в нем определению;

б) любого другого деяния, направленного на то, чтобы вызвать смерть какого-либо гражданского лица или любого другого лица, не принимающего активного участия в военных действиях в ситуации вооруженного конфликта, или причинить ему тяжкое телесное повреждение, когда цель такого деяния в силу его характера или контекста заключается в том, чтобы запугать население или заставить правительство или международную организацию совершить какое-либо действие или воздержаться от его совершения» [236, с. 310].

«Ссылка на ряд международных договоров в статье содержится в силу отсутствия в международном праве универсального определения понятия «терроризм». В числе указанных международных договоров присутствуют [22]:

а) Конвенция о борьбе с незаконным захватом воздушных судов, от 16 декабря 1970 года.

б) Конвенция о борьбе с незаконными актами, направленными против безопасности гражданской авиации от 23 сентября 1971 года.

в) Конвенция о предотвращении и наказании преступлений против лиц, пользующихся международной защитой, в том числе дипломатических агентов, от 14 декабря 1973 года.

г) Международная конвенция о борьбе с захватом заложников, от 17 декабря 1979 года.

д) Конвенция о физической защите ядерного материала, от 3 марта 1980 года.

е) Протокол о борьбе с незаконными актами насилия в аэропортах, обслуживающих международную гражданскую авиацию, дополняющий Конвенцию о борьбе с незаконными актами, направленными против безопасности гражданской авиации, от 24 февраля 1988 года.

ж) Конвенция о борьбе с незаконными актами, направленными против безопасности морского судоходства, от 10 марта 1988 года.

и) Протокол о борьбе с незаконными актами, направленными против безопасности стационарных платформ, расположенных на континентальном шельфе, от 10 марта 1988 года.

к) Международная конвенция о борьбе с бомбовым терроризмом, от 15 декабря 1997 года» [236, с. 310].

В принятом Советом глав государств СНГ 15 октября 2021 года Договоре государств – участников Содружества Независимых Государств о противодействии легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения (далее – Договор СНГ о ПОД/ФТ/ФРОМУ) определение финансирования терроризма приведено в более узкой (в части предикатных преступлений, то есть преступлений, предшествующих основному [201]) формулировке: «предоставление или сбор средств либо оказание финансовых услуг любыми методами или способами, прямо или косвенно, с осознанием того, что они предназначены или будут использованы полностью или частично для финансирования организации, подготовки, включая финансирование поездок лиц в иные государства, или совершения хотя бы одного из преступлений террористического характера либо для подготовки террористов или прохождения такой подготовки, обеспечения террориста или организованной группы, незаконного вооруженного формирования, преступного сообщества (преступной организации), созданных или создаваемых для совершения хотя бы одного из преступлений террористического характера» [17].

«В российском правовом пространстве понятие «финансирование терроризма» закреплено в ст. 3 Федерального закона «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», согласно которому к финансированию терроризма следует отнести предоставление или сбор средств либо оказание финансовых услуг с осознанием того, что они предназначены для финансирования организации, подготовки и совершения хотя бы одного из преступлений, предусмотренных статьями 205; 205.1; 205.2; 205.3, 205.4; 205.5; 206; 208; 211; 220; 221; 277; 278; 279; 360 и 361 Уголовного кодекса Российской Федерации, либо для финансирования или иного материального обеспечения лица в целях совершения им хотя бы одного из указанных преступлений, либо для обеспечения организованной группы,

незаконного вооруженного формирования или преступного сообщества (преступной организации), созданных или создаваемых для совершения хотя бы одного из указанных преступлений» [34; 236, с. 310–311].

Основной объем средств, направляемых в целях финансирования терроризма, согласно информации из научных источников, расходуется на материально-техническое обеспечение деятельности террористических организаций, а также на вербовку их сторонников, тогда как непосредственно на осуществление террористических актов затрачиваются сравнительно небольшие суммы (так, стоимость серии террористических актов в США 11 сентября 2021 года оценивается в 300-500 тыс. долларов) [6]. «Специалистами в сфере противодействия финансированию терроризма выделяются следующие направления финансового обеспечения террористической деятельности:

– спонсирование пропаганды экстремистской и террористической идеологии (в том числе, финансирование деятельности соответствующих учебных заведений, выпуска экстремистской литературы и иных пропагандистских материалов);

– финансирование подготовки членов террористических организаций и незаконных вооруженных формирований (в том числе, вербовка новых сторонников и содержание тренировочного лагеря);

– расходы на непосредственную подготовку террористических актов (включая расходы на приобретение оружия, боеприпасов, взрывчатых веществ, транспорта и средств связи, осуществления иных подготовительных мероприятий);

– выплата вознаграждений членам террористических организаций и родственникам погибших боевиков;

– организация деятельности «спящих» ячеек террористов;

– содержание организаций, являющихся легальным «прикрытием» для террористических сообществ (например, благотворительные и иные виды некоммерческих организаций);

– расходы на подкуп государственных служащих и оплату услуг специалистов» [236, с. 311].

«Специалисты отмечают, что общие расходы на обеспечение деятельности террористических структур в разы превышают стоимость отдельных террористических актов.

Финансирование терроризма может осуществляться различными лицами, начиная от благотворительных фондов и заканчивая организованными преступными сообществами. В научной литературе содержится следующая классификация источников финансирования терроризма:

а) Доходы от нелегальной деятельности:

1) Незаконный оборот оружия, боеприпасов и взрывчатых веществ.

2) Незаконный оборот наркотических средств и их прекурсоров.

3) Хищение имущества в крупных размерах, разбой и рэкет.

4) Похищение людей с целью получения выкупа.

5) Фальшивомонетничество.

6) Контрабанда.

7) Отмывание денежных средств, полученных преступным путем.

б) Доходы от деятельности предприятий, подконтрольных террористической организации:

1) Доходы от предприятий легального сектора.

2) Доходы от предприятий теневого сектора экономики.

3) Доходы от офшорного бизнеса.

в) Финансовая поддержка:

1) Частных лиц.

2) Организаций (в первую очередь, некоммерческих организаций социальной, политической и религиозной направленности).

3) Спецслужб заинтересованных государств.

В целом, можно отметить, что несмотря на направленность самой террористической деятельности на совершение террористических актов, как способа устрашения населения, оказания давления на органы государственной власти, финансирование терроризма направленно преимущественно не на финансовое обеспечение терактов, а на обеспечение деятельности

террористических структур, в целом. Соответственно, связь между денежными средствами, поступающими в целях финансирования терроризма, и совершаемыми террористическими актами опосредуется террористической организацией, осуществляющей (на централизованном уровне или на уровне местных ячеек) аккумулирование поступлений и их распределение в целях осуществления террористической деятельности. Однако, для самой террористической организации поступающие финансовые потоки играют весьма существенную (если не ключевую) роль. Так, по оценкам экспертов, годовые расходы запрещенной в Российской Федерации террористической организации «Исламское государство» в 2015 году составляли 1-2 млрд долларов в год» [236, с. 311–312].

1.2 Сущность механизма мониторинга противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма[1]

Приступая к анализу сущности механизма мониторинга противодействия легализации доходов, полученных преступным путем, и финансированию терроризма (далее – механизм мониторинга ПОД/ФТ) стоит отметить слабую научную разработанность понятия «механизм мониторинга ПОД/ФТ», что зачастую выражается в его объединении с термином «механизм противодействия легализации доходов, полученных преступным путем, и финансированию терроризма» (далее – механизм ПОД/ФТ) [218; 224]. В связи с этим первоначально необходимо обратиться к анализу понятия «механизм ПОД/ФТ». Данный термин получил широкое доктринальное и нормативное распространение, однако в то же время в научных источниках наблюдается дефицит определений данного понятия [34; 204; 242; 264; 272; 273]. «Так, Юсупов Н.В. дает следующее определение термину – политико-правовой механизм противодействия отмыванию преступных доходов представляет собой совокупность целенаправленных, юридически

1) Текст подготовлен на основе публикаций автора [229; 231].

закрепленных отношений между общественными группами по поводу использования институтов публичной власти, в целях обеспечения экономической безопасности государства [272]. Также в учебном пособии «Финансовый мониторинг» под редакцией Ю.А. Чиханчина и А.Г. Братко приводится характеристика нормативной основы правового механизма ПОД/ФТ – федеральные законы, нормативные акты Банка России и нормативные правовые акты федеральных органов исполнительной власти» [11; 232, с. 44]. Однако, вышеприведенные трактовки тяготеют к юридическому дискурсу и не являются полноценно релевантными к научной тематике работы. В связи с этим, существует необходимость формулирования авторского определения понятия «механизм ПОД/ФТ».

Существующие в настоящее время трактовки термина «механизм» можно разделить на два вида:

– физическую: «Механизм – система звеньев (тел), преобразующая движение одних звеньев в требуемое движение других» [122];

– книжную: «Механизм – внутреннее устройство, система функционирования чего-нибудь, аппарат какого-нибудь вида деятельности» [122].

Применительно к тематике работы интерес представляют экономические подходы к понятию «механизм». В научных статьях отмечается, что «под механизмом в экономике целесообразно понимать характеристики процесса: способы, методы, нормы, средства, формы функционирования чего-либо или воздействия на что-либо, а не совокупность ресурсов или состояний объекта» [219, с. 20], так как для обозначения последнего используется понятие «система». Согласно трактовке лауреата Нобелевской премии по экономике за 2007 год Лео Гурвица, механизм представляет собой взаимодействие между субъектами и центром, состоящее из трех стадий: «каждый субъект в частном порядке посылает центру сообщение m, центр, получив все сообщения, вычисляет предполагаемый результат $Y = f(m_i, \ldots, m)$; центр объявляет результат Y и по необходимости претворяет его в жизнь» [94].

Понятие системы противодействия отмыванию доходов, полученных преступным путем, и финансированию терроризма содержится в Концепции развития национальной системы противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, утвержденной Президентом Российской Федерации 30 мая 2018 года (далее – Концепция). В ст. 3 Концепции приводится определения национальной системы ПОД/ФТ под которой понимается «совокупность федеральных органов исполнительной власти, других государственных органов и организаций, реализующих государственную политику в сфере противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма во взаимодействии с организациями, осуществляющими операции с денежными средствами или иным имуществом … посредством принятия мер организационного, координационного, аналитического, оперативного, нормативно-правового и информационного характера» [106]. Также термин «система ПОД/ФТ» раскрывается в статье О.В. Зимина «Понятие и структура государственной системы противодействия легализации (отмыванию) преступных доходов в Российской Федерации», в которой «государственная система противодействия легализации (отмыванию) преступных доходов» характеризуется, как «совокупность подсистем и элементов, основное назначение которых состоит в правовом, организационном и тактическом обеспечении противодействия легализации (отмыванию) преступных доходов и минимизации негативных последствий указанного противоправного деяния» [226, с. 47]. Зимин выделяет четыре подсистемы системы ПОД – «субъекты противодействия», «право», «деятельность», «меры противодействия». Экстраполируя вышеприведенную формулировку к государственной системе противодействия финансирования терроризма (с учетом того, что в обеих системах центральное место принадлежит подразделениям финансовой разведки) можно схожим образом определить, в целом, систему ПОД/ФТ.

«Анализируя вышеуказанные определения применительно к цели научного исследования, стоит отметить, что оба не являются полностью релевантными и

заменяющими понятие механизма ПОД/ФТ. Приведенная в Концепции трактовка рассматривает систему ПОД/ФТ как совокупность государственных органов и организаций, осуществляющих государственную политику в сфере ПОД/ФТ. Данное определение нельзя рассматривать в качестве охватывающего понятие механизма ПОД/ФТ, в силу того, что сам термин «механизм» предполагает больший акцент на деятельной стороне ПОД/ФТ, тогда как вышеприведенное понятие более склонно к структурной стороне противодействия отмыванию преступных доходов и финансированию терроризма. Кроме того, согласно приведенному в Концепции определению составляющими системы ПОД/ФТ являются государственные органы и организации, которые, в свою очередь, реализуют государственную политику во взаимодействии с организациями, осуществляющими операции с денежными средствами или иным имуществом, и иными лицам, перечисленными в Концепции. Однако, экономический подход к анализу механизма ПОД/ФТ требует учета в равной степени деятельности органов государственных власти и организаций, являющихся субъектами Закона № 155-ФЗ, в силу того, что именно последние непосредственно имеют дело с финансовыми потоками, в которых они обязаны выявлять операции, подлежащие обязательному контролю, и подозрительные операции.

Подход, предложенный Зиминым О.В., несмотря на то, что охватывает деятельную сторону противодействия отмыванию преступных доходов и финансированию терроризма, является чрезмерно широким для целей исследования, а также имеет правовой характер, что затрудняет его применение в экономическом дискурсе» [232, с. 45].

При этом, с понятием механизма ПОД/ФТ наиболее близко соотносится в классификации О.В. Зимина подсистема «деятельность», которая по мнению ученого состоит из «совокупности видов деятельности (оперативно-розыскной, уголовно-процессуальной, административно-процессуальной, профилактической, контрольной, надзорной, исполнительной, правотворческой, ревизионной и других), которые осуществляются субъектами противодействия легализации преступных доходов» [226, с. 47].

В целях выработки экономического определения механизма ПОД/ФТ необходимо интерпретировать суть противодействия ОД/ФТ. В соответствии с вышеприведенным подходом к экономической трактовке отмывания доходов, полученных преступным путем, а также с учетом процедурной составляющей финансирования терроризма можно привести следующее определение противодействия отмыванию преступных доходов и финансированию терроризма: процесс выявления и пресечения потоков денежных средств и иных активов, связывающих теневую и легальную экономику, а также потоков денежных средств и иных активов, направленных на материальное обеспечение деятельности террористических организаций или на содействие в организации и осуществлении преступлений террористической направленности.

Также для выработки определения понятию «механизм ПОД/ФТ» важную роль играет определенность термина «субъект противодействия отмыванию преступных доходов и финансированию терроризма». Так, Ю.А. Чиханчин и А.Г. Братко выделяют следующие субъекты ПОД/ФТ:

а) Росфинмониторинг, надзорные и правоохранительные органы;

б) субъекты Закона № 115-ФЗ;

в) клиенты субъектов Закона № 115-ФЗ;

г) бенефициарные владельцы и выгодоприобретатели клиентов Закона № 115-ФЗ [11].

В вышеуказанной статье О.В. Зимина подсистема «субъекты противодействия» описывается, как «совокупность государственных органов противодействия в широком смысле — органов законодательной, исполнительной и судебной власти, наделенных общей либо специальной компетенцией в сфере противодействия легализации (отмыванию) преступных доходов» [226, с. 47]. Однако, стоит учитывать, что тематика научной статьи О.В. Зимина ограничена исключительно государственной системой ПОД/ФТ. Более обширным представляется определение, приведенное И.А. Новиковым, согласно которому в систему ПОД/ФТ (что в контексте научного исследования равнозначно субъектам противодействия ОД/ФТ) входят «федеральные органы исполнительной власти и

другие государственные органы и организации, осуществляющие работу в данной области», так как данное определение охватывает не только государственный сектор механизма ПОД/ФТ, но и комплаенс-систему финансовых организаций и иных организаций, в чьи обязанности входит проверка клиентов и операций на соответствие требованиям законодательства в сфере ПОД/ФТ, которую также относят к системе противодействия отмыванию преступных доходов [200; 251, с. 63].

Таким образом, применительно к тематике исследования к субъектам ПОД/ФТ следует относить первые две группы субъектов, выделенных Ю.А. Чиханчиным и А.Г. Братко, в связи с тем, что «последние две группы субъектов системы ПОД/ФТ непосредственно не участвуют в деятельности, направленной на противодействие отмыванию преступных доходов и финансированию терроризма, хоть и обладают в соответствии с Федеральным законом № 115-ФЗ рядом прав и обязанностей» [232, с. 46].

С учетом вышеприведенных определений понятий противодействия ОД/ФТ и субъекта противодействия ОД/ФТ механизм противодействия отмыванию доходов, полученных преступным путем, и финансированию терроризма можно охарактеризовать следующим образом: «опосредованная международными и национальными нормами права и созданная в целях обеспечения экономической безопасности государства система организации деятельности субъектов противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, заключающейся в выявлении и пресечении потоков денежных средств и иных активов, связывающих теневую и легальную экономику, а также потоков денежных средств и иных активов, направленных на обеспечение деятельности террористических организаций или на содействие в организации и осуществлении преступлений террористической направленности» [232, с. 46].

Так как ключевым звеном механизма ПОД/ФТ является деятельность субъектов противодействия легализации (отмыванию) преступных доходов и финансированию терроризма, то и структура механизма ПОД/ФТ будет

определяться структурой данных субъектов (что также является системой организации деятельности субъектов противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма) [11]:

а) Блок финансового мониторинга:

1) Организации-субъекты первичного финансового мониторинга, осуществляющие операции с денежными средствами или иным имуществом, а также иные организации и лица, в чьи обязанности входит проверка клиентов и операций на соответствие требованиям законодательства в сфере ПОД/ФТ.

2) Подразделение финансовой разведки, осуществляющее государственный финансовый мониторинг.

б) Контрольно-надзорные органы, осуществляющие контроль (надзор) за соблюдением требований антиотмывочного законодательства субъектами первичного финансового мониторинга.

в) Правоохранительные органы и иные органы государственной власти.

г) Законотворческие и иные правотворческие органы в сфере ПОД/ФТ.

Отмечаем, что разделение механизма ПОД/ФТ на четыре составляющие обусловлено тем, что в рамках финансового мониторинга осуществляется аналитическая деятельность субъектов ПОД/ФТ, тогда как в блоке правоохранительных и иных государственных органов осуществляется непосредственно правоприменительная деятельность, направленная на предупреждение, пресечение правонарушений, а также на привлечение к юридической ответственности лиц, виновных в совершении тех или иных нарушений. Стоит оговориться, что ряд полномочий в сфере предупреждения отмывания преступных доходов и финансирования терроризма имеется также у подразделения финансового мониторинга (например, Федеральная служба по финансовому мониторингу уполномочена издавать постановления о приостановлении операций с денежными средствами или иным имуществом) и организаций, осуществляющих операции с денежными средствами и иным имуществом, управомоченным в Российской Федерации приостанавливать операции организаций и физических лиц при наличии оснований,

предусмотренных Федеральным законом № 115-ФЗ от 07.08.2001 «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» [52; 230]. Блок финансового мониторинга и блок правоохранительных и иных государственных органов, в свою очередь, осуществляют свою деятельность на основании законов и подзаконных актов, изданных правотворческими органами. Блок контрольно-надзорных органов обеспечивает соблюдение требований антиотмывочного законодательства субъектами первичного финансового мониторинга в части предоставления необходимой информации об операциях и сделках, которые могут быть связаны с ОД/ФТ.

Под финансовым мониторингом понимается «комплекс мер, принимаемых финансовыми учреждениями и компетентными государственными органами в целях предупреждения, выявления и пресечения операций, связанных с легализацией (отмыванием) доходов, полученных преступным путем, или финансированием терроризма» [6, с. 103]. Первичный финансовый мониторинг представляет собой деятельность организаций, осуществляющих операции с денежными средствами или иным имуществом, а также иных организаций и лиц, по контролю за клиентами и проводимыми ими операциями и сделками, направленную на соблюдение требований антиотмывочного законодательства [11]. Государственный финансовый мониторинг, соответственно, осуществляется подразделением финансовой разведки (в Российской Федерации – Федеральной службой по финансовому мониторингу).

Блок финансового мониторинга, блок надзора за соблюдением требований антиотмывочного законодательства субъектами первичного финансового мониторинга, а также процесс взаимодействия блока финансового мониторинга с правоохранительным блоком и составляет механизм мониторинга ПОД/ФТ. Блок финансового мониторинга составляет основу механизма мониторинга ПОД/ФТ. Блок надзора является неотъемлемой частью механизма мониторинга, так как необходим для обеспечения генерации информации об операциях и сделках, связанных с ОД/ФТ. Процесс взаимодействия блока финансового мониторинга с

правоохранительным блоком необходимо включить в механизм мониторинга ПОД/ФТ в силу того, что на данном этапе осуществляется реализация механизма мониторинга ПОД/ФТ.

Сущность механизма мониторинга ПОД/ФТ формулируется исходя из присущих механизму мониторингу нижеперечисленных общих черт, выделенных на основе анализа приведенных в научных источниках определений механизма мониторинга [214; 216; 217; 248]:

– «Объектом механизма мониторинга является информация, представляющая интерес в целях выработки тех или иных практических решений;

– Субъектами механизма мониторинга являются органы или лица, осуществляющие получение или генерацию информации в рамках механизма мониторинга;

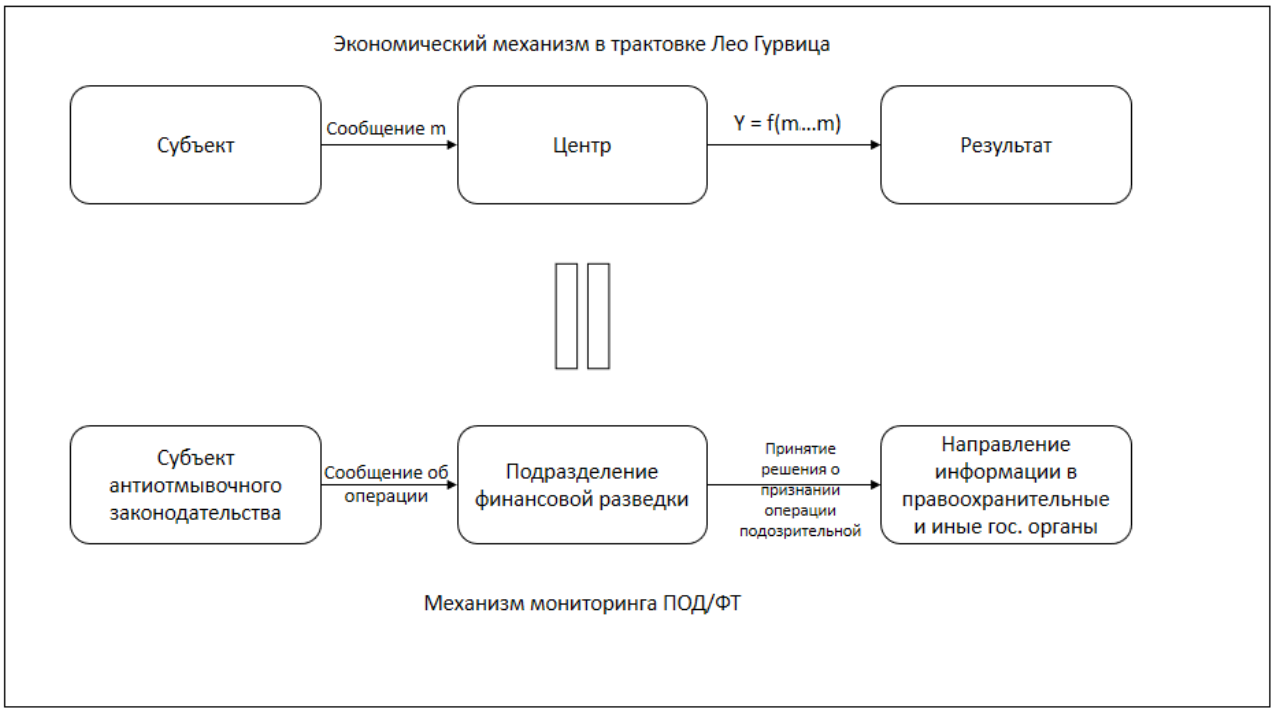
– Целью механизма мониторинга является предоставление информации лицам, принимающим решения, для последующего принятия ими тех или иных практических мер» [234, с. 4].

Таким образом, механизм мониторинга ПОД/ФТ можно охарактеризовать, как составную часть механизма ПОД/ФТ, в рамках которой на основании анализа информации «о проводимых финансовых операциях и заключаемых сделках осуществляется выявление операций, связанных с легализацией (отмыванием) доходов, полученных преступным путем, или финансированием терроризма, результаты чего передаются в правоохранительные и иные государственные органы в целях принятия ими мер, направленных на противодействие легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» [234, с. 6].

Модель функционирования механизма мониторинга ПОД/ФТ можно описать посредством вышеприведенной модели экономического механизма с позиции Лео Гурвица, если вместо сообщения m подставить сообщение о подозрительной операции или об иной операции, информация о которой направляется в подразделение финансовой разведки, а вместо результата Y – решение подразделения финансовой разведки о наличии в той или иной

операции/деятельности признаков ОД/ФТ с последующим извещением правоохранительных или иных государственных органов.

На рисунке 4 представлена модель функционирования механизма мониторинга ПОД/ФТ в преломлении концепции экономического механизма Лео Гурвица.



Источник: составлено автором.

Рисунок 4 – Интерпретация механизма мониторинга ПОД/ФТ в рамках модели экономического механизма Лео Гурвица

Структура механизма противодействия отмыванию преступных доходов и финансированию терроризма представлена на рисунке 5 (где пунктиром отмечен механизм мониторинга ПОД/ФТ).

Стоит отметить, что вышеприведенная структура механизма ПОД/ФТ не является идентичной для всех существующих в мире систем ПОД/ФТ и имеет скорее российскую специфику, однако для большинства национальных механизмов противодействия отмыванию преступных доходов и финансированию терроризма характерно наличие подразделения финансовой разведки (далее – ПФР), осуществляющего анализ поступающей информации о подозрительных операциях (сделках), профильных органов, осуществляющих контроль за соблюдением законодательства в области ПОД/ФТ, а также правоохранительных органов, осуществляющих оперативно-розыскную и правоприменительную

деятельность [232]. В некоторых случаях в одном ведомстве могут объединены контрольный орган и ПФР (например, в Армении), в некоторых – ПФР может иметь часть полномочий правоохранительных органов (например, в Казахстане). Однако, за исключением одного звена опциально исключаемого или добавляемого в зависимости от особенностей национальной системы ПОД/ФТ, общая структура механизма ПОД/ФТ остается неизменной.

Источник: составлено автором.

Рисунок 5 – Структура механизма противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма

Также для тематики исследования важную роль имеет определение понятия «цифровизация экономики». В научных источниках термин «цифровизация» в широком смысле понимается, как «современный общемировой тренд развития экономики и общества, который основан на преобразовании информации в цифровую форму и приводит к повышению эффективности экономики и улучшению качества жизни» [253, с. 355]. Также цифровизация экономики раскрывается, как «внедрение цифровых и информационно-коммуникационных технологий в экономику, делающее возможным снижение стоимости услуг, как государственных, так и коммерческих, увеличение доступности товаров и упрощение их вывода на глобальные рынки, повышение скорости доработки

предполагаемых продуктов под новые ожидания и потребности их потенциальных пользователей» [181].

При этом, к основным технологиям цифровизации экономики принято относить [181]:

– технологии больших данных (Big Data) – «инструменты и способы обработки информации в массивах большого объема и с разнообразными структурами» [181];

– интернет вещей (Internet of Things) – «сеть предметов, способных контактировать друг с другом или с внешней средой без вовлечения человека» [181];

– блокчейн – «технология шифрования и хранения данных (реестра), которые распределены по множеству компьютеров, объединенных в общую сеть» [61];

– технологии искусственного интеллекта и машинного обучения – «комплекс методик математики, биологии, психологии, кибернетики и других наук, с помощью которого создаются технологии для написания «интеллектуальных» программ и обучения компьютеров самостоятельному решению задач. Главная задача искусственного интеллекта - это моделирование человеческого разума. Машинное обучение (machine learning, ML) - это одно из направлений разработки ИИ, основанное на выполнении компьютером множества сходных задач без использования прямых инструкций» [178].

С понятием «цифровизация экономики» непосредственно связан термин «цифровая экономика». При изучении сущности данного термина Р. Мещеряков выделяет два подхода к определению цифровой экономики: классический и расширенный. Согласно классическому подходу, под цифровой экономикой подразумевается «экономика, основанная на цифровых технологиях», то есть ограниченная областью электронных товаров и услуг. Тогда как согласно расширенному подходу, «цифровая экономика – это экономическое производство с использованием цифровых технологий» [211, с. 56].

Определение понятия «цифровая экономика» представлено также в Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы, утвержденной Указом Президента Российской Федерации от 09.05.2017 г. № 203, согласно которой «цифровая экономика – хозяйственная деятельность, в которой ключевым фактором производства являются данные в цифровом виде, обработка больших объемов и использование результатов анализа которых по сравнению с традиционными формами хозяйствования позволяют существенно повысить эффективность различных видов производства, технологий, оборудования, хранения, продажи, доставки товаров и услуг» [42].

С учетом вышеизложенного «механизм мониторинга ПОД/ФТ можно представить в виде единой многоуровневой системы организации деятельности субъектов механизма мониторинга ПОД/ФТ, в котором следует выделить следующие уровни:

а) Микроуровень механизма мониторинга ПОД/ФТ:

1) структурные подразделения и должностные лица организаций, осуществляющих операции с денежными средствами или иным имуществом, а также иные организации и лица, в чьи обязанности входит проверка клиентов и операций на соответствие требованиям законодательства в сфере ПОД/ФТ (первичный финансовый мониторинг).

б) Национальный уровень механизма мониторинга ПОД/ФТ (включает в себя также региональный уровень, обусловленный структурой территориальных подразделений субъектов национального уровня механизма мониторинга ПОД/ФТ):

1) подразделение финансовой разведки (государственный финансовый мониторинг);

2) органы финансового контроля, осуществляющие контроль (надзор) за соблюдением требований законодательства в сфере ПОД/ФТ.

в) Наднациональный уровень механизма мониторинга ПОД/ФТ:

1) международные координационные органы в сфере ПОД/ФТ» [234, с. 6].

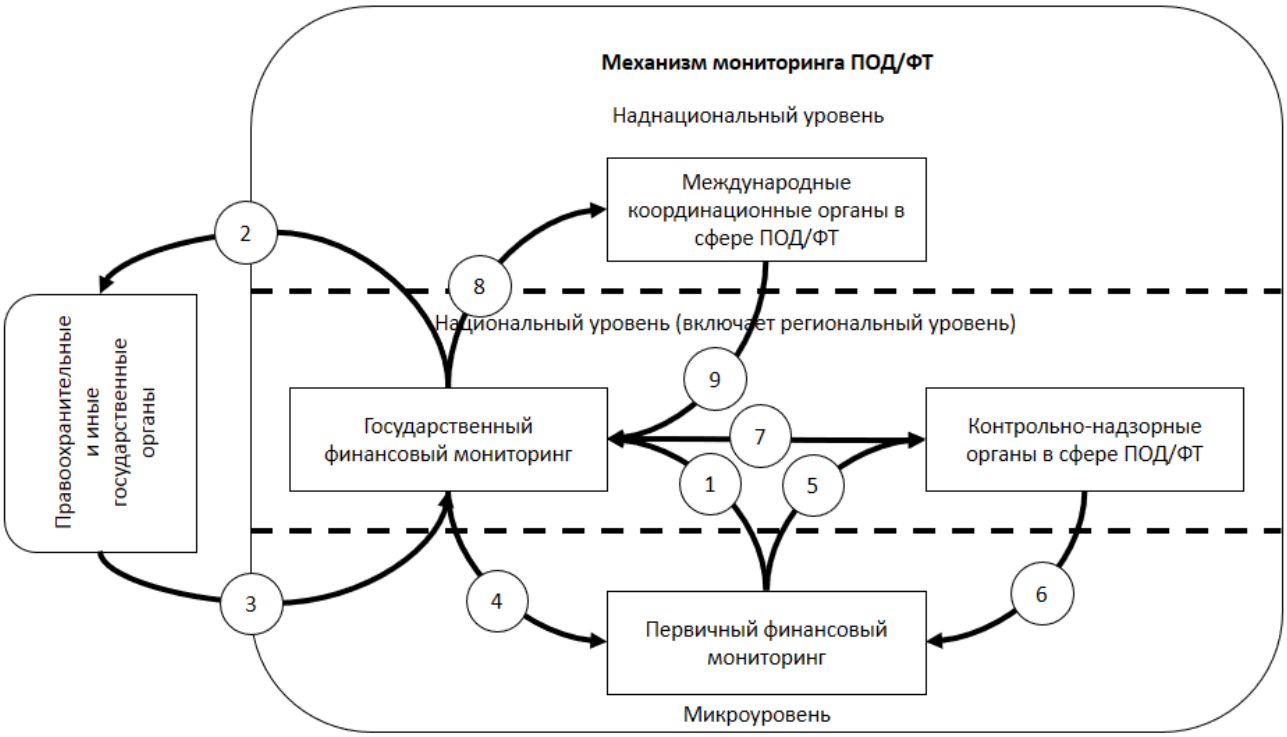
«Разделение на уровни обусловлено функциональным назначением субъектов ПОД/ФТ в механизме мониторинга ПОД/ФТ, кругом их прав и обязанностей, а также масштабом осуществляемой ими деятельности.

Так, несмотря на то, что субъекты первичного финансового мониторинга могут осуществлять свою деятельность на всей территории страны, круг их полномочий ограничивается выявлением операций, которые могут быть связаны с ОД/ФТ, а также совершением ряда иных обязанностей в сфере ПОД/ФТ, что может быть охарактеризовано, как генерация аналитической информации для субъектов более верхнего уровня, а также выполнение распоряжений субъектов ПОД/ФТ национального уровня (например, о направлении информации о финансовых операциях в отношении объектов заинтересованности, а также исполнение требований о замораживании средств лиц, причастных к террористической и экстремистской деятельности). При этом, область анализа непосредственно самих субъектов первичного финансового мониторинга ограничивается финансовыми операциями и сделками их клиентов.

Подразделение финансовой разведки, в свою очередь, оперирует информацией, поступающей от различных субъектов первичного финансового мониторинга, что позволяет ему осуществлять анализ информации уже на национальном уровне, в разрезе операций, совершаемых объектами заинтересованности, в различных субъектах микроуровня на территории всей страны (или на территории отдельных регионов в рамках компетенции соответствующих территориальных подразделений). В то же время, подразделение финансовой разведки имеет возможность осуществлять анализ, как на макроуровне путем проведения исследований, характеризующих обстановку в сфере ПОД/ФТ на территории всей страны, так и на микроуровне путем изучения финансовой деятельности тех или иных объектов заинтересованности. Подразделение финансовой разведки осуществляет генерацию аналитической информации для руководства страны, правоохранительных органов, иных органов государственной власти, а также для международных координационных органов в сфере ПОД/ФТ (в

части передачи макроаналитической информации об обстановке в сфере ПОД/ФТ)» [234, с. 6–7].

«Иными полномочиями обладают международные координационные органы в сфере ПОД/ФТ (ФАТФ и рабочие группы по типу ФАТФ), информация к которым поступает уже деперсонифицированная, представляющая собой макроаналитический срез обстановки в сфере ПОД/ФТ (в целом, а также в отдельных ее контекстах), на основе чего осуществляется обмен практиками между подразделениями финансовыми разведками мира, а также вырабатываются рекомендации по совершенствованию национальных механизмов мониторинга ПОД/ФТ» [234, с. 7]. Соответственно, модель механизма мониторинга ПОД/ФТ можно изобразить в схематичном виде, представленном на рисунке 6.



Источник: составлено автором.

Рисунок 6 – Модель механизма мониторинга противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма

Используемые в схеме обозначения представлены в таблице 1.

Таблица 1 – Обозначения, используемые в модели механизма мониторинга противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма

Номер элемента	Описание
1	2
1	Информация об операциях, которые могут быть связаны с ОД/ФТ, направляемая субъектами первичного финансового мониторинга в адрес подразделения финансовой разведки
2	Результаты анализа полученной информации с выявленными признаками ОД/ФТ, передаваемые подразделением финансовой разведки в адрес правоохранительных и иных государственных органов
3	Реакция правоохранительных органов на полученную информацию, а также запросы в адрес подразделения государственного финансового мониторинга
4	Запросы, направляемые подразделением финансовой разведки в адрес субъектов первичного финансового мониторинга, а также иные сведения, предусмотренные национальным антиотмывочным законодательством
5	Информация о результатах исполнения требований антиотмывочного законодательства, предоставляемая в адрес органов финансового контроля в рамках поднадзорности
6	Запросы, предписания и иные требования органов финансового контроля в отношении соблюдения субъектами первичного финансового мониторинга требований антиотмывочного законодательств
7	Информация о ситуации в сфере соблюдения требований антиотмывочного законодательства, передаваемая в рамках взаимодействия между подразделением финансовой разведки и органами финансового контроля
8	Информация, направляемая в международные организации в сфере ПОД/ФТ в части предоставления макроаналитических данных по интересующим международные органы вопросам соблюдения требований ПОД/ФТ, а также информация, передаваемая в рамках взаимодействия с иностранными подразделениями финансовой разведки
9	Результаты проведенных международных исследований в сфере ПОД/ФТ, рекомендации по совершенствованию национального механизма мониторинга в сфере ПОД/ФТ, а также иная значимая информация, получаемая подразделением финансовой разведки от международных органов в сфере ПОД/ФТ

Источник: составлено автором и опубликовано [234, с. 7-8].

Схожие модели механизма мониторинга ПОД/ФТ можно отметить у ряда авторов. Так, М.М. Прошунин выделяет три уровня «системы уполномоченных органов и организаций в сфере финансового мониторинга» [258, с. 44]:

а) Росфинмониторинг (или подразделение финансовой разведки), который «обеспечивает накопление и анализ информации, поступающей от организаций, осуществляющих операции с денежными средствами (третий уровень), и осуществляет выявление признаков легализации незаконных доходов» [258, с. 44].

б) Надзорные органы, которые осуществляют надзорные функции в отношении субъектов третьего уровня.

в) Субъекты финансового мониторинга (организации, осуществляющие операции с денежными средствами или иным имуществом).

При этом, автор подчеркивает, что понятие «субъекты финансового мониторинга» может иметь две трактовки. Согласно широкой трактовке, под субъектами финансового мониторинга следует понимать «любой уполномоченный орган или организацию, представленную на одном из трех уровней, так как любой из них выполняет ряд мер, направленных на противодействие отмыванию преступных доходов и финансированию терроризма» [258, с. 45]. В узком значении (тот, который используется в вышеприведенной модели) субъектами финансового мониторинга являются «уполномоченные организации, которые непосредственно осуществляют финансовый мониторинг, а именно постоянное наблюдение за клиентами и операциями на предмет выявления клиентов и операций, связанных с противодействием легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» [258, с. 45].

Прошунин М.М. также поднимает вопрос о необходимости выделения четвертого уровня в представленной им модели механизма мониторинга ПОД/ФТ в лице правоохранительных органов. Однако, автор резонно отмечает, что в данном случае имеет место уже не финансовый мониторинг, так как «отношения в сфере финансового мониторинга являются предметом правового регулирования финансового права, в свою очередь, деятельность правоохранительных органов регулируется уголовно-процессуальным правом» [258, с. 45].

Зубков В.А. и Осипов С.К. выделяют два уровня финансового мониторинга [6]:

а) Первичный финансовый мониторинг.

б) Государственный финансовый мониторинг.

В представленной авторами двухуровневой модели механизма мониторинга ПОД/ФТ к первому уровню отнесены организации и иные лица, осуществляющие

операции с денежными средствами и иным имуществом, а также принимающие участие в реализации данных операций.

Ко второму уровню механизма мониторинга ПОД/ФТ отнесены подразделение финансовой разведки, надзорные и иные государственные органы.

Схожая модель механизма мониторинга ПОД/ФТ содержится и в учебном пособии «Финансовый мониторинг», опубликованном под редакцией Чиханчина Ю.А. и Братко А.Г. [11], а также в статье Овчинникова О.П. и Аничкина И.М. [252].

Также можно выделить подход Едроновой В.Н. к описанию модели механизма мониторинга ПОД/ФТ, который отличается тем, что помимо выделения двух ранее упомянутых уровней (государственный финансовый мониторинг и корпоративный (он же первичный) финансовый мониторинг) автор отмечает, что государственный уровень финансового мониторинга «представлен двумя подуровнями:

а) федеральным уполномоченным органом – Росфинмониторингом и другими федеральными надзорными органами, важнейшим из которых в сфере ПОД/ФТ является Банк России;

б) межрегиональными управлениями (территориальными органами) Росфинмониторинга» [222, с. 50].

Иная структура механизма мониторинга ПОД/ФТ представлена Ващекиной И.В. (в оригинале – классификация «систем финансового мониторинга, осуществляющих деятельность по ПОД/ФТ», однако, анализ содержания классификации позволяет отнести уровни систем «финансового мониторинга, осуществляющих деятельность по ПОД/ФТ», к уровням механизма мониторинга ПОД/ФТ в силу схожести их смыслового наполнения с уровнями ранее представленных моделей) [213, с. 116]. Ващекина И.В. выделяет три уровня механизма мониторинга ПОД/ФТ:

а) «Объединения международного статуса» [213, с. 116].

б) «Национальные системы финансового мониторинга» [213, с. 116].

в) «Отдельные финансовые и коммерческие организации» [213, с. 116].

Соответственно, можно отметить, что все приведенные модели механизма мониторинга ПОД/ФТ имеют ряд общих элементов. Так, они предполагают разделение механизма мониторинга ПОД/ФТ на уровни по функционалу и масштабу деятельности субъектов механизма мониторинга ПОД/ФТ. Также все модели включают в себя микроуровень (он же первичный или корпоративный финансовый мониторинг) и национальный уровень.

При этом, несколько выделяется модель Прошунина М.М., который ПФР и надзорные органы разделяет в качестве разных уровней механизма мониторинга ПОД/ФТ. На авторский взгляд такое разделение является не совсем точным, так как уровневая классификация предполагает качественную и/или количественную разницу между субъектами, размещенными на разных уровнях. Отмечаем, что, масштабируя механизм мониторинга ПОД/ФТ от микроуровня организаций, являющихся субъектами антиотмывочного законодательства, надзорные органы и ПФР будут расположены относительно них на один уровень выше, так как подразделение финансовой разведки получает информацию от данных организаций, а надзорные органы контролируют точность и своевременность предоставления информации. При этом, отношения подчиненности между ПФР и надзорными органами могут быть установлены исключительно в силу административного устройства того или механизма мониторинга ПОД/ФТ, но не вытекают из их функционального назначения и масштаба деятельности (деятельность ПФР и надзорных органов осуществляется на всей территории страны, а их круг их полномочий требует осуществления взаимодействия между органами, но не подчинения одного из них другому).

Также отличительные особенности присутствуют в моделях механизма мониторинга ПОД/ФТ Едроновой В.Н. (где национальный уровень разделяется на два подуровня: федеральный и территориальный) и Ващекиной И.В. (добавлен международный уровень).

Таким образом, представленная в исследовании модель механизма мониторинга ПОД/ФТ отличается от ранее сформулированных авторами тем, что комплексно отображает структуру механизма мониторинга ПОД/ФТ, включая, как

микроуровень и национальный уровень (с выделением регионального уровня, обусловленного наличием территориальных органов у субъектов национального уровня), состоящий из блока подразделения финансовой разведки и блока органов финансового контроля, так и наднациональный уровень, включающий в себя международные координационные органы в сфере ПОД/ФТ.

Также сформулированная в исследовании модель отличается акцентом на процессы информационного взаимодействия между субъектами механизма мониторинга ПОД/ФТ. Контекст информационного взаимодействия участников механизма мониторинга ПОД/ФТ позволяет применительно к предмету исследования охарактеризовать представленную в исследовании модель механизма мониторинга ПОД/ФТ посредством анализа влияния на него организационно-технологических факторов трансформации механизма мониторинга ПОД/ФТ в условиях цифровизации экономики. С учетом рассмотренных ранее технологий цифровизации экономики данные факторы, по нашему мнению, возможно объединить в две группы, которые, в свою очередь, следует разделить на несколько подгрупп и сформулировать их следующим образом:

а) Факторы, способствующие развитию механизма мониторинга ПОД/ФТ:

1) «Повышение аналитических возможностей (увеличение скорости осуществления расчетов, автоматизация процесса контроля и др.).

2) Расширение возможностей по хранению информации и ее обработке (использование технологии блокчейн в целях осуществления распределенного хранения и обработки информации, применение технологии Big Data для обработки больших объемов информации).

3) Увеличение скорости обмена информации и объема передаваемых данных» [234, с. 8].

б) Факторы, затрудняющие реализацию механизма мониторинга ПОД/ФТ:

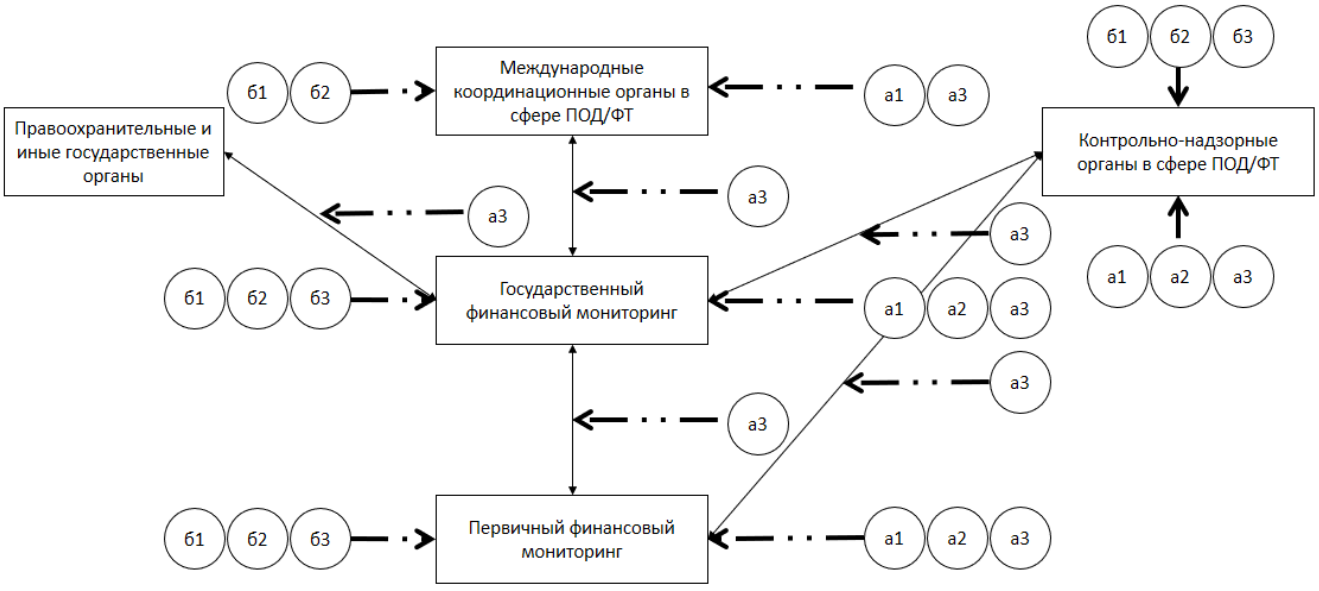
1) Появление новых технологий, способов, средств платежа и осуществления сделок, а также иных новшеств, влияющих на эффективное функционирование механизма мониторинга ПОД/ФТ, не охваченных требованиями антиотмывочного

законодательства (например, использование криптовалют, операции с которыми не отслеживаются в рамках национального механизма мониторинга ПОД/ФТ).

2) Использование технологий цифровой экономики в целях воспрепятствования осуществлению и реализации механизма мониторинга ПОД/ФТ (например, использование криптомиксеров для затруднения отслеживания криптовалютных транзакций даже в случае, если криптовалюты отслеживаются в рамках национального механизма мониторинга ПОД/ФТ).

3) Повышение требований к скорости осуществления и реализации процедур механизма мониторинга ПОД/ФТ, а также к аналитическим возможностям структурных звеньев механизма мониторинга ПОД/ФТ в силу увеличения скоростей проведения и роста объемов финансовых операций и сделок в условиях цифровизации экономики.

Модель функционирования механизма мониторинга ПОД/ФТ в контексте влияния на него организационно-технологических факторов трансформации механизма мониторинга ПОД/ФТ в условиях цифровизации экономики представлена на рисунке 7.



Источник: составлено автором.

Рисунок 7 – Модель механизма мониторинга противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма в контексте влияния на него организационно-технологических факторов трансформации механизма мониторинга ПОД/ФТ в условиях цифровизации экономики

Все вышеуказанные организационно-технологические факторы трансформации механизма мониторинга ПОД/ФТ в условиях цифровизации экономики свое отражение находят в рамках как микроуровня, так и национального, а также наднационального уровней механизма мониторинга ПОД/ФТ. Рассматривая, факторы, способствующие развитию механизма мониторинга ПОД/ФТ, стоит отметить, что «для субъектов первичного финансового мониторинга актуально увеличение скорости обмена информацией за счет применения цифровых технологий в рамках взаимодействия с клиентами, а также в процессе осуществления взаимодействия между структурными подразделениями по вопросу осуществления внутреннего контроля на предмет выявления операций, связанных с ОД/ФТ. Расширение возможностей по хранению и обработке информации, а также повышение аналитических мощностей субъектам микроуровня механизма мониторинга ПОД/ФТ необходимо для осуществления оперативного и качественного анализа информации о проводимых финансовых операциях и заключаемых сделках в целях выявления тех из них, которые могут быть связаны с ОД/ФТ.

Аналогичная потребность существует у подразделения финансовой разведки с тем дополнением, что увеличение скорости обмена информацией необходимо для повышения оперативности взаимодействия между региональными подразделениями ПФР, а требования к аналитическим мощностям, возможностям по хранению и обработке информации выше в связи с тем, что субъект национального уровня механизма мониторинга ПОД/ФТ агрегирует информацию от множества субъектов первичного финансового мониторинга» [234, с. 9]. Схожий набор организационно-технологических факторов трансформации механизма мониторинга ПОД/ФТ в условиях цифровизации экономики применим и в отношении органов финансового контроля с тем дополнением, что расширение возможностей по хранению и обработке информации, а также повышение аналитических возможностей необходимо в целях совершенствования контроля за соблюдением требований антиотмывочного законодательства.

В деятельности международных координационных органов в сфере ПОД/ФТ наибольшее значение имеют факторы повышения аналитических возможностей по анализу поступающей информации (например, в части автоматизации их анализа) и ускорения процесса информационного взаимодействия. Фактор хранения и обработки значительных объемов информации в деятельности международных координационных органов играет меньшую роль в связи с тем, что в рамках такой деятельности используется преимущественно агрегированная и абстрагированная информация от национальных ПФР и отсутствует необходимость хранить поступившие от субъектов первичного финансового мониторинга данные о совершенных финансовых операциях и сделках.

На качество, скорость и эффективность взаимодействия между субъектами микроуровня, национального и наднационального уровней механизма мониторинга ПОД/ФТ, взаимодействия между субъектами первичного финансового мониторинга и органами финансового контроля, а также между подразделением финансовой разведки и правоохранительными органами непосредственное влияния оказывают организационно-технологические факторы трансформации механизма мониторинга ПОД/ФТ в условиях цифровизации экономики, способствующие повышению скорости обмена информацией.

В части факторов, затрудняющих реализацию механизма мониторинга ПОД/ФТ, подгруппы факторов, связанные с использованием технологий цифровой экономики в целях воспрепятствования осуществлению и реализации механизма мониторинга ПОД/ФТ, а также связанные с появлением новых технологий, способов, средств платежа и осуществления сделок и иных новшеств, являются актуальными для всех уровней механизма мониторинга ПОД/ФТ, так как требуют учета в деятельности субъектов первичного финансового мониторинга, выработки соответствующих нормативно-правовых, организационно-технических и методических решений со стороны субъектов национального уровня механизма мониторинга ПОД/ФТ, а также агрегирования информации от ПФР о данных факторах и выработки универсальных рекомендаций со стороны субъектов наднационального уровня механизма мониторинга ПОД/ФТ.

Подгруппа факторов трансформации механизма мониторинга ПОД/ФТ, связанная с повышением требований к скорости осуществления и реализации процедур механизма мониторинга ПОД/ФТ, а также к аналитическим возможностям структурных звеньев механизма мониторинга ПОД/ФТ, имеет наибольшую актуальность для микроуровня и национального уровня механизма мониторинга ПОД/ФТ, так как от учета данных факторов зависит конкурентоспособность, как отдельных организаций, осуществляющих финансовые операции и сделки, так и всей финансовой системы страны, в целом.

Таким образом, цифровизация и развитие информационно-коммуникационных технологий оказывает значительное влияние на функционирование механизма мониторинга противодействия отмыванию преступных доходов и финансированию терроризма. «Это выражается в сокращении сроков предоставления информации о подозрительных операциях в ПФР, повышении возможностей подразделений финансовой разведки по обработке поступаемой от организаций сообщений, повышении эффективности процесса межведомственного взаимодействия.

Однако, цифровизация экономики не только способствует развитию механизма мониторинга ПОД/ФТ, но и повышает требования к нему в силу повышения количества и скорости осуществляемых финансовых операций. Появились и получили популярность различные криптовалюты, затрудняющие отслеживание переводов между двумя субъектами, как в силу невозможности в ряде случаев идентифицировать получателя и отправителя цифровых финансовых активов, так и из-за использования некоторыми провайдерами услуг перевода криптовалют специальных сервисов, предназначенных для затруднения отслеживания транзакций (например, «миксеров» - программного обеспечения, смешивающего между собой несколько транзакций, а затем в дальнейшем разбивающим их на исходные суммы). В целях решения проблем обработки и анализа увеличивающегося объема информации подразделения финансовой разведки и подразделения внутреннего контроля финансовых организаций внедряют в свою деятельность технологии BigData и искусственного интеллекта.

Необходимость повышения эффективности и скорости отслеживания подозрительных операций, а также возрастающее требование к ресурсам может подтолкнуть к сближению микроуровень механизма мониторинга ПОД/ФТ с национальным уровнем в целях в определенной степени интеграции их информационных ресурсов, вплоть до слияния первичного и государственного финансового мониторинга в единый уровень механизма мониторинга ПОД/ФТ» [234, с. 10].

1.3 Определение роли и места механизма мониторинга противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма в системе обеспечения экономической безопасности государства в условиях цифровизации экономики

Легализация доходов, полученных преступным путем, не только позволяет лицам, совершившим преступления, уходить от ответственности за преступные деяния, но и использовать полученные в результате своей незаконной деятельности доходы в экономическом обороте. При этом создается ситуация, когда лица, осуществляющие свою деятельность в соответствии с правовыми предписаниями, в условиях рыночной конкуренции по сравнению с предприятиями, получающими ресурсы за счет осуществления противоправной деятельности, оказываются в заранее проигрышном положении, так как доходность криминальной деятельности не только, как правило, превышает маржинальность легального бизнеса, но и находится в теневом секторе экономики, не связана требованиями государственного регулирования и, соответственно, не облагается налогами и сборами [208]. Это позволяет лицам, использующим доход от криминальной деятельности в легальном экономическом обороте, получать преимущества над своими законопослушными конкурентами, «выдавливать» их с рынка, как законными, так и незаконными способами.

Такая ситуация создает непосредственную угрозу экономической безопасности государства, особенно в условиях нарастающих процессов деглобализации в мировой экономике и применения недружественными странами ограничительных мер в отношении Российской Федерации, направленных, в том числе, на затруднение доступа к высокотехнологичным товарам, что приводит к необходимости развития опережающими темпами отечественного производства высокотехнологичной продукции с целью недопущения влияния ограничительных мер на национальную безопасность страны. Потребность в развитии производства высокотехнологичной продукции и осуществлении цифровизации экономики порождает необходимость принятия мер поддержки предпринимателей, осуществляющих деятельность в данных областях, и обеспечения условий для развития предпринимательских инициатив. Это, в свою очередь, актуализирует важность осуществления контроля за эффективностью и законностью расходования бюджетных средств, выделенных в рамках вышеуказанных мер поддержки, недопущения хищения и последующей легализации данных средств, а также обеспечения общей декриминализации экономики. Выполнению данных задач и, соответственно, обеспечению экономической безопасности государства в условиях цифровизации экономики призван способствовать механизм мониторинга ПОД/ФТ [1].

Само понятие «экономическая безопасность» получило достаточно широкое нормативное и доктринальное применение. Так, согласно Стратегии экономической безопасности Российской Федерации на период до 2030 года, утвержденной Указом Президента Российской Федерации от 13 мая 2017 года № 208, под экономической безопасностью понимается «состояние защищенности национальной экономики от внешних и внутренних угроз, при котором обеспечиваются экономический суверенитет страны, единство ее экономического пространства, условия для реализации стратегических национальных приоритетов Российской Федерации» [43]. Доктринально понятие «экономическая безопасность» имеет множество определений, которые, однако, можно разделить на три подхода [14].

Сторонники первого подхода приводят наиболее близкое к нормативному определение и характеризуют экономическую безопасность как состояние защищенности экономики государства, позволяющее обезопасить его жизненно важные интересы. Сторонником такого подхода являлся, в частности, Вячеслав Константинович Сенчагов, который сущность экономической безопасности раскрывал, как «такое состояние экономики и институтов власти, при котором обеспечивается гарантированная защита национальных интересов, социально направленное развитие страны в целом, достаточный оборонный потенциал даже при наиболее неблагоприятных условиях развития внутренних и внешних процессов» [15, с. 72].

Сторонники второго подхода рассматривают экономическую безопасность, как совокупность условий, защищающих хозяйство страны от внешних и внутренних угроз. Так, сторонник данного подхода Леонид Иванович Абалкин приводил следующее определение экономической безопасности – «совокупность условий и факторов, обеспечивающих независимость национальной экономики, ее стабильность и устойчивость, способность к постоянному обновлению и совершенствованию» [199, с. 12].

В рамках третьего подхода экономическая безопасность рассматривается, как «способность экономики обеспечивать эффективное удовлетворение общественных потребностей на межнациональном и международном уровнях» [14, с. 35]. Сторонниками данного подхода являются, в частности, А. Архипов и А. Городецкий.

Составляющими экономической безопасности являются [14]:

– технико-производственная;

– технологическая;

– энергетическая;

– экологическая;

– валютно-кредитная;

– сырьевая;

– продовольственная;

– информационная.

В рамках данного научного исследования интерес представляет валютно-кредитная составляющая экономической безопасности, в той ее части, которая касается организации стабильного функционирования национальной финансовой системы. В то же время от стабильного функционирования финансовой системы также зависят и технико-производственная (в части обеспечения необходимых финансовых ресурсов для выпуска продукции, обеспечения функционирования производственных фондов, их модернизации), технологическая (в части привлечения инвестиций в технологические отрасли экономики страны, обеспечения необходимых условий для развития отечественных технологических проектов, в том числе, связанных с использованием цифровых технологий), а также иные составляющие экономической безопасности. В свою очередь, на обеспечение стабильного функционирования национальной финансовой системы непосредственное влияние оказывает способность государства противостоять теневой экономике, противодействовать отмыванию преступных доходов и финансированию терроризма.

Так, в вышеупомянутой Стратегии экономической безопасности Российской Федерации на период до 2030 года в числе вызовов и угроз экономической безопасности перечисляются «высокий уровень криминализации и коррупции в экономической сфере» и «сохранение значительной доли теневой экономики» [43]. Также легализация преступных доходов и финансирование терроризма связаны со следующими вызовами и угрозами экономической безопасности Российской Федерации:

– «повышение конфликтного потенциала в зонах экономических интересов Российской Федерации, а также вблизи ее границ» (чему непосредственно способствует финансирование терроризма);

– «подверженность финансовой системы Российской Федерации глобальным рискам (в том числе в результате влияния спекулятивного иностранного капитала), а также уязвимость информационной инфраструктуры финансово-банковской

системы» (что, помимо прочего, может быть обусловлено использованием финансовой системы Российской Федерации в целях отмывания преступных доходов);

– «недостаточный объем инвестиций в реальный сектор экономики, обусловленный неблагоприятным инвестиционным климатом, высокими издержками бизнеса, избыточными административными барьерами, неэффективной защитой права собственности» (негативное влияние на процесс инвестирования в Российской Федерации в реальный сектор экономики могут оказывать опасения инвесторов, связанные с рисками криминального характера, включая рейдерство, хищение вложенных инвестиций и иные виды противоправной деятельности в сфере экономики, которые зачастую предполагают легализацию доходов, или придание правомерного вида тем или иным операциям и сделкам, имеющим фиктивный характер; также негативное влияние на объем и качество инвестиций их государственных и муниципальных денежных фондов оказывает коррупция, которая также предполагает отмывание похищенных бюджетных средств [207]);

– «слабая инновационная активность, отставание в области разработки и внедрения новых и перспективных технологий (в том числе технологий цифровой экономики), недостаточный уровень квалификации и ключевых компетенций отечественных специалистов» (связь с ОД/ФТ аналогична предыдущему пункту);

– «низкие темпы экономического роста, обусловленные внутренними причинами, в том числе ограниченностью доступа к долгосрочным финансовым ресурсам, недостаточным развитием транспортной и энергетической инфраструктуры» (чему также может способствовать хищение бюджетных средств и их последующая легализация);

– «несбалансированность национальной бюджетной системы» (аналогично предыдущему пункту);

– «недостаточно эффективное государственное управление» (аналогично предыдущему пункту) [43].

В Стратегии экономической безопасности Российской Федерации на период до 2030 года перечислены основные направления государственной политики в сфере обеспечения экономической безопасности, к которым отнесены:

– «развитие системы государственного управления, прогнозирования и стратегического планирования в сфере экономики;

– обеспечение устойчивого роста реального сектора экономики;

– создание экономических условий для разработки и внедрения современных технологий, стимулирования инновационного развития, а также совершенствование нормативно-правовой базы в этой сфере;

– устойчивое развитие национальной финансовой системы;

– сбалансированное пространственное и региональное развитие Российской Федерации, укрепление единства ее экономического пространства;

– повышение эффективности внешнеэкономического сотрудничества и реализация конкурентных преимуществ экспортно-ориентированных секторов экономики;

– обеспечение безопасности экономической деятельности;

– развитие человеческого потенциала» [43].

Эффективная работа механизма мониторинга ПОД/ФТ, а также его трансформация в соответствии с требованиями времени непосредственно связаны с решением следующих задач по реализации вышеперечисленных направлений обеспечения экономической безопасности Российской Федерации:

а) В рамках направления, касающегося развития системы государственного управления, прогнозирования и стратегического планирования в сфере экономики:

1) … «принятие комплекса дополнительных мер, направленных на деофшоризацию национальной экономики» …;

2) … «совершенствование деятельности контрольно-надзорных органов, в том числе на основе широкого внедрения риск-ориентированного подхода и развития практики страхования ответственности субъектов экономической деятельности» …;

3) «борьба с нецелевым использованием и хищением государственных средств, коррупцией, теневой и криминальной экономикой» [43].

б) В рамках направления, касающегося устойчивого развития национальной финансовой системы:

1) … «противодействие переводу безналичных денежных средств в теневой оборот наличных денежных средств и легализации доходов, полученных преступным путем от предикатных экономических преступлений» [43].

в) В рамках, направления касающегося обеспечения безопасности экономической деятельности:

1) … «создание условий, исключающих возможность сращивания интересов должностных лиц бизнес-структур и представителей государственных органов, профилактика и предупреждение формирования коррупционных схем их взаимодействия, в том числе с участием в этих схемах представителей бизнеса иностранных государств» …;

2) … «повышение уровня безопасности и антитеррористической защищенности критически важных и потенциально опасных объектов» [43].

По мнению С.П. Колтовича, отмывание денег может «отрицательно влиять на валюты и процентные ставки, поскольку лица, отмывающие свои доходы, реинвестируют средства в те области, где менее вероятно раскрытие их схем, а не в те, где выше норма отдачи» [240, с. 79]. Также подчеркивается, что легализация доходов «может увеличивать угрозу валютной нестабильности ввиду неправильного распределения ресурсов, обусловленного деформациями в ценах на активы и товары» [240, с. 79].

При этом, в научных источниках отмечается сложность количественной оценки влияния отмывания преступных доходов на экономику государства и указывается на то, что данное явление оказывает негативное воздействие не столько на отдельные экономические параметры, сколько на нормальное функционирование финансовых институтов и национальной экономики, в целом [215]. Однако, данное негативное воздействие имеет проявления в рамках отдельных экономических показателей. Так, одним из способов отмывания

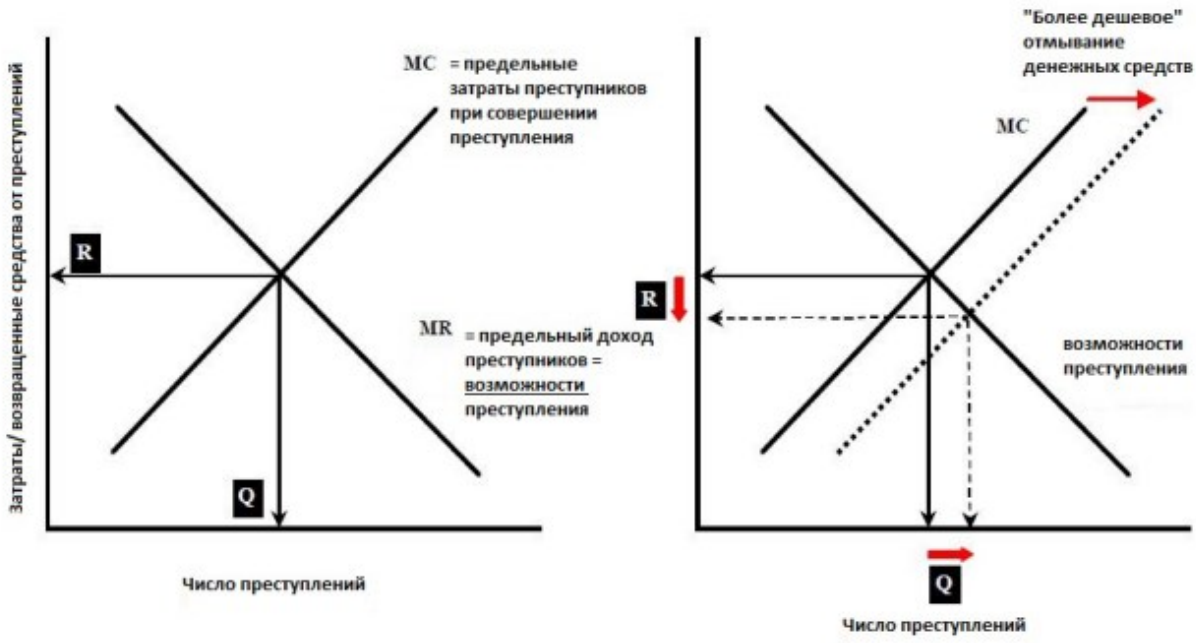
преступных доходов и финансирования терроризма является вывод капитала за границу по фиктивным основаниям (например, по поддельным договорам о поставке продукции/оказании услуг, по договорам о покупке недвижимости в отсутствии такого факта либо по завышенной цене и так далее). В связи с этим фиксируется связь между объемом оттока капитала из страны и снижением национального ВВП, что, в свою очередь, приводит к повышению безработицы [269].

Отсутствие или недостаточный уровень противодействия отмыванию преступных доходов с очевидностью будет способствовать снижению издержек осуществления криминальной деятельности, снижать риски обнаружения преступной деятельности (осуществляемой, в том числе, в цифровом пространстве). Особую опасность такая ситуация представляет в связи с тем, что, как было указано выше, легализация денежных средств используется преимущественно организованными преступными группировками (в частности, при торговле наркотическими средствами, оружием, контрафактной продукцией, хищении бюджетных средств, краже денежных средств с использованием инфокоммуникационных технологий и т.д.), деятельность которых создает непосредственную угрозу росту рождаемости, повышения продолжительности жизни населения, обеспечению общественной безопасности, обеспечению функционирования системы государственного управлению, экономическому развитию государства, наконец, и самому существованию государства [51].

В научных источниках отмечается, что непосредственную угрозу экономической безопасности создает также терроризм (и финансирование терроризма, в частности) [4]. При этом, в условиях цифровизации экономики общественная опасность финансирования терроризма только возрастает в силу того, что для осуществления данного преступления требуется только иметь мобильное устройство и доступ к сети Интернет. О разрушающем влиянии, которое оказывает терроризм на экономику говорится и в Стратегии партнерства государств и бизнеса в противодействии терроризму, принятой на Глобальном форуме по партнерству государств и бизнеса в противодействии терроризму,

состоявшемся 30 ноября 2006 года в Москве [176]. В стратегии указывается, что в качестве одного из ведущих направлений противодействия терроризму должно рассматриваться обеспечение экономической безопасности.

Взаимосвязь уровня преступности с затратами на совершение преступных деяний (в которые, в том числе, входят расходы на легализацию полученных в криминальной деятельности денежных средств или иного имущества) представлена на рисунке 8.



Источник: составлено [254].

Рисунок 8 – Взаимосвязь уровня преступности с затратами на совершение преступных деяний

Правый график демонстрирует возможность увеличения уровня преступности при снижении издержек на совершение преступной деятельности, что возможно, в том числе, при снижении затрат на легализацию доходов, полученных преступным путем. Таким образом, эффективность функционирования механизма мониторинга ПОД/ФТ оказывает непосредственное влияние на уровень преступности и степень криминализации экономики.

Отдельного внимания заслуживает влияние на экономическую безопасность государства рейтингов ФАТФ. ФАТФ регулярно проводит оценку соответствия национальных систем ПОД/ФТ (и механизмов мониторинга ПОД/ФТ, в частности) разработанным Группой рекомендациям. В случае если страна не соблюдает рекомендации по противодействию отмыванию доходов и финансированию

терроризма ФАТФ включает государство в специализированные списки: «черный список» и «серый список» ФАТФ.

В отношении стран, у которых имеются «стратегические недостатки в области противодействия отмыванию доходов, финансированию терроризма и финансированию распространения оружия массового уничтожения» ФАТФ призывает все юрисдикции применять повышенные меры надлежащей проверки клиентов, а в отдельных случаях применять «контрмеры для защиты международной финансовой системы от исходящих от такого государством рисков ОД/ФТ/ФРОМУ» [278]. Такие государства включаются в «черный список» ФАТФ, который иначе называется «Юрисдикции с высоким уровнем риска, в отношении которых действует призыв к действию».

Также существует список «Юрисдикций, находящихся под усиленным мониторингом» (или «серый список» ФАТФ). Находящиеся в таком списке государства несмотря на наличие стратегических недостатков в сфере ПОД/ФТ/ФРОМУ взяли на себя обязательства оперативно устранить данные недостатки в установленные сроки. В отношении данных государства применяется усиленный мониторинг.

Включение страны в «черный список» и «серый список» ФАТФ может иметь существенное негативное влияние на национальную экономику. Указанные выше ограничения означают затруднение процесса осуществления транзакций в отношении клиентов и финансовых институтов из государств, включенных в перечни. Связано это с увеличением сроков проведения процедур надлежащей проверки клиентов, а также с расширением количества запрашиваемых документов. В отношении клиентов из стран, включенных в «черный список» ФАТФ, возможна блокировка проводимых операций. Тогда как, включение государства в «серый список» по подсчетам экспертов Международного валютного фонда (далее – МВФ) приводит к снижению в среднем притока капитала в страну на 7,6% ВВП, притока прямых иностранных инвестиций на 3% ВВП, притока портфельных инвестиций на 2,9% ВВП, иных видов инвестиций на 3,6% ВВП [239]. Также по результатам анализа, проведенного Колин, Кук и Сорамаки,

количество платежей, отправляемых в адрес страны, включенной в «серый список» ФАТФ сокращается на 7-10% (цитируется по [239]).

Стоит отметить, что потенциальный негативный эффект от включения в списки ФАТФ для российской экономики в последнее время уменьшился в связи с введением в отношении Российской Федерации США, государствами-членами ЕС и рядом иных стран санкций. Помимо ожидаемого сокращения объема двухстороннего финансового потока с государствами-инициаторами санкций, ограничительные меры в некоторых случаях также негативно сказываются на процессе осуществления транзакций между финансовыми организациями из России и третьих стран в связи с опасениями последних попасть под действие санкционных ограничений [66; 87]. В то же время, действующие санкции в отношении Российской Федерации введены в одностороннем порядке в нарушение норм международного права, в связи с чем у стран, не вводивших антироссийские санкции, отсутствуют обязательства по ужесточению контроля и блокировке финансовых операций из России (мотивом чего могут служить только опасения попасть под вторичные санкции США и их союзников). Кроме того, антироссийские санкции на момент написания исследования не носят всеобъемлющий характер в отношении российского финансового сектора, по сравнению со списками ФАТФ. В связи с вышеизложенным можно отметить, что включение России в «черный список» ФАТФ и «серый список» ФАТФ несмотря на действующие в отношении Российской Федерации санкционные ограничения все еще может оказать негативное влияние на национальную экономику.

Таким образом, отмывание доходов и финансирование терроризма оказывает комплексное прямое и опосредованное (в виде включения государства в списки ФАТФ) негативное влияние на состояние национальной экономики [229]. Помимо повышения уровня криминализации общества отмывание доходов, полученных преступным путем, и финансирование терроризма также нарушают стабильное функционирование финансовой системы, препятствуют развитию реального сектора экономики, способствуют разрастанию теневой экономики, что, в конечном итоге, может привести к эрозии государственного управления

(составлено на основе результатов, полученных совместно с Кравченко С.И. [233]). Особую общественную опасность в Российской Федерации имеет финансирование терроризма, которое по самой своей сути бросает вызов существованию государства и целостности российского общества. В связи с этим, ПОД/ФТ стоит рассматривать, как важную составную часть обеспечения экономической безопасности государства.

Выводы по 1 главе

В рамках первой главы диссертационного исследования проведен сравнительный анализ существующих подходов к определению термина отмывания (легализации) преступных доходов и составлена классификация интерпретаций понятия, в соответствии с которой трактовки отмывания (легализации) доходов, полученных преступным путем, можно разделить на четыре типа: результирующие, процессные, операционные и комплексные. В ходе анализа выявлено, что большинство имеющихся определений тяготеют к юридическому дискурсу, в связи с чем существует необходимость выработки экономической трактовки понятия отмывания преступных доходов, которая, по-нашему мнению, заключается в комбинировании результирующей составляющей отмывания доходов (перевод доходов, полученных преступным путем, из теневого сектора экономики в легальный, создание условий для использования преступных доходов в рамках экономической системы) и процедурной составляющей (осуществление финансовых операций, гражданско-правовых сделок и иных действий, направленных на размещение полученных преступных доходов в финансовой системе, их расслоение, а затем интеграцию) [230].

В части определения понятия финансирования терроризма применительно к данной работе релевантным является определение, закрепленное в ст. 3 Федерального закона «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», согласно которому к финансированию терроризма следует отнести «предоставление или

сбор средств либо оказание финансовых услуг с осознанием того, что они предназначены для финансирования организации, подготовки и совершения хотя бы одного из преступлений, предусмотренных статьями 205; 205.1; 205.2; 205.3; 205.4; 205.5; 206; 208; 211; 220; 221; 277; 278; 279; 360 и 361 Уголовного кодекса Российской Федерации, либо для финансирования или иного материального обеспечения лица в целях совершения им хотя бы одного из указанных преступлений, либо для обеспечения организованной группы, незаконного вооруженного формирования или преступного сообщества (преступной организации), созданных или создаваемых для совершения хотя бы одного из указанных преступлений» [34]. Достаточность правового определения обусловлена правовой природой разделения финансовых операций и услуг, связанных с финансированием терроризма, от иных финансовых операций и услуг, в связи с наличием в деятельности лиц, осуществляющих первые, умысла на оказание финансирования организации и совершения одного из преступлений, перечисленных в ст. 3 Закона № 115-ФЗ, либо для материального обеспечения групп лиц, созданных для совершения хотя бы одного из указанных преступлений.

Также выявлена слабая научная разработанность понятия «механизм мониторинга ПОД/ФТ», зачастую выражающаяся в его объединении с термином «механизм ПОД/ФТ», что, наряду с выявленным дефицитом экономических трактовок понятия «механизм ПОД/ФТ», потребовало выработки с учетом имеющихся определений механизма ПОД/ФТ (склонных к правовым областям научного знания), а также на основе ранее приведенных определений отмывания преступных доходов и финансирования терроризма экономической трактовки противодействия ОД/ФТ, а также механизма ПОД/ФТ. Механизм ПОД/ФТ с экономической точки зрения раскрывается, как «опосредованная международными и национальными нормами права и созданная в целях обеспечения экономической безопасности государства система организации деятельности субъектов противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, заключающейся в выявлении и пресечении потоков денежных средств и иных активов, связывающих теневую и легальную

экономику, а также потоков денежных средств и иных активов, направленных на обеспечение деятельности террористических организаций или на содействие в организации и осуществлении преступлений террористической направленности» [232, с. 46].

Механизм мониторинга ПОД/ФТ можно охарактеризовать, как составную часть «механизма ПОД/ФТ, в рамках которой на основании анализа информации о проводимых финансовых операциях и заключаемых сделках осуществляется выявление операций, связанных с легализацией (отмыванием) доходов, полученных преступным путем, или финансированием терроризма, результаты чего передаются в правоохранительные и иные государственные органы в целях принятия ими мер, направленных на противодействие легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» [234, с. 6].

С учетом представленных определений сформирована модель функционирования механизма мониторинга ПОД/ФТ с позиции информационного взаимодействия его участников, разделенных на следующие уровни:

а) «Микроуровень механизма мониторинга ПОД/ФТ:

1) структурные подразделения и должностные лица организаций, осуществляющих операции с денежными средствами или иным имуществом, а также иные организации и лица, в чьи обязанности входит проверка клиентов и операций на соответствие требованиям законодательства в сфере ПОД/ФТ (первичный финансовый мониторинг).

б) Национальный уровень механизма мониторинга ПОД/ФТ (включает в себя также региональный уровень, обусловленный структурой территориальных подразделений субъектов национального уровня механизма мониторинга ПОД/ФТ):

1) подразделение финансовой разведки (государственный финансовый мониторинг);

2) органы финансового контроля, осуществляющие контроль (надзор) за соблюдением требований законодательства в сфере ПОД/ФТ.

в) Наднациональный уровень механизма мониторинга ПОД/ФТ:

1) международные координационные органы в сфере ПОД/ФТ» [234, с. 6].

На основе сформированной модели функционирования механизма мониторинга ПОД/ФТ с учетом представленных в первой главе подходов к определению цифровизации экономики автором выделены следующие группы организационно-технологических факторов трансформации механизма мониторинга ПОД/ФТ в условиях цифровизации экономики:

а) Факторы, способствующие развитию механизма мониторинга ПОД/ФТ:

1) «Повышение аналитических возможностей (увеличение скорости осуществления операций, автоматизация процесса контроля и др.).

2) Расширение возможностей по хранению информации и ее обработке (использование технологии блокчейн в целях осуществления распределенного хранения и обработки информации, применение технологии Big Data для обработки больших объемов информации).

3) Увеличение скорости обмена информации» [234, с. 8].

б) Факторы, затрудняющие реализацию механизма мониторинга ПОД/ФТ:

1) Появление новых технологий, способов, средств платежа и осуществления сделок, а также иных новшеств, влияющих на эффективное функционирование механизма мониторинга ПОД/ФТ, не охваченных требованиями антиотмывочного законодательства (например, использование криптовалют, операции с которыми не отслеживаются в рамках национального механизма мониторинга ПОД/ФТ).

2) Использование технологий цифровой экономики в целях воспрепятствования осуществлению и реализации механизма мониторинга ПОД/ФТ (например, использование криптомиксеров для затруднения отслеживания криптовалютных транзакций даже в случае, если криптовалюты отслеживаются в рамках национального механизма мониторинга ПОД/ФТ).

3) Повышение требований к скорости осуществления и реализации процедур механизма мониторинга ПОД/ФТ, а также к аналитическим возможностям структурных звеньев механизма мониторинга ПОД/ФТ в силу увеличения

скоростей проведения и роста объемов финансовых операций и сделок в условиях цифровизации экономики.

Важность противодействия отмыванию доходов, полученных преступным путем, и финансированию терроризма обусловлена, помимо прочего, негативным влиянием оказываемым данными процессами на экономическую безопасность государства, что выражается в повышении конфликтного потенциала, как в самой Российской Федерации, так и в зоне ее экономических интересов, дестабилизации финансовой системы, снижении объемов инвестиций, направляемых в реальный сектор экономики, а также инновационного потенциала экономики Российской Федерации, разбалансировании бюджетной системы России.

Несмотря на отмечаемую в научных источниках затруднительность количественной оценки отмывания преступных доходов на экономическую безопасность государства отслеживается взаимосвязь между ростом безработицы в стране и объемом оттока капитала из государства (что является одним из способов легализации доходов).

Также проведенные исследования указывают еще на то, что на экономическую безопасность государства оказывают непосредственное влияние и рейтинги, публикуемые ФАТФ, в части соблюдения странами рекомендаций организации по ПОД/ФТ. По подсчетам экспертов включение государства в «серый список» ФАТФ приводит к снижению в среднем притока капитала в страну на 7,6% ВВП, а количества платежей, отправляемых в адрес страны – на 7-10%.

Глава 2

Анализ функционирования механизма мониторинга противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма в условиях цифровизации экономики

2.1 Исследование международного опыта становления механизма мониторинга противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма

Механизм мониторинга противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, как указывалось ранее, связан с деятельностью государственных органов, а также организаций, в чьи обязанности входит проверка клиентов и операций на соответствие требованиям законодательства в сфере ПОД/ФТ (в первую очередь, кредитных организаций). При этом, одна из ключевых ролей в механизме мониторинга ПОД/ФТ принадлежит субъектам первичного финансового мониторинга, в целом, и кредитным организациям, в частности. Закономерно, что один из первых международных правовых актов в сфере ПОД/ФТ относится к деятельности банков по противодействию отмыванию преступных доходов.

В декабре 1988 года Базельским комитетом по банковском надзору (далее – БКБН) была принята Декларация о предотвращении преступного использования банковской системы для отмывания денег [299]. Декларация, не являющаяся предписывающим документом, а относящаяся к «мягкому» праву (то есть рекомендательного характера), впервые на международном уровне предоставила определение термину «отмывание доходов», а также указала на возможность использования банков в целях перемещения денежных средств, полученных в результате преступной деятельности. В Декларации отмечается о том, что от отмывания преступных доходов могут пострадать сами банки, чьей репутации и

материальном благополучию будет нанесен ущерб. В связи с этим Базельский комитет по банковскому надзору счел необходимым выработать стандарты этического поведения работников банковской сферы. По замыслу БКБН Декларация о предотвращении преступной использованию банковской системы для отмывания денег должна была стать основополагающим документом для руководства банков на основе которого осуществлялась бы разработка внутренней политики. Декларация призывает кредитные организации:

– осуществлять идентификацию клиента;

– препятствовать операциям, в отношении которых есть обоснованные предположения о связи с отмыванием преступных доходов;

– взаимодействовать с правоохранительными органами, а также препятствовать попыткам клиентов ввести в заблуждение правоохранительные органы.

Стоит отметит, что еще в Рекомендации Совета Европы от 27 июня 1980 г. (R (80)101) отмечалось, что банковская система может играть значительную роль в борьбе с легализацией преступных доходов (цитируется по [6]).

Первым актом международного жесткого права в сфере ПОД/ФТ принято считать Венскую конвенцию ООН, заключенную 20.12.1988. Участниками Венской конвенции являются 191 государство (включая Российскую Федерацию). В конвенции, как отмечают В.А. Зубков и С.К. Осипов, по сути, содержится определение отмывания преступных доходов, хоть сам термин и не фигурирует в тексте Венской конвенции [6]. Так, согласно ст. 3 Венской конвенции, страны обязуются принять меры, чтобы признать уголовными преступлениями, помимо прочих, следующие деяния:

– «конверсию или перевод собственности, если известно, что такая собственность получена в результате любого правонарушения или правонарушений, признанных таковыми (Венской конвенцией – примечание автора) …, в целях сокрытия или утаивания незаконного источника собственности или в целях оказания помощи любому лицу, участвующему в совершении такого

правонарушения или правонарушений, с тем чтобы он мог уклониться от ответственности за свои действия»;

– «сокрытие или утаивание подлинного характера, источника, местонахождения, способа распоряжения, перемещения, подлинных прав в отношении собственности или ее принадлежности, если известно, что такая собственность получена в результате правонарушения или правонарушений, признанных таковыми (Венской конвенцией – примечание автора)» [19].

Кроме того, в конвенции признается преступным «приобретение, владение или использование собственности, если в момент ее получения было известно, что такая собственность получена в результате правонарушения или правонарушений, признанных таковыми (Венской конвенцией – примечание автора)» [19].

Помимо обязанности признать уголовно наказуемым деянием легализацию доходов, полученных преступным путем, Венская конвенция обязует страны-участницы принять меры по конфискации доходов, полученных в результате совершения указанных в конвенции правонарушений, или стоимости, эквивалентной данным доходам. Согласно ст. 5 Венской конвенции каждая страна «принимает также такие меры, которые могут потребоваться, с тем чтобы ее компетентные органы могли определить, выявить и заморозить или арестовать доходы, собственность, средства или любые другие предметы (доходы, полученные преступным путем, или наркотические и психотропные вещества, а также оборудование для их производства – примечание автора) … с целью последующей конфискации» [19]. Венская конвенция обязывает государства предоставлять полномочия судам и компетентным органам арестовывать финансовую и коммерческую документацию, игнорируя требования о сохранности банковской тайны.

В июле 1989 года в Париже по инициативе глав правительств «Большой семерки» (G7) была создана ФАТФ, ставшая ведущим международным стандартизирующим органом в сфере ПОД/ФТ [6]. Задачей ФАТФ стала оценка международного сотрудничества в сфере противодействия использованию

финансовой системы в целях отмывания доходов, полученных в результате незаконного оборота наркотиков.

На состоявшемся в 1990 году саммите G7 был одобрен представленный ФАТФ отчет, содержащий 40 рекомендаций по борьбе с отмыванием доходов, вырученных от продажи наркотических средств. Данные рекомендации стали основой Международных стандартов по противодействию отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения ФАТФ, содержащих в себе меры ПОД/ФТ, подлежащие имплементации в национальные законодательства.

Первые 40 рекомендаций ФАТФ не содержали определения отмывания доходов (как не содержат его и дальнейшие модификации рекомендаций ФАТФ) и являлись своеобразным продолжением Венской конвенции ООН, но включали ряд положений, относящихся к деятельности банков, а также небанковских финансовых организаций. Так, в рекомендации 12 содержался запрет на открытие анонимных счетов. В рекомендации 13 отмечалось, что финансовые организации должны принимать «разумные меры» к определению, действительно ли лицо, открывшее счет и осуществляющее операции, действует от своего имени. В рекомендации 14 содержалась обязанность финансовых организаций сохранять в течение, как минимум, 5 лет информацию о совершенных операциях. Также предписывалось в течение тех же 5 лет после закрытия счета хранить информацию, позволяющую идентифицировать владельца счета [296].

Рекомендации ФАТФ содержали, кроме того, нормы, указывающие на необходимость финансовым организациям обращать внимание на все операции, не имеющие явного правового и экономического смысла, и в случае наличия подозрений, что такие операции связаны с ОД, сообщать об этом в компетентные органы. Также в Рекомендациях содержался запрет на сообщение клиентам финансовых организаций о том, что в отношении их операций представлены данные в компетентные органы. В Рекомендациях отдельно указывалось, что в случае, если у финансовых организаций отсутствует обязанность сообщать о подозрительной операции в компетентные органы, они должны прекратить

обслуживание клиента, совершившего подозрительную транзакцию, и закрыть его счет [296].

В первых Рекомендациях ФАТФ особое внимание уделялось противодействию отмыванию доходов с использованием валютных операций. Так, подчеркивалась целесообразность закрепления обязанности для финансовых организаций сообщать в «национальное центральное агентство» информацию о всех обменных операциях, превышающих фиксированную сумму.

Несмотря на необязывающий характер Рекомендаций ФАТФ их имплементация со временем стала фактически одним из обязательных требований беспрепятственного доступа к международной банковской системе [123]. Рекомендации ФАТФ, по сути, изначально были нацелены на применение не только членами организации. Предпосылка для этого была заложена в рекомендации 21 первой версии Рекомендаций ФАТФ, согласно которой, «финансовые организации должны уделять особое внимание деловым отношениям и транзакциям с лицами, включая компании и финансовые организации, из стран, которые не применяют или применяют в недостаточной степени данные Рекомендации» [296]. А с учетом того, что членами ФАТФ на момент создания являлись страны с наиболее развитой экономикой требования Рекомендаций de facto стали обязательными для всех стран мира, включенных в мировую (западноцентричную) финансовую систему.

Рекомендации ФАТФ отличает от предыдущих документов в области ПОД их комплексный характер, затрагивающий сразу три направления борьбы с ОД: уголовно-правовое (криминализация ОД), финансово-контрольное (установление обязанностей для банков и небанковских финансовых организаций в сфере ПОД) и административное (создание специализированного государственного органа, ответственного за внедрение Рекомендаций ФАТФ). При этом, семантика положений Рекомендаций ФАТФ позволяет говорить о том, что они обращены не только к национальным правительствам в целях внесения соответствующих правок в законодательство, но и непосредственно к финансовым организациям (например, в рекомендации 19 отмечается, что финансовые организации в случае отсутствия

обязанности сообщать о подозрительных операциях в компетентные органы должны в случае наличия подозрений о связи операций клиента с ОД «отказать в оказании услуг этому клиенту, разорвать с ним отношения и закрыть его счет», а в рекомендации 20 содержатся основные требования к программам финансовых организаций по борьбе с отмыванием доходов) [296].

Также характерной особенностью Рекомендаций ФАТФ, как уже отмечалось выше, является предложение криминализации не только отмывания доходов от незаконного оборота наркотиков, но и от совершения других серьезных преступлений. Устойчиво связала отмывание доходов со всеми преступлениями, а не только наркотического характера принятая 8 ноября 1990 года Конвенция Совета Европы об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности (далее – Страсбургская конвенция) [18].

Работа Совета Европы по противодействию отмыванию доходов началась в 1977 с момента учреждения Европейским комитетом по проблемам преступности Совета Европы Комитета экспертов в целях изучения проблем, возникающих в результате перемещения денежных средств, полученных преступным путем [10]. Результатом работы данного комитета явилась Страсбургская конвенция. В научных источниках отмечается, что Федеральный закон № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» был принят в рамках исполнения международных обязательств, вытекающих из Страсбургской конвенции [10].

Страсбургская конвенция, как отмечается в некоторых научных источниках, стала первым международно-правовым актом жесткого характера (не рекомендательного, а обязывающего), закрепившим определение отмывания доходов, полученных преступным путем [209]. Однако, фактически Страсбургская конвенция соединила определение, содержащееся в Венской конвенции с термином «отмывание средств», и расширила его до отмывания доходов в результате совершения любых уголовных преступлений.

Примечательно, что практически одновременно с опубликованием рекомендаций ФАТФ стали вырабатываться региональные подходы к проблеме выработки мер противодействия отмыванию преступных доходов. В мае 1990 года в ходе встречи в Арубе (самоуправляемое государственное образование на юге Карибского моря, входит в Королевство Нидерландов) представители стран Карибского бассейна и Центральной Америки согласовали общий подход к проблеме борьбы с отмыванием доходов, который был представлен 19 рекомендациями, дополнявшими Рекомендации ФАТФ [281].

10 июня 1991 года Советом Европейского экономического Сообщества (предшественник Совета Европейского союза) была принята Директива 91/308/ЕЕС «О предотвращении использования финансовой системы в целях отмывания денег» [282]. По результатам анализа текста Директивы можно отметить, что в Директиве, несмотря на признание главенства уголовно-правовых мер в борьбе с отмыванием преступных доходов (которым посвящены Венская конвенция и Страсбургская конвенция), отмечалось, что уголовно-правовой подход не должен являться единственным способом противодействия легализации доходов, и что финансовая система может играть «высокоэффективную роль» с отсылками на положения Рекомендации Совета Европы от 27 июня 1980 г. (R (80)101) и Декларации о предотвращении преступного использования банковской системы для отмывания денег Базельского комитета по банковском надзору [6; 299]. Таким образом, Директива аккумулировала все предыдущие международно-правовые документы в сфере ПОД/ФТ (за исключением Рекомендаций ФАТФ), но с акцентом на финансовую сторону ПОД.

В части финансовых мер противодействия легализации доходов Директива детализирует и дополняет направления ПОД, содержащиеся в Декларации о предотвращении преступного использования банковской системы для отмывания денег БКБН. В Директиве отмечается, что кредитные и финансовые организации должны обеспечить идентификацию клиентов при вступлении с ними в деловые отношения (в частности, при открытии счета). Отличительной чертой Директивы по сравнению с вышеуказанной декларацией БКБН и Рекомендациями ФАТФ

является установление пороговой границы в размере 15 000 ЭКЮ (валютная единица ЕЭС и ЕС в 1979 – 1998 гг.) для финансовых операций, участники которых подлежат идентификации, если они не были идентифицированы при установлении деловых отношений (тогда как в первой версии Рекомендаций ФАТФ указывалось, в целом, о необходимости идентификации лиц, осуществляющих финансовые операции). При этом, в Директиве содержится исключение из данного правила в отношении страховых полисов, к которым требования по идентификации не предъявляются, если размер страховой премии или суммы подлежащих за один год выплат не превышают 1000 ЭКЮ, а также в случае если выплачивается единовременная страховая премия, не превышающая 2 500 ЭКЮ. Государствам также предлагается рассмотреть возможность исключения из правил идентификации для страховых полисов, связанных с пенсионными программами, если такие полисы не содержат пункта о возврате или не могут использоваться в качестве обеспечения по кредиту. Содержится в Директиве положения о необходимости идентификации лиц, участвующих в операциях, предположительно связанных с ОД, независимо от суммы таких операций, и хранении информации о клиентах и операциях в течение 5 лет после прекращения деловых отношений / совершения операции.

Рассматривая вопрос взаимодействия с органами государственной власти, Директива выделяет два способа взаимодействия:

– инициативное направление финансовыми организациями информации в государственные органы об операциях, предположительно связанных с ОД;

– ответы на запросы государственных органов с предоставлением всей необходимой информации в соответствии с процедурами, утвержденными национальным законодательством.

В продолжение положений Декларации о предотвращении преступного использования банковской системы для отмывания денег БКБН в Директиве указывается, что государства должны обеспечить, чтобы финансовые организации воздерживались от осуществления операций, в отношении которых имеются

подозрения о связи с ОД, до момента уведомления государственных органов за исключением случаев, когда такое приостановление операций невозможно.

По аналогии с Рекомендациями ФАТФ в Директиве ЕЭС было уделено внимание запрету руководству и работникам финансовых организаций уведомлять клиентов или третьих лиц о направлении информации в государственные органы, а также принятию мер по установлению в финансовых организациях процедур внутреннего контроля в целях противодействия ОД и ознакомлению персонала с положениями Директивы.

Несмотря на отсутствие отсылок Директива по содержанию оказалась близка к Рекомендациям ФАТФ, но в отличие от них носила юридически обязательный характер для государств-участников Европейского экономического сообщества (Европейского союза) и, таким образом, стала первым международно-правовым актом, регулирующим создание механизма мониторинга ПОД/ФТ.

В ноябре 1993 года в рамках созданной в 1991 году Программы ООН по контролю над наркотиками был разработан проект Типового закона о противодействии отмыванию денег [6]. Ст. 14 Типового закона предусматривалось создание специализированного органа, уполномоченного на получение сообщений о подозрительных операциях от финансовых организаций, в виде «Службы по контролю за отмыванием, подведомственной министру финансов или министру юстиции» [6, с. 52].

В качестве приложения к Типовому закону был представлен Типовой декрет о создании Службы по контролю за отмыванием. Согласно данному декрету в обязанности учреждаемого уполномоченного органа должны были входить:

– «получение сообщений от финансовых учреждений;

– анализ полученных сообщений на базе имеющейся у нее и получаемой дополнительно от других госорганов информации;

– передача соответствующих материалов органу, уполномоченному осуществлять уголовное преследование, при наличии явных признаков отмывания денег» [6, с. 52].

В июне 1995 года представители подразделений финансовой разведки из 24 стран учредили Международное объединение подразделений финансовой разведки — Группу «Эгмонт» с целью оказания содействия оперативном обмену информацией между подразделениями финансовой разведки [9]. В определении, принятом Группой «Эгмонт» в 1996 году, дается следующее определение подразделению финансовой разведки (ПФР): «ПФР является центральным национальным органом, ответственным за получение (и, если разрешено, запрашивание), анализ и дальнейшую передачу в компетентные органы раскрываемой финансовой информации:

– относящейся к доходам, которые, как подозревается, являются результатом преступной деятельности;

– требуемой в соответствии с национальным законодательством или нормативным актом в целях борьбы с отмыванием денег» [6, с. 53].

В 1996 году начался процесс создания региональных групп по типу ФАТФ (далее – РГТФ). Создание региональных групп по типу ФАТФ стало важным шагом, способствующим расширению географии международных стандартов противодействия отмыванию преступных доходов, так как ФАТФ на тот момент не принимала новых членов, а после прием новых государств-участниц происходил достаточно ограниченными темпами (в 1996 году ФАТФ состояла из 26 государств и одной региональной организации, тогда как по состоянию на февраль 2023 года ФАТФ состояла из 37 стран-участниц и двух международных организаций). Тогда как деятельность РГТФ заключается в признании и способствовании внедрению Рекомендаций ФАТФ странами-членами РГТФ, в том числе посредством взаимной оценки государств-участников РГТФ. Список РГТФ в порядке их создания приведен на рисунках 9; 10.

Дата создания	Наименование РГТФ
1992 (дата подписания Кингстонской декларации; формализация структуры осуществлена в октябре 1996 года, когда представители государств Карибского бассейна и Центральной Америки утвердили Меморандум о взаимопонимании в отношении целей и условий членства в Карибской группе разработки финансовых мер борьбы с отмыванием денег)	Карибская группа разработки финансовых мер борьбы с отмыванием денег (The Caribbean Financial Action Task Force, КФАТФ)
1995 (год основания Азиатско-Тихоокеанского регионального отделения ФАТФ; текущее наименование получила в 1997 году)	Азиатско-Тихоокеанская группа по борьбе с отмыванием денег (The Asia/Pacific Group on Money Laundering, АТГ)
1997 (первоначально был создан под названием Специального комитета экспертов по оценке мер борьбы с отмыванием денег Совета Европы, текущее наименование получил в 2002 году)	Комитет экспертов Совета Европы по оценке мер борьбы с отмыванием денег и финансированием терроризма (The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL), Манивэл)
1999	Группа по борьбе с отмыванием денег в Восточной и Южной Африке (Eastern and Southern Africa Anti-Money Laundering Group, ЕСААМЛГ)

Источник: составлено автором на основании материалов [6; 9; 277; 281; 284].
Рисунок 9 - Список РГТФ в порядке их создания (начало)

Дата создания	Наименование РГТФ
2000 (первоначальное наименование – Группа разработки финансовых мер борьбы с отмыванием денег в Южной Америке (Financial Action Task Force of South America), переименована в 2014 году связи с включением в группу стран из Центральной Америки)	Группа разработки финансовых мер борьбы с отмыванием денег в Латинской Америке (Financial Action Task Force of Latin America, ГАФИЛАТ)
2000	Межправительственная группа по борьбе с отмыванием денег в Западной Африке (Inter-Governmental Action Group against Money Laundering in West Africa, ГИАБА)
2000 (признана ФАТФ в качестве РГТФ в 2015 году)	Группа Центральной Африки по борьбе с отмыванием денег (Task Force on Money Laundering in Central Africa, ГАБАК)
2004	Группа разработки финансовых мер борьбы с отмыванием денег на Ближнем Востоке и в Северной Африке (Middle East And North Africa Financial Action Task Force, МЕНАФАТФ)
2004 (создана по инициативе Российской Федерации, представленной на пленарном заседании ФАТФ в октябре 2003 года)	Евразийская группа по противодействию легализации преступных доходов и финансированию терроризма (Eurasian Group on Combating Money Laundering and financing of terrorism, ЕАГ)

Источник: составлено автором на основании материалов [136; 275; 285; 286; 294].
Рисунок 10 - Список РГТФ в порядке их создания (окончание)

С конца 1996 года международное сообщество начинает уделять внимание вопросу противодействия финансированию терроризма. В резолюции 51/210 от 17 декабря 1996 года Генеральная Ассамблея ООН призвала государства

«предпринять шаги, с тем чтобы воспрепятствовать и противодействовать посредством соответствующих внутренних мер финансированию террористов и террористических организаций» [6, с. 67], в том числе использованием некоммерческих организаций, а также преступных организаций. Также в резолюции содержался призыв «рассмотреть вопрос о принятии мер регулирования, для того чтобы воспрепятствовать и противодействовать движению средств, в отношении которых есть подозрения, что они предназначены для террористических целей» [6, с. 67].

15 октября 1999 года Совет Безопасности ООН принял Резолюцию № 1267 (1999), в которой осудил предоставление в Афганистане движением «Талибан» (организация признана террористической решением Верховного Суда Российской Федерации от 14.02.2003 № ГКПИ 03-116) убежища для Усамы бен Ладена и иных международных террористов, а также потребовал выдачи Усамы бен Ладена. В целях обеспечения выполнения требования о выдаче главаря «Аль-Каиды» (организация признана террористической решением Верховного Суда Российской Федерации от 14.02.2003 № ГКПИ 03-116) Совет Безопасности ООН предписал всем государствам запретить взлет и посадку летательных аппаратов, принадлежащих движению «Талибан», а также заморозить «средства и другие финансовые ресурсы, включая средства, получаемые или извлекаемые благодаря имуществу, находящемуся во владении или под прямым или косвенным контролем движения «Талибан», или любого предприятия, находящегося во владении или под контролем движения «Талибан» [155].

В целях обеспечения выполнения введенных мер данной резолюцией Совета Безопасности ООН был учрежден Комитет Совета Безопасности, осуществляющий контроль за исполнением санкционного режима, уполномоченный обращаться к государствам за получением информации о принимаемых ими мерах, рассматривать сообщения о нарушениях санкционного режима, предоставлять Совету Безопасности ООН доклады о предполагаемых случаях нарушения введенных мер, а также санкционировать исключения из введенных Резолюцией № 1267 (1999) мер.

9 декабря 1999 года резолюцией 54/109 Генеральной Ассамблеи ООН была принята Международная конвенция о борьбе с финансированием терроризма. В Конвенции были определены деяния, составляющие объективную сторону финансирования терроризма, и содержался призыв к странам ввести уголовную ответственность за их совершение. Помимо вопросов уголовного преследования лиц, причастных к террористической деятельности, Конвенция призвала участвующие государства принимать необходимые меры, для того, чтобы «определить, обнаружить, заблокировать или арестовать любые средства, используемые или выделенные в целях совершения преступлений (финансирования терроризма – примечание автора)» [22], а также для конфискации данных средств.

Непосредственное отношение к механизму мониторинга ПОД/ФТ имеет ст. 18 Международной конвенции о борьбе с финансированием терроризма, в которой содержится призыв к предупреждению финансирования терроризма посредством, как принятия мер, направленных на запрет деятельности физических лиц и организаций, причастных к финансированию терроризма (что является результатом реализации механизма мониторинга ПОД/ФТ), так и установления обязанности для финансовых учреждений и других организаций, участвующих в совершении финансовых операций, идентифицировать своих клиентов, выявлять подозрительные операции и сообщать о них [22].

В целях выполнения указанных положений государствам предлагается изучить возможность:

– «принятия правил, запрещающих открытие счетов, владельцы или бенефициары которых не идентифицированы или не могут быть идентифицированы, и мер для обеспечения проверки такими учреждениями личности настоящих участников таких операций;

– в отношении идентификации юридических лиц — предъявления к финансовым учреждениям требования, когда это необходимо, принимать меры по проверке юридического статуса и структуры клиента посредством получения — от государственного регистрационного органа, клиента или от обоих —

доказательства оформления клиента как юридического лица, включая данные о наименовании клиента, его юридической форме, адресе, руководителях и положениях, регулирующих полномочия по принятию обязательств от имени этого юридического лица;

– принятия правил, налагающих на финансовые учреждения обязательство оперативно сообщать компетентным властям обо всех сложных, необычайно крупных операциях и о необычной динамике операций, не имеющих явной экономической или очевидно законной причины, не опасаясь при этом уголовной или гражданской ответственности за нарушение любых ограничений на разглашение информации, если они добросовестно сообщают о своих подозрениях;

– предъявления к финансовым учреждениям требования хранить в течение как минимум пяти лет все необходимые документы по операциям, как внутренним, так и международным» [22].

На момент создания механизм мониторинга противодействия финансирования терроризма являлся институционально независимым от механизма мониторинга ПОД. Процесс конвергенции механизмов начался после террористических актов в США 11 сентября 2001 года.

28 сентября 2001 года Совет Безопасности ООН принял Резолюцию № 1373 (2001), в которой требования по заморозке денежных средств и иных экономических ресурсов, ранее действовавшие в отношении «Талибана» и «Аль-Каиды» (организации признаны террористическими решением Верховного Суда Российской Федерации от 14.02.2003 № ГКПИ 03-116), были распространены на всех лиц, «которые совершают или пытаются совершить террористические акты, или участвуют в совершении террористических актов, или содействуют их совершению; организаций, прямо или косвенно находящихся в собственности или под контролем таких лиц, а также и лиц, и организаций, действующих от имени или по указанию таких лиц и организаций, включая средства, полученные или приобретенные с помощью собственности, прямо или косвенно находящейся во владении или под контролем таких лиц и связанных с ними лиц и организаций» [156]. Также в резолюции устанавливался запрет на «предоставление любых

средств, финансовых активов или экономических ресурсов, или финансовых или иных соответствующих услуг, прямо или косвенно, для использования в интересах лиц, которые совершают или пытаются совершить террористические акты, или содействуют или участвуют в их совершении, организаций, прямо или косвенно находящихся в собственности или под контролем таких лиц, а также лиц и организаций, действующих от имени или по указанию таких лиц» [156].

В октябре 2001 году ФАТФ приняла Восемь рекомендаций по борьбе с финансированием терроризма, которые в 2004 году были расширены до Девяти рекомендаций. К тому моменту претерпела ряд изменений и дополнений международно-правовая база механизма мониторинга ПОД. В июне 2000 года был опубликован перечень из 15 несотрудничающих стран и территорий (далее – НССТ), чьи национальные система не соответствовали в полной мере Рекомендациям ФАТФ. В данный перечень (также называемый, как «черный список ФАТФ») вошли: «Багамские острова, Доминика, Израиль, Каймановы острова, Острова Кука, Ливан, Лихтенштейн, Маршалловы острова, Науру, Ниуэ, Панама, Россия, Сент-Киттс и Невис, Сент-Винсент и Гренадины, Филиппины» [6, с. 60]. Попадание в «черный список ФАТФ» означало усложнение процесса осуществления международных расчетов, в связи с тем, что в соответствии с Рекомендациями ФАТФ банки и иные финансовые организации должны уделять особое внимание операциям, совершаемым лицами из юрисдикций, не выполняющих в полной мере Рекомендации.

15 ноября 2000 года Генеральной Ассамблеей ООН Резолюцией 55/25 была принята Конвенция Организации Объединенных Наций против транснациональной организованной преступности (Палермская конвенция), в которой помимо криминализации участия в организованной преступной группе и коррупции было предусмотрено признание уголовно-наказуемым деянием отмывание преступных доходов в трактовке Венской конвенции.

Также Палермская конвенция содержит ряд мер, направленных на противодействие отмыванию преступных доходов. Так, отмечается, что наиболее уязвимыми лицами к отмыванию преступных доходов являются банки и

небанковские финансовые учреждения, в связи с чем требуется установление режима регулирования, содержащего требования по идентификации клиентов, ведению отчетности и информированию о подозрительных операциях. Подчеркивается в Палермской конвенции важность обмена информацией на национальном и наднациональном уровнях, в связи с чем отмечается важность создания «подразделения по финансовой оперативной информации, которое будет действовать в качестве национального центра для сбора, анализа и распространения информации, касающейся возможных случаев отмывания денежных средств» [21].

Таким образом, можно отметить, что при отсутствия принципиальной новизны в положениях Палермской конвенции в части функционирования механизма мониторинга противодействия отмыванию доходов в ней осуществлено структурирование положений, содержащихся в предыдущих документах международного характера. Палермская конвенция объединила уголовно-правовое направление ПОД в виде криминализации отмывания преступных доходов, предоставив ему определение, с мерами ПОД финансово-правового характера. Также Палермская конвенция призвала страны-участницы создать подразделения финансовой разведки и учитывать стандарты ФАТФ и РГТФ.

В 2000 году с целью разработки стандартов в области противодействия финансированию терроризма была основана Вольфсбергская группа (The Wolfsberg Group of International Financial Institutions) – объединение 11 транснациональных банковских групп: Banco Santander S.A., Barclays Bank, Citigroup, Credit Suisse Group AG, Deutsche Bank AG, Goldman Sachs, HSBC, J.P. Morgan Chase, Mitsubishi UFJ Financial Group, Société Générale S.A. и UBS Group AG [10]. В июне 2015 года к объединению присоединились еще два банка: Bank of America и Standard Chartered Bank. В 2021 году Вольфсбергская группа была зарегистрирована в Базеле (Швейцария) в качестве ассоциации [276].

30 октября 2000 года Вольфсбергская группа приняла Всеобщие директивы по противодействию отмыванию доходов в частном банковском секторе (также известны, как Вольфсбергские принципы) [67]. Вольфсбергские принципы

представляли собой рекомендации ведущих мировых банков всему банковскому частному сектору.

В Вольфсбергских принципах подчеркивалась необходимость осуществления идентификации, как клиентов, так и бенефициаров (в первой версии Вольфсбергских принципов определение бенефициаров отсутствовало, оно было включено в более поздний вариант Вольфсбергских принципов, где отмечается, что под бенефициарами следует понимать физических лиц, имеющих окончательный контроль над средствами, находящимися на счете, или являющимися конечным источником средств на счете [304]).

В Вольфсбергских принципах были отмечены три группы субъектов, подлежащих повышенному вниманию, которые представлены на рисунке 11.

Группы субъектов, подлежащих повышенному вниманию, согласно Вольфсбергским принципам:

- клиенты и бенефициары, являющиеся резидентами и получателями средства из стран, о которых из достоверных источников известно, что они не соблюдают общепринятые стандарты области ПОД, или из стран с повышенным уровнем преступности;
- клиенты и бенефициары, источниками средств которых является деятельность, связанная с рисками отмывания денег;
- лица, занимающие или занимавшие должности, предполагавшие общественное доверие (государственные служащие, политические деятели, руководители государственных компаний).

Источник: составлено автором на основании материала [304].

Рисунок 11 – Группы субъектов, подлежащих повышенному вниманию, согласно Вольфсбергским принципам

Также в Вольфсбергских принципах были отмечены признаки необычного характера и подозрительности операций, а также способы обнаружения таких подозрительных операций, которые содержатся на рисунке 12.

При этом, для осуществления мониторинга операций банкам предлагалось разработать специальную программу мониторинга операций. Отдельно отмечалось, что банк сам определяет в какой степени использовать автоматизированные системы для целей мониторинга операций.

Признаки необычного характера и подозрительности операций, согласно Вольфсбергским принципам:	Способы обнаружения таких подозрительных операций, согласно Вольфсбергским принципам:
• движение средств по счету не соответствует деятельности клиента; • сумма операции превышает пороговое значение; • счет используется в качестве транзитного или по счету совершаются частые переводы денежных средств.	• мониторинг операций; • анализ контактов клиента; • анализ информации из открытых источников; • анализ собственной (внутрибанковской) информации об окружении клиента.

Источник: составлено автором на основании материала [304].

Рисунок 12 - Признаки необычного характера и подозрительности операций, а также способы обнаружения подозрительных операций, согласно Вольфсбергским принципам

Вольфсбергские принципам было посвящено Указание Центрального банка Российской Федерации от 15 февраля 2001 года № 24-Т «О Вольфсбергских принципах», которым предписывалось довести содержание Вольфсбергских принципов до сведения кредитных организаций [143].

В дальнейшем Вольфсбергские принципы претерпели несколько модификаций. Помимо включения определения бенефициара в Вольфсбергские принципы были добавлены положения, касающиеся отношений банков с разными типами посредников. Определены процедуры «должной осмотрительности» (due diligence) при вступлении банка в деловые отношения с новым клиентом, предполагающие составление профиля клиента. Кроме того, были включены рекомендации для банков разработать программу по контролю за санкционными ограничениями, предполагающую проверку потенциальных и существующих клиентов, а также операций на нарушение санкционных мер [304].

Как отмечается в некоторых научных источниках, особое значение Вольфсбергским принципам придает тот факт, что они разработаны кредитными организациями, то есть непосредственно субъектами противодействия отмыванию доходов, полученных преступным путем, и финансированию терроризма [10].

Помимо вопросов противодействия отмыванию преступных доходов, Вольфсбергская группа после террористических актов в сентябре 2001 года стала уделять внимание противодействию финансированию терроризма. Так, в 2002 году было опубликовано Заявление Вольфсбергской группы о пресечении финансирования терроризма, в котором отмечена важность соблюдения политик и процедур «Знай своего клиента» (Know Your Customer), предусматривающих идентификацию клиентов, в целях противодействия финансированию терроризма путем сравнения существующих и потенциальных клиентов со списком террористов и лиц, подозреваемых в причастности к террористической деятельности, публикуемых компетентным органами. Также в Заявлении рекомендуется осуществлять усиленный контроль в отношении клиентов, ведущих деятельность в секторах, которые широко используются для финансирования терроризма, осуществлять мониторинг операций по счету клиентов, подозреваемых в причастности к террористическим организациям, взаимодействовать с органами государственной власти в части выявления закономерностей и тенденций, связанных с финансированием терроризма, и совершенствовать процедуры мониторинга в целях выявления закономерностей и тенденций, связанных с финансированием терроризма [305].

Помимо ЕАГ (в состав которой помимо Российской Федерации входят Беларусь, Индия, Казахстан, Китай, Кыргызстан, Таджикистан, Туркменистан, Узбекистан) важную роль на постсоветском пространстве в сфере противодействия отмыванию доходов, полученных преступным путем, и финансированию терроризма играет Совет руководителей подразделений финансовой разведки государств – участников Содружества Независимых Государств (далее – СРПФР СНГ), созданный в соответствии с Соглашением об образовании Совета руководителей подразделений финансовой разведки государств – участников Содружества Независимых Государств, принятым 5 декабря 2012 года в г. Ашхабаде (Туркменистан) [173].

5 октября 2007 года Решением Совета глав государств СНГ был принят Договор государств – участников Содружества Независимых Государств о

противодействии легализации (отмыванию) преступных доходов и финансированию терроризма (далее – Договор СНГ о ПОД/ФТ) [16]. 15 октября 2021 года Совет глав государств СНГ утвердил Договор государств – участников Содружества Независимых Государств о противодействии легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения (вступил в силу для Российской Федерации 26 апреля 2023 года) [17].

В Договоре СНГ о ПОД/ФТ/ФРОМУ определение легализации (отмывания) доходов, полученных преступным путем, идентично содержащемуся в Венской, Страсбургской и Палермской конвенциях, однако, содержащийся в Договоре СНГ о ПОД/ФТ от 5 октября 2007 года термин «уполномоченный орган» заменен на принятый в международном дискурсе «подразделение финансовой разведке», которое характеризуется, как «уполномоченный орган Стороны, осуществляющий сбор, получение, анализ сообщений о подозрительных операциях (сделках) и иной информации, относящейся к легализации (отмыванию) доходов, полученных преступным путем, предикатным преступлениям и финансированию терроризма, и передачу результатов анализа в соответствующие компетентные органы» [17].

Также Договором СНГ о ПОД/ФТ/ФРОМУ предусматривается принятие нормативных правовых актов, предписывающих юридическим и физическим лицам предпринимать меры, направленные на противодействие ОД/ФТ/ФРОМУ, в том числе:

– осуществлять надлежащую проверку клиента (далее – НПК);

– документально фиксировать сведения о клиентах, бенефициарах и операциях;

– хранить в течение 5 лет документы об операциях (со дня совершения операции), а также клиентах и бенефициарах (со дня прекращения отношений);

– в порядке, предусмотренном национальным законодательством, замораживать (блокировать) операции;

– установить запрет на информирование клиентов о предпринимаемых мерах ПОД/ФТ/ФРОМУ;

– при наличии обстоятельств, установленных национальным законодательством, отказывать в установлении деловых отношений с клиентом, а также в осуществлении операций.

Отдельное внимание в Договоре СНГ о ПОД/ФТ/ФРОМУ уделяется международному сотрудничеству подразделений финансовой разведки государств-участников СНГ, в том числе описывается формат запросов на получение информации, направляемых подразделениями финансовой разведки, а также устанавливается ряд ограничений на использование информации, полученной от иностранного ПФР.

Целям организации взаимодействия между ПФР государств-участников СНГ служит СРПФР СНГ. Помимо организации взаимодействия ПФР и иных органов, в чью сферу деятельности входят вопросы ПОД/ФТ, к основным направлениям деятельности СРПФР СНГ относятся:

– «определение приоритетных направлений сотрудничества и принятие совместных эффективных мер;

– содействие выработке единых подходов в целях сближения и гармонизации национального законодательства государств - участников СНГ;

– разработка предложений о совершенствовании правовой базы сотрудничества государств - участников СНГ;

– обеспечение реализации принятых в рамках СНГ документов» [23].

СРПФР СНГ формируется из руководителей подразделений финансовой разведки государств - участников СНГ. Правом совещательного голоса наделены руководитель Секретариата СРПФР СНГ и представитель Исполнительного комитета СНГ [173].

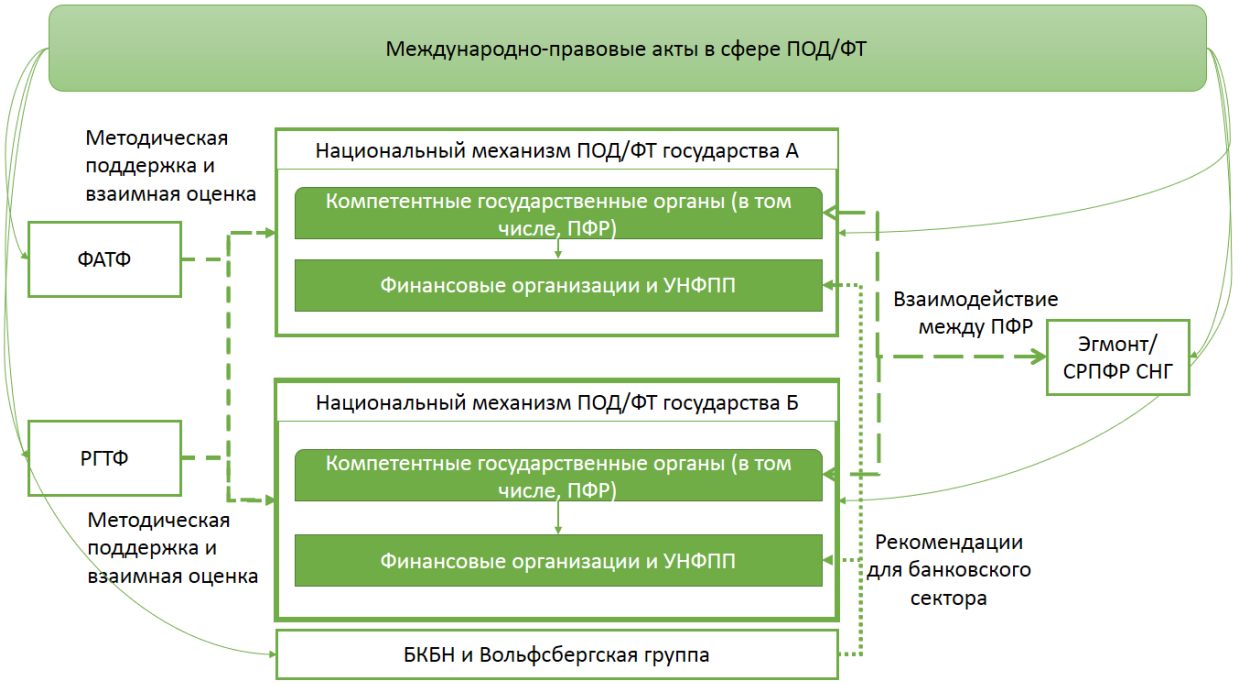
В составе СРПФР СНГ функционируют три рабочих группы:

– Рабочая группа по противодействию легализации (отмыванию) доходов, полученных преступным путем (РГПОД);

– Рабочая группа по противодействию финансированию терроризма (РГПФТ);

– Рабочая группа по созданию Системы обмена информацией между подразделениями финансовой разведки государств - участников Содружества Независимых Государств «СиНерГия» (РГСОИ).

В целом, схематичное описание международной основы механизма мониторинга ПОД/ФТ представлено на рисунке 13.



Источник: составлено автором.

Рисунок 13 – Международная основа механизма мониторинга ПОД/ФТ

Деятельность национальных механизмов мониторинга ПОД/ФТ, а также международных и региональных организаций в сфере ПОД/ФТ преимущественно опосредуется нормами международного права. К таковым помимо перечисленных выше конвенций ООН относится Конвенция Организации Объединенных Наций против коррупции (далее – Конвенция о коррупции), принятая Генеральной Ассамблеи ООН 31 октября 2003 года резолюцией 58/4 [20]. В Конвенции о коррупции, помимо прочего, рассматриваются вопросы противодействия отмыванию денежных средств. Однако, в части ПОД/ФТ положения Конвенции о коррупции в значительной степени повторяют положения Палермской конвенции.

К нормам международного мягкого права в сфере ПОД/ФТ можно отнести Рекомендации ФАТФ, а также рекомендации и стандарты для банковского сектора, устанавливаемые в части ПОД/ФТ Базельским комитетом по банковском надзору

и Вольфсбергской группой. Особое значение для механизма мониторинга ПОД/ФТ имеют Рекомендации ФАТФ.

С момента своего первого опубликования в 1990 году Рекомендации ФАТФ претерпели ряд изменений. В соответствии с действующей на момент написания исследования редакцией Рекомендаций ФАТФ, в рамках механизма мониторинга ПОД/ФТ странам следует «определить, оценить и понимать риски отмывания денег и финансирования терроризма для страны» [120], а также предпринять меры по снижению данных рисков. Отдельно в Рекомендациях (в частности, в Рекомендации 2) подчеркивается важность сотрудничества и обмена информацией между компетентными органами (в том числе, ПФР) в рамках национального уровня механизма мониторинга ПОД/ФТ. В части противодействия финансированию терроризма, в Рекомендациях ФАТФ отмечается возможность использования в данных целях некоммерческих организаций, в связи с чем к уязвимым для рисков ОД/ФТ некоммерческим организациям необходимо применять соответствующие меры по минимизации рисков.

По сравнению с ранними версиями в Рекомендациях ФАТФ были расширены и детализированы основания применения мер НПК, которые в новой редакции должны осуществляться при:

– «установлении деловых отношений;

– совершении разовых операций (сделок): (i) на сумму, превышающую установленное пороговое значение (15 000 долларов США/евро); или (ii) которые являются электронными переводами…;

– наличии подозрений в отмывании денег или финансировании терроризма;

– наличии у финансового учреждения сомнений в достоверности или достаточности полученных ранее данных о личности клиента» [120].

При этом для электронных денежных переводов в Рекомендации 16 устанавливается требование, чтобы «финансовые учреждения включали требуемую и точную информацию об отправителе и требуемую информацию о получателе в электронный перевод и сопровождающие сообщения, а также чтобы эта информация сопровождала электронный перевод или передаваемое сообщение

по всей цепочке платежа» [120]. Кроме того, странам предписывается принять меры в целях обеспечения мониторинга со стороны финансовых учреждений электронных переводов, в которых отсутствуют необходимые сведения.

Был расширен перечень мер, осуществляемых в рамках НПК, к таковым помимо идентификации клиента были отнесены определение бенефициарного собственника, цели и характера деловых отношений, а также регулярный анализ сделок с целью проверки их соответствия информацией о клиенте, которой располагает финансовое учреждение. Отдельно в Рекомендациях отмечается необходимость риск-ориентированного подхода при применении мер НПК.

В соответствии с Рекомендацией 12 для иностранных публичных должностных лиц предусматривается расширенный перечень мер НПК, устанавливающий обязанность для финансовых учреждений помимо обычных мер:

– «использовать соответствующие системы управления рисками для определения того, является ли клиент или бенефициарный собственник публичным должностным лицом;

– получать разрешение старшего руководства на установление (или продолжение для существующих клиентов) таких деловых отношений;

– принимать разумные меры для установления источника благосостояния и источника денежных средств; и

– осуществлять углубленный постоянный мониторинг деловых отношений» [120].

При этом, в соответствии с Рекомендацией 17 «Доверие мерам третьих сторон» осуществление мер НПК возможно делегировать третьей стороне при условии предоставления третьей стороной документации, полученной в рамках НПК, а также при условии учета страновых рисков места нахождения третьей стороны.

Применительно к страновым рискам Рекомендацией 19 предусмотрено применение расширенных мер НПК применительно к деловым отношениям и сделкам с физическими и юридическими лицами и финансовыми учреждениями из стран, входящих в «черный список» ФАТФ.

В Рекомендациях ФАТФ были сохранены требования, касающиеся хранения по меньшей мере в течение 5 лет записей об операциях (с момента их совершения) и записей, полученных в результате НПК (с момента окончания деловых отношений или совершения разовой сделки).

Также требования в части НПК и хранения информации распространяются на установленные нефинансовые предприятия и профессии (далее – УНФПП), в том числе к казино, агентам по операциям с недвижимостью, дилерам по драгоценным металлам и камням, адвокатам, нотариусам и другим юристам и бухгалтерам, провайдерам услуг траста и компании. В случае наличия подозрений в отношении указанных в Рекомендации 22 сделок/операций о причастности к ОД/ФТ УНФПП должны уведомить об этом ПФР.

Рекомендациями ФАТФ предусмотрено лицензирование и регистрация физических и юридических лиц, предоставляющих услуги перевода денег или ценностей, или по обмену денег (в качестве минимального уровня соответствия Рекомендациям ФАТФ, в Рекомендации 26 содержится призыв установить режим лицензирования и регистрации в отношении всех финансовых учреждений), казино, а также провайдеров услуг в сфере виртуальных активов (далее – ПУВА), включенных в Рекомендации в связи с набирающими процесс тенденциями цифровизации экономики. В пояснительной записке к Рекомендации 15 также подчеркивается необходимость применения странами риск-ориентированного подхода по отношению к ПУВА в целях выявления и минимизации рисков ОД/ФТ, связанных с виртуальными активами (которые в ФАТФ предлагает рассматривать в качестве «имущества», «доходов», «средств», «средств или иных активов» или «иной соответствующей стоимости»). В качестве предупредительных мер ФАТФ предлагает установить пороговую сумму разовых операций в размере 1000 долларов США/евро, при превышении которой ПУВА будут обязаны проводить НПК, а также обязать ПУВА хранить требуемую информацию об отправителях и получателях переводов виртуальных активов, оперативно передавать ее другим ПУВА, финансовым учреждениям и соответствующим органам.

В части купирования рисков, связанных с новыми технологиями, в Рекомендации 15 указывается, что «странам и финансовым учреждениям необходимо определять и оценивать риски отмывания денег или финансирования терроризма, которые могут возникнуть в связи с (a) разработкой новых продуктов и новой деловой практики, включая новые механизмы передачи, и (b) использованием новых или развивающихся технологий как для новых, так и для уже существующих продуктов» [120]. При этом, такая оценка рисков должна проводиться до запуска новых продуктов или использования новых технологий.

В Рекомендациях ФАТФ содержится предписание финансовым учреждениям сообщать в подразделения финансовой разведки в случае наличия «разумных оснований» подозревать в том, что средства связаны с ОД/ФТ. В то же время, по сравнению с ранней версией Рекомендаций в поздней детализирован запрет на разглашение информации финансовыми учреждениями о предпринимаемых в сфере ПОД/ФТ мерах – запрещается разглашать факт отправки в ПФР сообщения о подозрительной операции или связанной с этим информации.

Рекомендациями 24 и 25 предусмотрено обеспечение государствами наличия «достаточной, точной и своевременной информации о бенефициарной собственности и контроле юридических лиц» [120], а также о трастах, учрежденных по соглашению сторон (в том числе, информации о доверителях, доверительных собственниках и бенефициарах). В Рекомендациях содержится призыв к странам облегчить доступ к бенефициарной собственности и контролю над юридическими лицами и юридическими образованиями для финансовых учреждений и УНФПП.

Отдельное внимание в Рекомендациях ФАТФ уделяется вопросам международного сотрудничества в части оказания взаимной правовой помощи, замораживания и конфискации отмытой собственности, экстрадиции лиц, связанных с ОД/ФТ, а также иным формам международного сотрудничества.

Как уже отмечалось ранее, особую значимость Рекомендациям ФАТФ помимо международного признания в качестве ведущих стандартов в сфере ПОД/ФТ придает процедура взаимной оценки государств, на основе которой

юрисдикция может быть признана не соблюдающей требования ПОД/ФТ со всеми вытекающими негативными экономическим последствиями.

Методология взаимной оценки также была усовершенствована по итогам третьего раунда взаимной оценки после принятия в феврале 2012 года новой версии Рекомендаций ФАТФ и опубликована в феврале 2013 года под названием «Методология оценки технического соответствия рекомендациям ФАТФ и эффективности систем ПОД/ФТ» [121]. Ключевым ее нововведением стала оценка выполнения не только самих рекомендаций, но и эффективности национальной системы ПОД/ФТ. Необходимость новеллы была обусловлена коллизиями, имевшими место, когда правоприменительная практика государств не отвечала их законодательству. Согласно обновленной методологии процедура взаимной оценки состоит из двух частей. Первая часть – оценка технического соответствия, в ходе которой преимущественно проверяется имплементация требований Рекомендаций ФАТФ в национальное нормативно-правовое пространство, оценка проводится по всем 40 рекомендациям. Вторая часть – оценка эффективности, в ходе которой устанавливается степень достижения национальной системой ПОД/ФТ целей Стандартов ФАТФ. То есть, оценка технического соответствия больше сориентирована на формальное выполнение Рекомендаций ФАТФ, тогда как в ходе оценки эффективности большее внимание уделяется анализу результатов, которые страна добилась в сфере ПОД/ФТ. Оценка эффективности проводится по 11 непосредственным результатам, которые представлены на рисунке 14.

Оценка технического соответствия рекомендациям ФАТФ и эффективности систем ПОД/ФТ осуществляется ФАТФ и РГТФ (при наличии таких) в отношении членов ФАТФ и только РГТФ в отношении членов РГТФ, не состоящих в ФАТФ.

Таким образом, международную основу механизма мониторинга ПОД/ФТ составляют международные акты в сфере ПОД/ФТ, и, в первую очередь, в силу своей большей специализации на тематике ПОД/ФТ, а также международного признания, Рекомендации ФАТФ.

Непосредственные результаты ФАТФ:

- Риски отмывания денег и финансирования терроризма понимаются и, там, где это необходимо, на национальном уровне координируются действия по борьбе с отмыванием денег, финансированием терроризма и распространения оружия массового уничтожения
- Международное сотрудничество обеспечивает необходимую информацию, оперативные финансовые данные, доказательства и способствует деятельности, направленной против преступников и их активов
- Надзорные органы должным образом осуществляют надзор, контролируют и регулируют финансовые учреждения, УНФПП и ПУВА в части выполнения требований по ПОД/ФТ соразмерно имеющимся рискам
- Финансовые учреждения, УНФПП и ПУВА должным образом применяют превентивные меры в сфере ПОД/ФТ соразмерно их рискам, и сообщают о подозрительных операциях
- Предотвращено использование в противозаконных целях юридических лиц и образований для отмывания денег и финансирования терроризма, а информация касательно бенефициарной собственности беспрепятственно доступна компетентным органам
- Оперативные данные финансовой разведки и вся другая относящаяся к делу информация должным образом используется компетентными органами для проведения расследований по фактам отмывания денег и финансирования терроризма
- Преступления и деятельность, связанные с отмыванием денег, расследуются, а правонарушители преследуются по закону и подвергаются эффективным, соразмерным и оказывающим сдерживающее воздействие санкциям
- Преступные доходы и средства совершения преступлений конфискуются
- Преступления и деятельность, связанные с финансирование терроризма, расследуются, а лица, финансирующие терроризма, преследуются по закону и подвергаются эффективным, соразмерным и оказывающим сдерживающее воздействие санкциям
- Террористам, террористическим организациям и тем, кто их финансирует, препятствуют в сборе, перемещении и использовании денежных средств, а также в использовании в противозаконных целях сектора НКО
- Лицам и организациям, причастным к распространению оружия массового уничтожения, препятствуют в сборе, перемещении и использовании денежных средств, согласно соответствующим Резолюциям Совета Безопасности ООН

Источник: составлено автором на основании материала [121].

Рисунок 14 – 11 непосредственных результатов ФАТФ

Обеспечению выполнения Рекомендаций ФАТФ способствуют процедуры взаимной оценки, а также механизм включения государств, не сотрудничающих с ФАТФ, или неспособных устранить значительные недостатки в национальных системах ПОД/ФТ, в «черный» и «серый» списки ФАТФ. Значительную роль в национальных механизмах мониторинга ПОД/ФТ играют каналы международного взаимодействия ПФР и иных компетентных органов, осуществляемого через системы обмена информацией, запущенные в рамках Группы «Эгмонт» и СРПФР СНГ.

При этом стоит отметить влияние, которое оказывает на процесс формирования международной основы механизма мониторинга ПОД/ФТ цифровизация экономики. Так, по сравнению с первой версией Рекомендаций ФАТФ в Рекомендации ФАТФ, опубликованные в 2012 году, были в рамках 15 Рекомендации включены вопросы, связанные с влиянием новых технологий на противодействие отмыванию преступных доходов и финансированию терроризма. В октябре 2018 года Рекомендация 15 была вновь пересмотрена, в нее были включены вопросы регулирования деятельности провайдеров услуг виртуальных

активов (в том числе, криптовалют), что было обусловлено наблюдавшимся в тот момент ростом вложений средств в криптовалюты и повышением интереса к технологиям блокчейн [56]. Также риски и возможности, связанные с цифровизацией экономики, регулярно рассматриваются в материалах методико-консультационного характера, публикуемых ФАТФ и РГТФ, к которым (применительно для российского механизма мониторинга ПОД/ФТ) можно отнести материалы, представленные на рисунке 15 [64; 101; 135; 141; 163; 164].

Организация	Год опубликования	Наименование документа	Тип документа
ФАТФ	2013	Предоплаченные карты, мобильные платежи и онлайн-платежи	Руководство по применению риск-ориентированного подхода
ФАТФ	2014	Виртуальные валюты. Ключевые определения и потенциальные риски в сфере ПОД/ФТ	Отчет
ФАТФ	2019	Виртуальные активы и провайдеры услуг в сфере виртуальных активов	Руководство по применению риск-ориентированного подхода
ФАТФ	2021	Возможности и проблемы новых технологий в сфере ПОД/ФТ	Отчет
ФАТФ	2021	Виртуальные активы и провайдеры услуг в сфере виртуальных активов	Обновленное руководство по применению риск-ориентированного подхода
ЕАГ	2022	Легализация (отмывание) преступных доходов от киберпреступлений, а также финансирование терроризма за счет указанной преступной деятельности, в том числе с использованием электронных денег или виртуальных активов и инфраструктуры их провайдеров	Типологический проект

Источник: составлено автором на основании материалов [64; 101; 135; 141; 163; 164].
Рисунок 15 – Список материалов методико-консультационного характера, опубликованных ФАТФ и ЕАГ, в которых рассматриваются риски и возможности, связанные с цифровизацией экономики

2.2 Анализ трансформации российского механизма мониторинга противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма

В качестве точки отсчета процесса формирования отечественного механизма мониторинга ПОД/ФТ исследователями принято рассматривать ратификацию Верховным советом СССР Венской конвенции в 1990 году [6; 263].

В Российской Федерации с середины 1990-х годов велась законопроектная деятельность, направленная на создание нормативно-правовой основы механизма мониторинга ПОД/ФТ, однако ни одна законодательная инициатива до 2000 года не была официально принята [6]. 15 июля 2000 года ФАТФ опубликовала список НССТ из 15 стран, в который, как отмечалось выше, вошла и Российская Федерация. ФАТФ рекомендовала финансовым учреждениям уделять «особое внимание деловым отношениям и сделкам с лицами, включая компании и финансовые учреждения, из «несотрудничающих стран и территорий» на период до того, как они примут и реализуют такие меры» [6, с. 361 – 362]. Кроме того, в докладе ФАТФ отмечалось, что в случае отсутствия необходимых преобразований в национальных системах страны-члены ФАТФ в отношении НССТ «должны будут рассмотреть вопрос о применении надлежащих контрмер» [6, с. 362]. В октябре 2000 года и январе 2001 года угрозы применить к странам и территориям из «черного списка» финансовые санкции (включая, блокировку зарубежных счетов компаний) озвучивали представители Европейского союза [100]. Внесение Российской Федерации в список НССТ способствовало активизации деятельности по разработке законодательной основы механизма мониторинга ПОД/ФТ.

7 августа 2001 года был принят Федеральный закон № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем», который стал основой для зарождающегося механизма мониторинга ПОД/ФТ в Российской Федерации. В Законе № 115-ФЗ содержался перечень операций, подлежащих обязательному контролю, а также устанавливалась обязанность организаций, осуществляющих операции с денежными средствами или иным имуществом, фиксировать операции, предположительно связанные с отмыванием доходов, полученных преступным путем. Также содержалось требование осуществлять процедуру идентификации клиентов. Первоначально действие Закона № 115-ФЗ распространялось на кредитные организации, профессиональных участников рынков ценных бумаг, страховые и лизинговые компании, организации почтовой, телеграфной связи и иные некредитные организации, осуществляющие перевод денежных средств, а

также на ломбарды. Предусматривалось Законом № 115-ФЗ создание уполномоченного органа, осуществляющего прием информации об операциях от субъектов Закона № 115-ФЗ [34].

Одновременно с Законом № 115-ФЗ был принят Федеральный закон от 7 августа 2001 г. № 121-ФЗ «О внесении изменений и дополнений в законодательные акты Российской Федерации в связи с принятием Федерального закона «О противодействии легализации (отмыванию) доходов, полученных преступным путем», предусматривающий, помимо прочего, аннулирование лицензии на осуществление профессиональной деятельности на рынке ценных бумаг, а также отзыв лицензий у кредитных организаций за неоднократные нарушения в течение одного года требований Закона № 115-ФЗ [31].

1 ноября 2001 года Президент Российской Федерации подписал Указ № 1263 «Об уполномоченном органе по противодействию легализации (отмыванию) доходов, полученных преступным путем» [39]. В указе поручалось образовать Комитет Российской Федерации по финансовому мониторингу (далее – КФМ России), являющимся федеральным органом исполнительной власти, уполномоченным принимать меры по противодействию легализации (отмыванию) доходов, полученных преступным путем, и координирующим деятельность в этой сфере иных федеральных органов исполнительной власти. КФМ России находился в ведении Министерства финансов Российской Федерации. 1 февраля 2002 г. КФМ России получил первое сообщение от кредитной организации [100].

4 июня 2002 года КФМ России был принят в число членов Группы «Эгмонт». Принятие Комитета в Группу «Эгмонт» подтвердило соответствие КФМ России общепринятому определению подразделения финансовой разведки и наличия у него соответствующих полномочий. По итогам пленарного заседания ФАТФ в Париже в октябре 2002 года было принято решение об исключении России из «черного списка» ФАТФ.

Также в октябре 2002 года изменения претерпел Закон № 115-ФЗ, его сфера действия была расширена на противодействие финансированию терроризма, в

связи с чем было изменено его название на Федеральный закон «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма». До того, в июле 2002 года Российская Федерация ратифицировала Международную конвенцию о борьбе с финансированием терроризма.

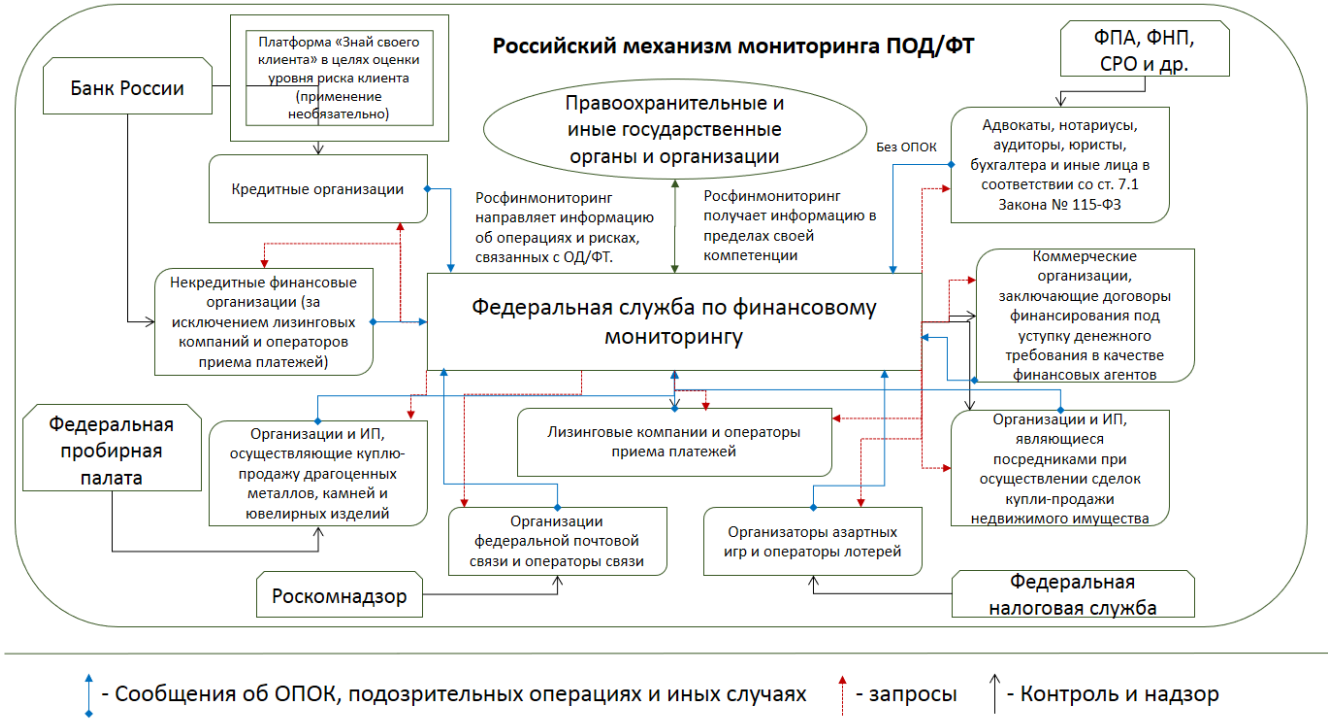
В соответствии с нововведениями в Закон № 115-ФЗ под требования об обязательном контроле попали операции, в которых хотя бы одной стороной является организация или физическое лицо, в отношении которого имеются сведения о причастности к террористической деятельности (либо организация или физическое лицо находятся под контролем таких лиц). Кроме того, был внедрен механизм административного приостановления финансовых операций с участием лиц, связанных с террористической деятельностью [34].

В целях исполнения вышеуказанных положений Закона № 115-ФЗ с 2003 года подразделение финансовой разведки России стало составлять Перечень организаций и физических лиц, в отношении которых имеются сведения об их причастности к экстремистской деятельности или терроризму [100].

В июне 2003 года после проведенной экспертами ФАТФ в отношении Российской Федерации комплексной оценки национальной системы ПОД/ФТ, по итогам которой было подтверждено ее соответствие требованиям Рекомендаций ФАТФ, Россия стала членом ФАТФ. 24 февраля 2023 года после череды неудачных попыток, инициированных ПФР Украины, заблокировать деятельность Российской Федерации в международной группе членство Российской Федерации в ФАТФ было приостановлено [108].

Указом Президента Российской Федерации от 9 марта 2004 г. № 314 «О системе и структуре федеральных органов власти» Комитет Российской Федерации по финансовому мониторингу был преобразован в Федеральную службу по финансовому мониторингу (Росфинмониторинг). В 2007 году руководство деятельность Росфинмониторинга было передано напрямую Правительству Российской Федерации. С 2012 года руководство деятельностью Росфинмониторинга осуществляет Президент Российской Федерации [100].

В настоящее время Федеральная служба по финансовому мониторингу занимает центральное положение в российском национальном механизме мониторинга ПОД/ФТ [237]. Схематически механизм мониторинга противодействия отмыванию преступных доходов и финансированию терроризма в Российской Федерации в части взаимодействия органов государственной власти и поднадзорных лиц организаций представлен на рисунке 16.



Источник: составлено автором.

Рисунок 16 – Механизм мониторинга противодействия отмыванию преступных доходов и финансированию терроризма в Российской Федерации в части взаимодействия органов государственной власти и поднадзорных лиц и организаций

Нормативную основу российского механизма мониторинга ПОД/ФТ составляют положения Закона № 115-ФЗ. Федеральным законом определяется список организаций и индивидуальных предпринимателей, в чьи обязанности входит предоставление сообщений в уполномоченный орган (Росфинмониторинг) в отношении двух видов операций [11]:

а) Операций, подлежащих обязательному контролю (ОПОК).

б) Операций, в отношении которых существует подозрение в причастности к ОД/ФТ/ФРОМУ (в практике работы Росфинмониторинга в отношении сообщений о данных операциях действует аббревиатура СПО – сообщения о подозрительных операциях (например, [145]).

Также с 2020 года в российское антиотмывочное законодательство введена возможность отправки сообщений о подозрительной деятельности (СПД) – «совокупности взаимосвязанных подозрительных операций, объединенных единым замыслом, транзакционными связями, общими организаторами и заказчиками теневых схем» [160].

В соответствии со ст. 5 Закона № 115-ФЗ субъектов ПОД/ФТ, в чьи обязанности входит информирование Росфинмониторинга о вышеуказанных операциях, можно разделить на следующие виды [34]:

а) Кредитные организации.

б) Некредитные финансовые организации (в соответствии с [35]):

1) профессиональные участники рынка ценных бумаг;

2) операторы инвестиционных платформ (отнесены к некредитным финансовым организациям в следующих источниках: [223; 268]);

3) страховые организации (а также индивидуальные предприниматели, являющиеся страховыми брокерами);

4) лизинговые компании (отнесены к некредитным финансовым организациям в следующих источниках: [223; 268]);

5) ломбарды;

6) управляющие компании инвестиционных фондов, паевых инвестиционных фондов и негосударственных пенсионных фондов;

7) операторы приема платежей (отнесены к некредитным финансовым организациям в следующих источниках: [223; 268]);

8) кредитные потребительские кооперативы, в том числе сельскохозяйственные кредитные потребительские кооперативы;

9) микрофинансовые организации;

10) общества взаимного страхования;

11) негосударственные пенсионные фонды;

12) операторы финансовых платформ;

13) операторы информационных систем, в которых осуществляется выпуск цифровых финансовых активов, и операторы обмена цифровых финансовых активов.

в) Организации и ИП, осуществляющие куплю-продажу драгоценных металлов и драгоценных камней, ювелирных изделий из них и лома таких изделий (за исключением религиозных организаций, музеев и организаций, использующих драгоценные металлы и камни в научно-исследовательских целях).

г) Организации федеральной почтовой связи и операторы связи, имеющие право самостоятельно оказывать услуги по передаче данных.

д) Организаторы азартных игр и операторы лотерей.

е) Организации и ИП, являющиеся посредниками при осуществлении сделок купли-продажи недвижимого имущества.

ж) Коммерческие организации, заключающие договоры финансирования под уступку денежного требования в качестве финансовых агентов.

В ст. 7.1 Закона № 115-ФЗ обязанность по направлению СПО в случае выявления подозрительных операций возлагается также на:

а) Адвокатов.

б) Доверительных собственников (управляющих) иностранной структуры без образования юридического лица.

в) Исполнительные органы личного фонда, имеющего статус международного фонда (кроме международного наследственного фонда).

г) Лиц, осуществляющих предпринимательскую деятельность в сфере оказания юридических или бухгалтерских услуг.

д) Лиц, осуществляющих майнинг цифровой валюты (в том числе участников майнинг-пулов).

Нормативное предписание в отношении данных лиц применяется только в случае совершения ими от имени или по поручению клиента:

– сделок с недвижимым имуществом;

– операций и сделок, связанных с управлением денежными средствами, ценными бумагами или иным имуществом клиента;

– операций и сделок, связанных с управлением банковскими счетами или счетами ценных бумаг;

– операций и сделок, связанных с привлечением денежных средств для создания организаций, обеспечения их деятельности или управления ими;

– операций и сделок, связанных с созданием юридических лиц и иностранных структур без образования юридического лица, обеспечение их деятельности или управления ими, а также куплей-продажей юридических лиц и иностранных структур без образования юридического лица;

– майнинга цифровой валюты или распределения цифровой валюты, выпущенной (полученной) в результате майнинга.

Обязанность по направлению СПО устанавливается и для нотариусов. Нотариусы помимо вышеописанных случаев обязаны направлять СПО в случае осуществления нотариальных действий, связанных с удостоверением сделок, принятием в депозит денежных сумм и ценных бумаг, совершением исполнительных надписей, а также при совершении нотариальных действий в связи с увеличением уставного капитала общества с ограниченной ответственностью во исполнение договора конвертируемого займа.

Возлагается обязанность по направлению СПО также на аудиторов и аудиторские организации, однако в их случае законодатель не стал ограничивать предписание закрытым перечнем операций.

Лица, организующие деятельность майнинг-пула, обязаны направлять СПО при распределении выпущенной (полученной) цифровой валюты между участниками майнинг-пула в случае наличия «любых оснований полагать, что распределенная цифровая валюта может быть использована участниками майнинг-пула в целях легализации (отмывания) доходов, полученных преступным путем, или финансирования терроризма» [34].

Надзор за соблюдением вышеуказанными лицами требований антиотмывочного законодательства осуществляется органами и организациями, перечисленными на рисунке 17.

Источник: составлено автором на основании материала [34].

Рисунок 17 – Органы и организации, осуществляющие контрольно-надзорную деятельность в сфере ПОД/ФТ, с указанием поднадзорных субъектов Закона № 115-ФЗ

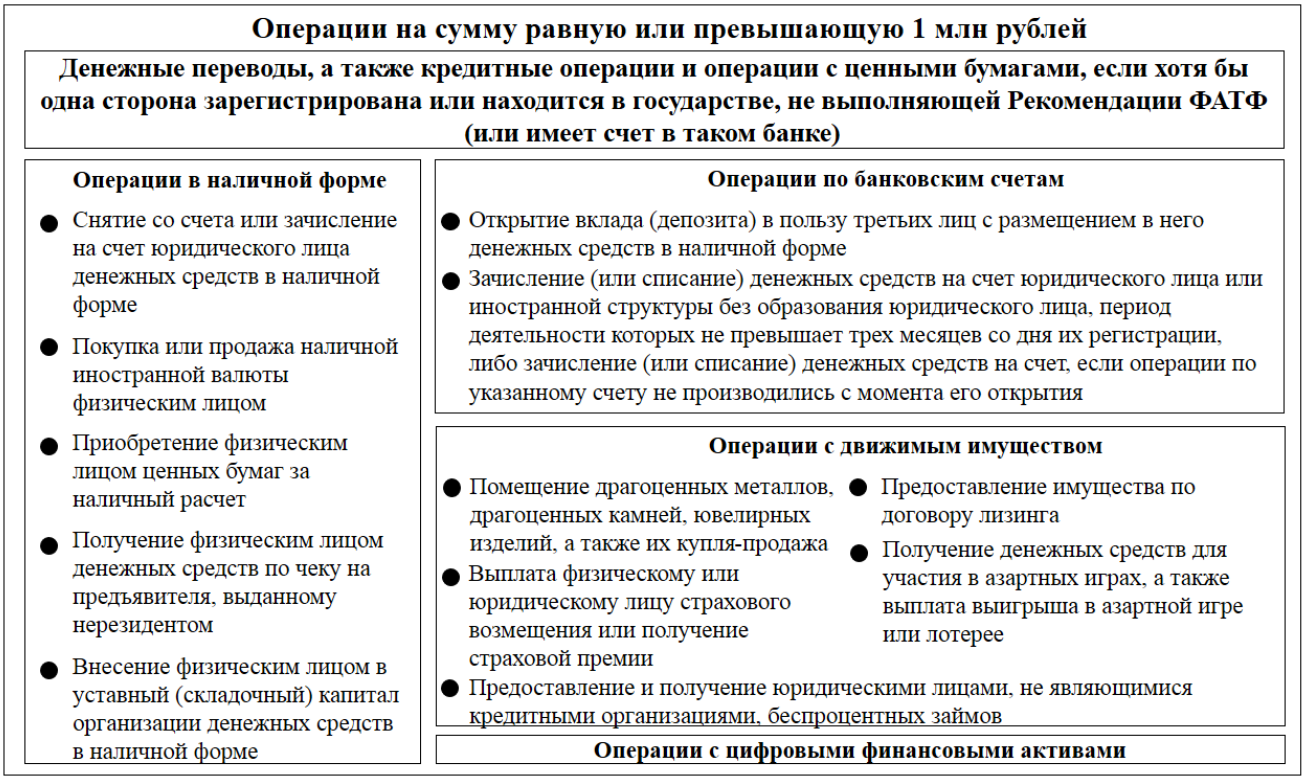
К операциям, подлежащим обязательному контролю, в соответствии со ст. 6 Закона № 115-ФЗ относятся [34]:

– операции с денежными средствами и иным имуществом (стоит отметить, что в соответствии со статьей 3 Закона № 115-ФЗ к имуществу, в том числе, относится цифровая валюта) на сумму, равную или превышающую 1 млн рублей, в случае наличия одного из признаков, содержащихся на рисунке 18;

– операции о сделке с недвижимым имуществом, равные или превышающие по стоимости 5 млн рублей;

– операции по получению или расходованию денежных средств некоммерческой организацией (за исключением государственных и ряда других НКО, приведенных в пункте 1.2 статьи 6 Закона № 115-ФЗ);

– операции по счету хозяйственных обществ, имеющих стратегическое значение для оборонно-промышленного комплекса и безопасности Российской Федерации, и обществ, находящихся под их прямым или косвенным контролем на сумму, равную или превышающую 10 млн рублей;



Источник: составлено автором на основании материала [34].

Рисунок 18 – Операции с денежными средствами и иным имуществом на сумму, равную или превышающую 1 млн рублей, подлежащие обязательному контролю

– получение перевода с территории иностранного государства или административно-территориальной единицы иностранного государства, обладающей самостоятельной правоспособностью, перечень которых утверждается уполномоченным органом;

– операции по счетам исполнителей государственного оборонного заказа на сумму, равную или превышающую 600 тыс. рублей (по второму и последующему зачислению или списанию – 10 млн рублей);

– операции по получению денежных средств физическим лицом в наличной форме с использованием платежной карты, эмитированной банком, зарегистрированным на территории иностранного государства или административно-территориальной единицы иностранного государства, обладающей самостоятельной правоспособностью, перечень которых утверждается уполномоченным органом;

– платежи по договору лизинга на сумму, равную или превышающую 1 млн рублей;

– операции почтового перевода и операции по возврату неиспользованного остатка денежных средств, внесенных в качестве аванса за услуги связи на сумму, равную или превышающую 100 тыс. рублей;

– операции, совершаемые по поручению клиента - иностранного гражданина на сумму, равную или превышающую 50 000 рублей (или операции, совершаемые в иностранной валюте на эквивалентную сумму), а также по поручению клиента - иностранного юридического лица на сумму, равную или превышающую 500 000 рублей (или операции, совершаемые в иностранной валюте на эквивалентную сумму) в случае, если идентификация клиента осуществлялась иностранным банком или иностранной финансовой организацией.

Также Законом № 115-ФЗ предусматривается возможность определения уполномоченным органом (при необходимости в согласовании с Банком России) операций, подлежащих обязательному контролю.

Обязательному контролю подлежат также операции, в случае, если «хотя бы одной из сторон является организация или физическое лицо, включенные в перечень организаций и физических лиц, в отношении которых имеются сведения об их причастности к экстремистской деятельности или терроризму, либо юридическое лицо, прямо или косвенно находящееся в собственности или под контролем таких организации или физического лица, либо физическое лицо или юридическое лицо, действующие от имени или по указанию таких организации или физического лица» [34]. Для лиц, включенных в перечень организаций и физических лиц, в отношении которых имеются сведения об их причастности к экстремистской деятельности или терроризму, действует запрет на осуществление ими операций, за исключением ряда операций, разрешенных в отношении физических лиц в целях обеспечения ими жизнедеятельности [34].

В отношении операций, подлежащих обязательному контролю, организации и ИП, осуществляющие операции с денежными средствами и имуществом, должны предоставлять информацию в течение трех рабочих дней после дня совершения операции [34]. Сведения, предоставляемые в отношении ОПОК в соответствии со ст. 7 Закона № 115-ФЗ, представлены на рисунке 19.

Сведения, предоставляемые организациями и ИП, осуществляющими операции с денежными средствами и имуществом в отношении операций, подлежащих обязательному контролю:
• вид операции и основания ее совершения; • дата совершения операции и ее сумма; • сведения, необходимые для идентификации лица, совершающего операцию (а также лица, от имени которого совершается операция, и лица, совершающего операцию от имени другого лица) и получателя денежных средств и иного имущества; • наименование, идентификационный номер налогоплательщика, государственный регистрационный номер, место государственной регистрации и адрес местонахождения юридического лица, совершающего операцию с денежными средствами или иным имуществом; • номер платежной карты, сведения о держателе платежной карты, наименование иностранного банка (предоставляются кредитными организациями для операций, по получению денежных средств физическим лицом в наличной форме с использованием платежной карты, эмитированной банком, зарегистрированным на территории иностранного государства или административно-территориальной единицы иностранного государства, обладающей самостоятельной правоспособностью, перечень которых утверждается уполномоченным органом).

Источник: составлено автором на основании материала [34].
Рисунок 19 – Сведения, предоставляемые организациями и ИП, осуществляющими операции с денежными средствами и имуществом в отношении операций, подлежащих обязательному контролю

В части СПО для вышеперечисленных организаций и лиц установлено требование разработки правил внутреннего контроля в целях ПОД/ФТ/ФРОМУ (или целевых правил внутреннего контроля для банковских холдингов) и назначения должностных лиц, ответственных за реализацию правил внутреннего контроля. В соответствии с данными правилами осуществляется фиксирование операций, предположительно связанных с ОД/ФТ.

К признакам подозрительности операций в ст. 7 Закона № 115-ФЗ отнесены:

– «запутанный или необычный характер сделки, не имеющей очевидного экономического смысла или очевидной законной цели;

– несоответствие сделки целям деятельности организации, установленным учредительными документами этой организации;

– выявление неоднократного совершения операций или сделок, характер которых дает основание полагать, что целью их осуществления является уклонение от процедур обязательного контроля;

– совершение операции, сделки клиентом, в отношении которого уполномоченным органом в организацию направлен либо ранее направлялся запрос;

– отказ клиента от совершения разовой операции, в отношении которой у работников организации возникают подозрения, что указанная операция осуществляется в целях легализации (отмывания) доходов, полученных преступным путем, или финансирования терроризма;

– решение клиента об отказе от установления отношений с организацией, осуществляющей операции с денежными средствами или иным имуществом, или о прекращении отношений с такой организацией, если у работников такой организации возникают обоснованные подозрения, что указанное решение принимается клиентом в связи с осуществлением организацией внутреннего контроля;

– иные обстоятельства, дающие основания полагать, что сделки осуществляются в целях легализации (отмывания) доходов, полученных преступным путем, или финансирования терроризма» [34].

В случае, если у сотрудников организаций возникают подозрения, что разовая операция или совокупность операций и действий связаны с ОД/ФТ в течение трех рабочих дней организация обязана отправить сообщение в Росфинмониторинг. СПО отправляются независимо от того, является ли операция, в отношении которой направляется информация, подлежащей обязательному контролю, или нет.

Критерии подозрительности операций в более развернутом виде содержатся в требованиях к правилам внутреннего контроля для кредитных и некредитных финансовых организаций, утвержденных Положениями Банка России от 2 марта 2012 г. № 375-П «О требованиях к правилам внутреннего контроля кредитной организации в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» и от 15 декабря 2014 г. № 445-П «О требованиях к правилам внутреннего контроля некредитных финансовых организаций в целях противодействия легализации

(отмыванию) доходов, полученных преступным путем, и финансированию терроризма», в которых содержатся классификаторы признаков, указывающих на необычный характер операции (сделки) [45; 46]. Также перечень признаков подозрительности операций, содержится в документе под названием «Описание структур наименования, служебной и информационной частей ФЭС, описание кодов признаков, указывающих на необычный характер операций (сделок), и требования к технологическим электронным документам, направление которых регламентировано особенностями представления в Федеральную службу по финансовому мониторингу информации, предусмотренной Федеральным законом от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», утвержденными приказом Федеральной службы по финансовому мониторингу от 8 февраля 2022 г. № 18» (далее – Описание структур и частей ФЭС), опубликованном на сайте Росфинмониторинга, и применяемым для нефинансовых организаций (за исключением лизинговых компаний и операторов приема платежей) [137]. В данном же документе содержатся виды подозрительной деятельности, к которым отнесены следующие:

– «деятельность, связанная с проведением операций с денежными средствами или иными имуществом, возможной целью которых является вывод капитала за рубеж;

– деятельность операторов по приему платежей, связанная с исполнением денежных обязательств (прием наличных денежных средств) физического лица перед поставщиком по оплате товаров (работ, услуг), непосредственно с использованием терминалов;

– деятельность, связанная с незаконным получением субсидий в рамках государственных программ поддержки МСП в целях получения государственной поддержки в форме возмещения части затрат на уплату первого лизингового платежа;

– деятельность, связанная с возможной легализацией преступных доходов с использованием мнимых (притворных) сделок и факторинговых компаний;

– деятельность, связанная с возможным нецелевым использованием средств материнского (семейного) капитала;

– деятельность, связанная с осуществлением почтовых переводов денежных средств от юридического лица в адрес физических лиц в рамках заключенных договоров Почты России с юридическим лицом в целях последующего вывода денежных средств в неконтролируемый наличный оборот;

– деятельность, связанная с использованием инфраструктуры операторов сотовой связи, имеющих право самостоятельно оказывать услуги подвижной радиотелефонной связи в финансовых схемах, конечной целью которых может являться перемещение денежных средств и их вывод в неконтролируемый наличный оборот через лицевые счета операторов связи;

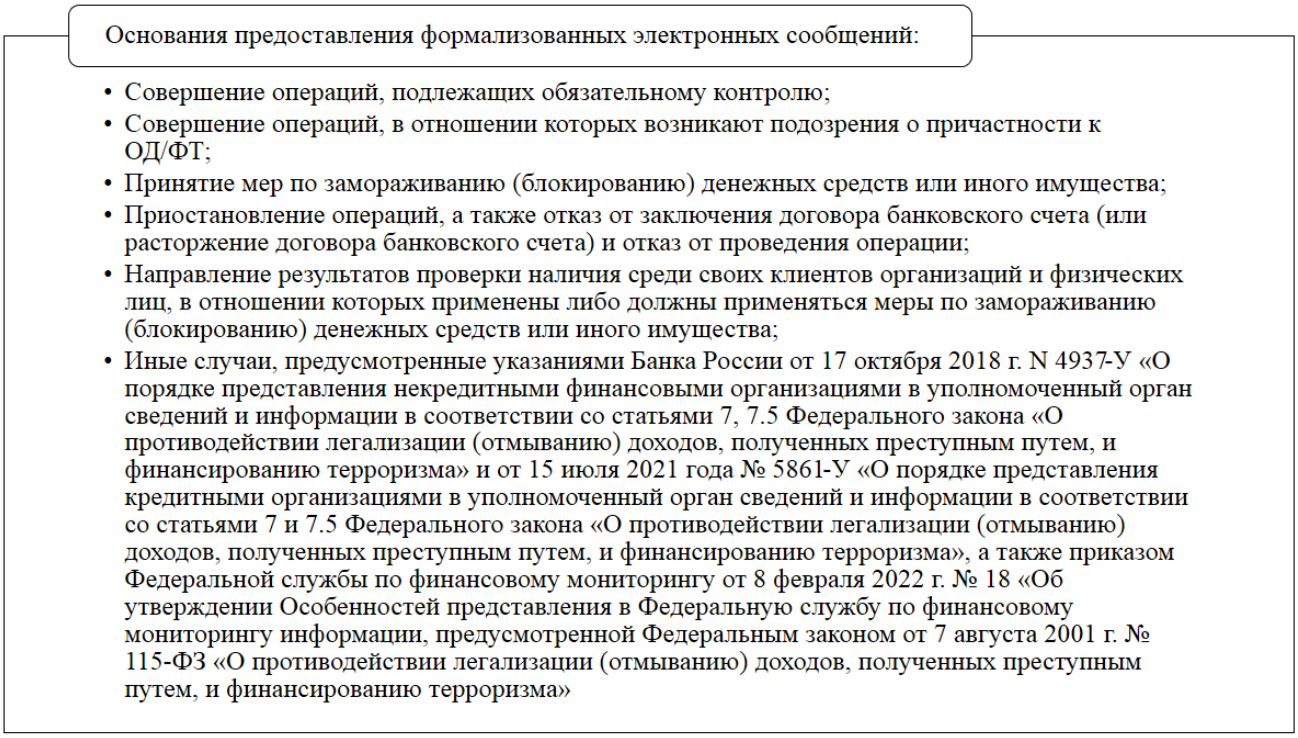
– деятельность, связанная с использованием инфраструктуры организаторов азартных игр (онлайн казино, букмекерских контор и так далее) в целях легализации денежных средств, полученных преступным путем;

– иная деятельность» [139].

Каждому признаку подозрительности операции и виду подозрительной деятельности соответствует свой код вида признака (вида деятельности). Данный код используется в формализованных электронных сообщениях (далее – ФЭС) – электронных документах, передаваемых субъектам Закона № 115-ФЗ в Росфинмониторинг. ФЭС предоставляются кредитными и некредитными финансовыми организациями, а также иными организациями, в чьи обязанности в соответствии с Законом № 115-ФЗ входит оповещение уполномоченного органа об операциях, подлежащих обязательному контролю, а также о подозрительных операциях.

Основания предоставления ФЭС указаны на рисунке 20. Формализованные электронные сообщения предоставляются в строго установленном формате. Несоблюдение формата (а также отсутствие усиленной квалифицированной электронной подписи и нарушение целостности ФЭС) являются основаниями для отказа в принятии ФЭС со стороны Росфинмониторинга. Форматы ФЭС установлены в вышеприведенном Описании структур и частей ФЭС,

опубликованным Росфинмониторингом, а также в Порядке составления некредитными финансовыми организациями в электронной форме информации, предусмотренной статьями 7; 7.5 Федерального закона «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» и Правилах составления кредитными организациями в электронной форме сведений и информации, предусмотренных статьями 7, 7.5 Федерального закона «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» [97; 149].

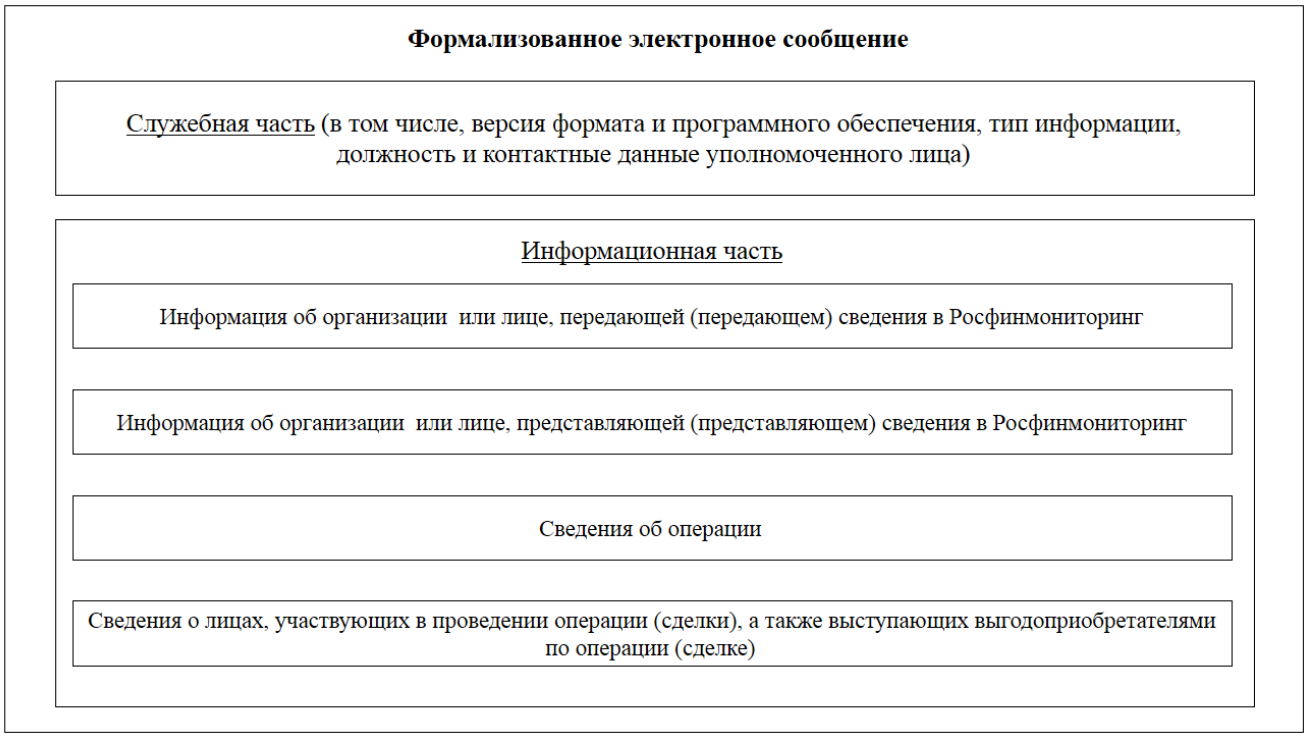


Источник: составлено автором на основании источников [44; 48; 49].
Рисунок 20 – Основания предоставления формализованных электронных сообщений

Каждое ФЭС состоит из служебной и информационной частей. При этом, информационная часть формируется в соответствии с Описанием структур и частей ФЭС, опубликованным Росфинмониторингом (в случае с документами ЦБ РФ список незначительно изменен), только для сообщений об ОПОК, СПО, сообщений о принятых мерах по замораживанию (блокированию) денежных средств или иного имущества (а также о результатах проверки наличия среди своих клиентов лиц, в отношении которых применены либо должны применяться меры

по замораживанию (блокированию) денежных средств или иного имущества), сообщений о случаях отказа в выполнении распоряжения клиента о совершении операции с денежными средствами или иным имуществом, а также для сообщений о фактах препятствия со стороны государства (территории), в котором (на которой) расположены филиалы и представительства организации выполнению требований Закона № 115-ФЗ.

Структура ФЭС для ОПОК, СПО и приостановленных операций приведена на рисунке 21.



Источник: составлено автором на основании материала [137].
Рисунок 21 – Структура формализованного электронного сообщения

В сведениях об операции помимо служебной информации включены дата совершения и выявления операции, сумма операции, основание и характеристика операции, а также код операции. В отношении всех операций, подлежащих обязательному контролю, а также подозрительных операций установлены соответствующие кодовые обозначения (в случае подозрительных операций установлены кодовые обозначения, классифицирующие признаки необычной операции).

ФЭС об ОПОК и СПО представляют значительный объем информации, направляемой в Росфинмониторинг, и формируют массив данных на основе

которых Федеральная служба по финансовому мониторингу выявляет операции, имеющие признаки ОД/ФТ. Так, в Отчете о взаимной оценке Российской Федерации, утвержденном на Пленарном заседании ФАТФ в октябре 2019 года, отмечается, что в Росфинмониторинг в среднем в год поступает 20 миллионов СПО и 10 миллионов сообщений об ОПОК [293]. Также растет количество СПД, являющихся нововведением в российском механизме мониторинга ПОД/ФТ. По сообщению Росфинмониторинга по состоянию на апрель 2022 года в службу поступило «несколько сотен сообщений от банков с указанием специального идентификатора», при том, что поправка в Закон № 115-ФЗ предусматривающая направление СПД вступила в силу первого марта 2022 года [160].

Кроме того, Законом № 115-ФЗ устанавливается обязанность для субъектов Закона № 115-ФЗ предоставлять в Росфинмониторинг по его запросам информацию в отношении операций своих клиентов и о бенефициарных владельцах своих клиентов. Аналогичная обязанность установлена для организаторов торгов на товарном или финансовом рынке (в отношении участников торгов и их клиентов), клиринговых организаций (в отношении участников клиринга), профессиональных участников рынка ценных бумаг, осуществляющих деятельность исключительно по инвестиционному консультированию (в отношении их клиентов).

В соответствии со ст. 7.2 Закона № 115-ФЗ кредитные организации и организации федеральной почтовой связи при осуществлении безналичных расчетов по банковским счетам и переводов денежных средств без открытия банковского счета (в случае организаций федеральной почтовой связи – почтовых переводов) должны обеспечить передачу в составе расчетных документов идентификационной информации о плательщике. В случае отсутствия такой информации кредитная организация и организация федеральной почтовой связи обязаны отказать в выполнении поручения плательщика, а в случае наличия подозрений о связи операции с ОД/ФТ сообщить об этом в уполномоченный орган.

Однако, в п. 12 ст. 7.2 Закона № 115-ФЗ установлены исключения для данных требований в отношении:

– безналичных расчетов и переводов на сумму, не превышающую 15 000 рублей;

– безналичных расчетов с использованием платежных карт;

– безналичных расчетов между счетами, открытыми в одной кредитной организации;

– безналичных расчетов, осуществляемых кредитными организациями от своего имени и за свой счет.

В ст. 7.3 Закона № 115-ФЗ содержится предписание для организаций, осуществляющих операции с денежными средствами или иным имуществом, принимать меры по выявлению среди своих клиентов иностранных и российских публичных должностных лиц (к российским публичным должностным лицам отнесены лица, занимающие «государственные должности Российской Федерации, должности членов Совета директоров Центрального банка Российской Федерации, должности федеральной государственной службы, назначение на которые и освобождение от которых осуществляются Президентом Российской Федерации или Правительством Российской Федерации, должности в Центральном банке Российской Федерации, государственных корпорациях и иных организациях, созданных Российской Федерацией на основании федеральных законов, включенные в перечни должностей, определяемые Президентом Российской Федерации», для определения является ли то или иное иностранное лицо публичным должностным лицом в Законе № 115-ФЗ содержится бланкетная отсылка к Рекомендациям ФАТФ [34]). На обслуживание организациями такие лица могут приниматься только с письменного согласия руководителя организации, его заместителя или руководителя обособленного подразделения. В отношении таких лиц организации должны принимать меры по определению источника денежных средств и иного имущества, а также уделять повышенное внимание операциям, совершаемым такими лицами и их близкими родственниками.

В рамках применения риск-ориентированного подхода к противодействию отмыванию преступных доходов и финансированию терроризма в Законе № 115-ФЗ содержится предписание для организаций и лиц, осуществляющих операции, оценивать уровень риска совершения подозрительных операций при приеме клиентов на обслуживание. В зависимости от уровня риска (низкий, средний, высокий) меняется частота обновления информации о клиентах (в случае низкого уровня риска – не реже одного раза в три года, в иных случаях – не реже одного раза в год).

Как отмечалось выше, организации, осуществляющие операции с денежными средствами или иным имуществом, а также иные лица, указанные в ст. 7.1 Закона № 115-ФЗ, помимо информирования Росфинмониторинга об ОПОК и подозрительных операциях должны принимать меры по блокированию денежных средств или иного имущества не позднее одного рабочего дня со дня размещения в на официальном сайте уполномоченного органа информации о включении организации или физического лица в перечень организаций и физических лиц, в отношении которых имеются сведения об их причастности к экстремистской деятельности или терроризму, с незамедлительным информированием об этом Росфинмониторинга. При этом, решение о замораживании денежных средств и иного имущества может быть принято Межведомственной комиссией по противодействию финансированию терроризма (далее – МВК по ПФТ), при наличии достаточных оснований, даже если физическое или юридическое лицо не включено в перечень организаций и физических лиц, в отношении которых имеются сведения об их причастности к экстремистской деятельности или терроризму, а также в перечни организаций и физических лиц, связанных с терроризмом или с распространением оружия массового уничтожения, составляемые в соответствии с решениями Совета Безопасности ООН [34]. Решение о замораживании денежных средств и иного имущества, принятое МВК по ФТ, публикуется на сайте Росфинмониторинга. В связи с этим стоит отметить о практике использования в работе Росфинмониторинга, так называемой, «взаимной заморозки», предполагающей обмен списками лиц, подозреваемых в причастности

к террористической деятельности, между финансовыми разведками иностранных государств и российским ПФР в случае наличия подозрений, что лица, подозреваемые иностранными ПФР, находятся в России, а лица из списка Росфинмониторинга - за границей [68].

Организации обязаны приостанавливать операции в случае, если одной из сторон является юридическое лицо, которое находится в собственности или под контролем лица, в отношении которых применены меры по замораживанию денежных средств или иного имущества. Информация о приостановлении операций передается в уполномоченный орган, который либо принимает решение о признании приостановления операций обоснованным и издает постановление о приостановлении операций сроком до 30 суток (на больший срок операции приостанавливаются по решению суда на основании заявления Росфинмониторинга), либо принимает решение о признании приостановления операций необоснованным [34].

Также у организаций, осуществляющих операции с денежными средствами и иным имуществом, есть право отказать в совершении операции при наличии подозрений в том, что операция совершается в целях ОД/ФТ [34]. Кредитные организации вправе отказаться от заключения договора в случае наличия подозрений, что целью заключения договора является ОД/ФТ, а также вправе расторгнуть договор банковского счета с клиентом в случае принятия в течение календарного года двух и более решений об отказе в совершении операции [34]. Исключение составляют клиенты, отнесенные кредитной организацией к низкой степени риска.

Обо всех случаях отказа в совершении операций, а также случаях отказа от заключения договора и расторжения договора организации обязаны сообщать в Росфинмониторинг. Уполномоченный орган передает об этом информацию в ЦБ РФ, который доводит ее до всех поднадзорных организаций. Организации используют данную информацию в целях оценки уровня риска ОД/ФТ в отношении клиента.

В целях унификации процесса оценки рисков клиента в 2022 году Банком России запущена платформа «Знай своего клиента» (в декабре 2021 года состоялся тестовый запуск). В платформе содержится информация об уровне риска юридических лиц и индивидуальных предпринимателей. Платформой предусмотрено присвоение банковским клиентам различных индикаторов в соответствии с группой риска ОД/ФТ. Благонадежным клиентам присваивается зеленый индикатор, клиентам, в деятельности которых присутствуют тревожные факторы присваивается желтый индикатор, клиентам с высоким уровнем риска ОД/ФТ присваивается красный индикатор. Тот или иной уровень присваивается клиенту в соответствии с рядом критериев, утвержденных Советом директором Банка России, на основе сведений об юридическом лице (далее – ЮЛ) или индивидуальном предпринимателе (далее – ИП), содержащихся в Едином государственном реестре юридических лиц (далее – ЕГРЮЛ) и Едином государственном реестре индивидуальных предпринимателей (далее – ЕГРИП), операций по счетам, оценки учредителей и руководителей ЮЛ, а также личности ИП, данных, полученных от государственных органов и в соответствии с Национальной оценкой рисков ОД/ФТ [147].

Информация платформы «Знай своего клиента» является для кредитных организаций вспомогательной, решение о присвоение уровня риска тому или иному клиенту, а также о подключении к платформе «Знай своего клиента» принимаются кредитными организациями самостоятельно [147].

При подключении кредитной организацией к платформе в соответствии с Законом № 115-ФЗ (в тексте федерального закона используется формулировка об использовании информации Банка России) в отношении ЮЛ и ИП, отнесенных к высокому уровню риска, кредитным организациям предписывается:

– запретить таким клиентам использование электронных средства платежа и системы быстрых платежей платежной системы Банка России;

– не проводить операцию по снятию денежных средств с банковского счета и по выдаче наличных денежных средств;

– не выдавать при расторжении договора банковского счета остаток денежных средств на счете либо не перечислять его на другой счет.

В п. 6 ст. 7.7 Закона № 115-ФЗ содержится ограниченный список операций, которые разрешается совершать клиенту, отнесенному к высокому уровню риска ОД/ФТ.

Помимо вышеперечисленных организаций и лиц в Росфинмониторинг необходимую для осуществления функций ведомства предоставляют органы государственной власти Российской Федерации, Центральный банк Российской Федерации, органы государственной власти субъектов Российской Федерации, органы местного самоуправления, государственные корпорации, Фонд пенсионного и социального страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования, а также иные организации, указанные в ст. 9 Закона № 115-ФЗ.

Росфинмониторинг в случае выявления операций, в отношении которых имеются достаточные основания предполагать их связь с ОД/ФТ, а также с иными преступлениями, направляет информацию в правоохранительные и налоговые органы, как по собственной инициативе, так и по запросу органов государственной власти. Также в полномочия Росфинмониторинга в соответствии с Положением о Федеральной службе по финансовому мониторингу, утвержденном Указом Президента РФ от 13 июня 2012 года № 808 «Вопросы Федеральной службы по финансовому мониторингу», входит информирование государственных органов об угрозах национальной безопасности, которые возникают в результате совершения операций с денежными средствами или иным имуществом [38].

В целях минимизации рисков отмывания доходов, полученных преступным путем, и финансирования терроризма Росфинмониторинг проводит национальную оценку рисков легализации преступных доходов и национальную оценку рисков финансирования терроризма. В соответствии с результатами национальной оценки рисков (далее – НОР) надзорные органы составляют оценку рисков ОД/ФТ по секторам экономической деятельности (секторальные оценки рисков). Результаты

НОР и секторальной оценки рисков используются при организации надзора за выполнением положений антиотмывочного законодательства.

Для анализа поступающих ФЭС, а также при организации деятельности ведомства Росфинмониторинг использует Единую информационную систему в сфере противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (далее – ЕИС в сфере ПОД/ФТ), состоящую из компонентов, обеспечивающих организационную и аналитическую деятельность [150]. В рамках реагирования на вызовы, связанные с цифровизацией экономики, Росфинмониторинг осуществляет работу по модернизации ЕИС в сфере ПОД/ФТ. Так, в январе 2023 года Росфинмониторинг объявил тендер на модернизацию модуля «Мониторинг и анализ криптовалютных транзакций» ЕИС в сфере ПОД/ФТ. Модернизация предполагает расширение состава криптовалют, улучшение анализа сведений о владельцах криптовалютных адресов, обеспечение о начале движения средств по криптовалютному адресу. По мнению члена экспертного совета рабочей группы по криптовалютам Государственной Думы Российской Федерации Михаила Успенского модернизация модуля позволит Росфинмониторингу создать реестр адресов криптокошельков в привязке к их владельцам [112].

Стоит отметить наличие у Росфинмониторинга программного продукта, предназначенного для анализа криптовалютных транзакций под названием «Прозрачный блокчейн». О разработке данного ПО впервые было сообщено в августе 2020 года. Тогда служба сообщила о разработке прототипа программного продукта для использования в отношении криптовалюты Bitcoin и его применении в сфере противодействия незаконному обороту наркотиков. Указывалось, что для анализа криптовалютных транзакций в «Прозрачном блокчейне» применяются технологии искусственного интеллекта. Также отмечалось, что проект до того момента разрабатывался за счет внебюджетных средств, но в целях развития нуждается в бюджетном финансировании [154]. Об использовании «Прозрачного блокчейна» в деятельности Росфинмониторинга сообщил директор Федеральной службы по финансовому мониторингу Юрий Анатольевич Чиханчин на встрече с

Президентом Российской Федерации Владимиром Владимировичем Путиным в феврале 2021 года, где было отмечено о том, что благодаря использованию «Прозрачного блокчейна» были возбуждены уголовные дела [69]. Об осуществлении усовершенствования продукта Росфинмониторингом совместно с ВТБ было сообщено на встрече директора Росфинмониторинга с Президентом Российской Федерации 9 марта 2023 года. Юрий Анатольевич отметил, что программный продукт позволяет отслеживать транзакции более 20 криптовалют. Также директор Росфинмониторинга сообщил об использовании «Прозрачного блокчейна» при закрытии крупной интернет-площадки «Гидра», использовавшейся для торговли наркотиками, оружием и отмывании денег, а также при выявлении факта финансирования украинской террористической националистической организации [68].

Кроме того, Росфинмониторингом реализуются информационные решения и на уровне международного взаимодействия. В 2019 году по инициативе Росфинмониторинга решением СРПФР СНГ одобрена Концепция «О создании Международного центра оценки рисков отмывания денег и финансирования терроризма» (далее – МЦОР) [174]. 13 октября 2023 года на заседании Совета глав государств – участников СНГ подписано Соглашение об образовании МЦОР [130]. МЦОР представляет собой единое информационное пространство, содержащее сведения из информационных систем финансовых разведок СРПФР СНГ, а также открытые данные по тематике противодействия отмыванию доходов и финансированию терроризма. Помимо функционала межгосударственного информационного взаимодействия в МЦОР предусмотрена возможность формирования финансовыми разведками риск-сигналов в целях консолидации усилий ПФР-участниц СРПФР СНГ по оценке рисков ОД/ФТ [186].

Информационные системы в сфере ПОД/ФТ применяются не только финансовой разведкой, но и кредитными организациями. На рынке имеется значительное количество программных продуктов, предназначенных для автоматизации процесса анализа операций, осуществляемых кредитными организациями, на предмет выявления в них признаков ОПОК и подозрительных

операций, а также процесса формирования отчетности в соответствии с Законом № 115-ФЗ. Такие программные продукты с начала 2010-х годов применяются Газпромбанком, Сбербанком, ВТБ, Росбанком, при этом некоторые кредитные организации уже начали внедрять программные комплексы с использованием технологий искусственного интеллекта [107; 157].

В развитии механизма мониторинга ПОД/ФТ «отслеживается прямая зависимость от процессов цифровизации экономики, хоть и наблюдается временной лаг между появлением цифровых новаций и внедрением соответствующих изменений в механизм мониторинга ПОД/ФТ. Данный временной лаг обусловлен временем, затрачиваемым на диффузию инноваций, а также на выработку соответствующего организационно-технического решения государственными органами, а также частными организациями на вызовы и возможности, порождаемые цифровой инновацией.

Процесс цифровизации механизма мониторинга ПОД/ФТ начался с момента его создания и развивался по мере расширения практики использования инфокоммуникационных технологий на российском рынке и с учетом положительного зарубежного опыта использования вычислительных систем в целях организации механизма мониторинга ПОД/ФТ (например, подразделение финансовой разведки США FinCEN с 1991 года использует в своей деятельности компьютерную базу данных подозрительных операций [243])» [235, с. 3–4]. В 2006 году завершился процесс разработки первой очереди ЕИС в сфере ПОД/ФТ, направленной на «информационное и автоматизированное обеспечение основных задач, стоящих перед службой, и вопросов, отнесенных к ее компетенции» [171]. В 2013 году Росфинмониторингом был запущен Личный кабинет для подотчетных организаций и лиц с целью повышения эффективности информационного взаимодействия [159]. Первоначально функционал Личного кабинета предусматривал онлайн-доступ и поиск по Перечню террористов и экстремистов, однако затем он был расширен, и с использованием Личного кабинета стало возможно, в частности, предоставлять ФЭС об ОПОК, подозрительных операциях, а также об иных случаях, предусмотренных Законом № 115-ФЗ. В 2021 году стало

известно о запуске Росфинмониторингом Личного кабинета правоохранительных органов для реализации онлайн-обмена с правоохранительными органами информацией об оперативной обстановке, о ходе работы по отдельным запросам и делам [158].

В 2010 году была создана Единая система идентификации и аутентификации (далее – ЕСИА), первоначальное предназначение которой заключалось в регистрации граждан на Портале государственных услуг. Однако, затем ЕСИА стала использоваться для получения удаленного доступа к банковским услугам, а также в целях авторизации на ряде Интернет-ресурсов. В 2019 году произошло объединение ЕСИА с Единой биометрической системой (далее – ЕБС) [169]. Таким образом, была обеспечена возможность для граждан удаленно получать доступ к финансовым услугам при соблюдении мер надлежащей проверки клиентов (в том числе, с использованием биометрической информации). Этому предшествовал процесс распространения технологий биометрический аутентификации на рынке. Так, в 2013 году компания Apple внедрила в новую линейку смартфонов функцию распознавания отпечатка пальцев Touch ID. В 2016 году компания Samsung выпустила смартфон Galaxy Note 7 со сканером радужной оболочки глаза. В 2017 году Apple представила iPhone X с технологией распознавания лица Face ID. Кроме того, с 2016 года MasterCard, Visa и другие финансовые организации начали внедрять возможность использования биометрической аутентификации при осуществлении платежей [109]. В России в 2015 году IT-компанией VisionLabs совместно с бюро кредитных историей Equifax была запущена система распознавания лиц клиентов на межбанковском уровне, предназначенная для противодействия кредитному мошенничеству [91]. К системе подключено более 20 крупнейших банков [198].

К середине 2015-х годов «в государственном и частном секторе Российской Федерации формируется интерес к технологиям искусственного интеллекта. В 2012 году была создана компания VisionLabs, специализирующаяся на разработке систем распознавания лиц с использованием технологий машинного обучения. С 2015 года разработку схожих систем на основе технологий искусственного

интеллекта осуществляет компания N-Tech.Lab [72]. В 2017 году компания «Яндекс» представила новую версию поисковой системы, основанной на алгоритме «Королев», функционирующем с использованием искусственных нейронных сетей [133]. В 2019 году был принят Указ Президента Российской Федерации № 490 от 10 октября 2019 года, утверждающий Национальную стратегию развития искусственного интеллекта на период до 2030 года» [40; 235, с. 4]. 17 июля 2024 года директор Росфинмониторинга Чиханчин Ю.А. заявил о применении в рамках деятельности службы технологий машинного обучения в целях выявления признаков, который могут указывать на связь операций и сделок с ОД/ФТ [105].

В 2020 году Росфинмониторинг и Банк России при осуществлении контрольно-надзорной деятельности в сфере ПОД/ФТ начали активно внедрять дистанционные формы надзоры [82; 139]. Обусловлено это было прежде всего пандемией коронавируса, которая привела к нарушению цепочек поставок товаров и создала ряд сложностей для представителей бизнеса, связанных с выстраиванием в дистанционной форме отношений покупатель-продавец и работодатель-работник, в связи с чем Правительством Российской Федерации было принято решение о введении моратория на проведение проверок бизнеса. Однако, ранее с 2016 года дистанционную форму контроля в отношении подконтрольных субъектов начала реализовывать Федеральная налоговая служб в виде внедрения налогового мониторинга [193]. Предпосылкой для этого послужило активное развитие электронного документооборота в Российской Федерации, начавшееся в 2010-х годах [90].

Однако, трансформация механизма мониторинга ПОД/ФТ происходила не только в части заимствования передовых цифровых технологий, но и управления рисками ОД/ФТ, возникающими в связи с внедрением цифровых инноваций в сектор финансовых услуг [50]. Так, исследователи отмечают, что цифровизация в сфере финансовых услуг Российской Федерации началась с платежных услуг, проявлением чего стали интернет-банкинг, электронные деньги и кошельки, мобильные платежи через операторов сотовой связи [246].

Технология интернет-банкинга начала распространяться в России в конце 1990-х годов. Первым отечественным банком, предоставившим возможность дистанционного управления банковским счетом по телефону, считается «Гута-банк», запустивший данную услугу в 1997 году, и заменивший ее через 2 года на дистанционное банковское обслуживание (далее – ДБО) через Интернет [95]. В 2009 году число активных пользователей интернет-банкинга в России оценивали уже в 1,5 млн человек (более 1% населения) [168]. В 2013 году по оценкам экспертов на интернет-транзакции приходилось до 35,3% от общего количества платежей физических лиц (а также 15,3% от общего объема платежей) [58]. В 2023 году, согласно опросу, проведенному аналитическим центром НАФИ, мобильным банкингом пользовались 70% россиян [103].

Резкий рост популярности ДБО потребовал выработки мер противодействия использованию данных услуг в противозаконных целях (в том числе, в целях ОД/ФТ). В письме Банка России от 27 апреля 2007 г. № 60-Т «Об особенностях обслуживания кредитными организациями клиентов с использованием технологии дистанционного доступа к банковскому счету клиента (включая интернет-банкинг)» было рекомендовано кредитным организациям «после предварительного предупреждения отказывать клиентам в приеме от них распоряжений на проведение операции по банковскому счету (вкладу), подписанных аналогом собственноручной подписи, в случае выявления сомнительных операций клиентов» [144]. В письме Банка России от 31 марта 2008 г. № 36-Т «О Рекомендациях по организации управления рисками, возникающими при осуществлении кредитными организациями операций с применением систем интернет-банкинга» содержались рекомендации по организации системы управления банковскими рисками, связанными с интернет-банкингом, включающими в себя, в том числе, риски использования ДБО в целях ОД/ФТ (в части использования интернет-банкинга в целях легализации преступных доходов и финансирования терроризма был отмечен повышенный риск совершения данных операций) [146]. В практической реализации распространение среди кредитных организаций получила такая мера минимизации

рисков использования интернет-банкинга в целях ОД/ФТ, как блокировка доступа к ДБО. Об этом, в частности, заявил в декабре 2023 года заместитель директора Росфинмониторинга Герман Юрьевич Негляд, который отметил сложившуюся практику ограничения доступа к интернет-банкингу в целях противодействия ОД/ФТ и отметил, что Росфинмониторингом ведется работа по выработке законодательного регулирования применения данной меры ПОД/ФТ [189].

Свое дальнейшее развитие в России интернет-банкинг получил в виде запуска в 2019 году Банком России совместно с АО «Национальная система платежных карт» Системы быстрых платежей (далее – СБП), функционал которой предусматривает осуществление денежных переводов между счетами в разных банках по номеру телефона получателя (при этом, также возможно использовать СБП для осуществления платежей по QR-коду и для оплаты товаров в интернет-магазинах) [194]. Согласно статистике Банка России за 2 квартал 2024 года, шесть из десяти жителей России использовали СБП для осуществления денежных переводов, четыре из десяти – для оплаты товаров и услуг [166]. Однако, в силу своего удобства и своей популярности СБП нашла применение и среди злоумышленников, в частности, для вывода незаконно полученных денежных средств в теневой оборот [167]. В рамках работы по противодействию использования СБП для отмывания доходов, полученных преступным путем, и финансированию терроризма, Росфинмониторинг в мае 2024 года выступил с предложением включить Национальную систему платежных карт в список субъектов ПОД/ФТ для получения данных об операциях, совершаемых через Систему быстрых платежей, и с использованием карт платежной системы «Мир» [161].

Одновременно с ростом популярности интернет-банкинга шло развитие мобильных платежей через операторов сотовой связи, а также электронных денежных переводов. Мобильные платежи через операторов сотовой связи представляют собой услугу операторов сотовой связи, при помощи которой можно оплачивать товары и услуги с мобильного счета абонента. Внедрение данной услуги в Российской Федерации началось в середине 2000-х годов (при этом,

начало развития мобильной коммерции, в целом, в России связывают с появлением у оператора сотовой связи «Билайн» услуги SMS-информирования в 2003 году [212]). Так, в 2005 году ПАО «Вымпелком» была запущена услуга «Мобильный кошелек», которая позднее трансформировалась в «Универсальную услугу Мобильного платежа» [148]. По данным за IV квартал 2007 года к данной услуге было подключено уже около 140 тыс. человек [111]. Развитием услуги мобильной оплаты товаров и услуг стала возможность осуществления денежных переводов между счетами мобильных телефонов. В частности, в 2018 году стало известно о том, что операторы сотовой связи «Мегафон» и МТС договорились о бесплатном осуществлении денежных переводов со счета одного мобильного телефона на счет другого [62]. При этом, ранее в 2016 году «Мегафон» осуществил выпуск собственных платежных карт, в которых банковский счет был объединен со счетом мобильного телефона [113].

Развитие электронных средств платежа в России началось в 1997 году с создания электронной платежной системы CyberPlat (появление электронных денег как нового средства платежа связано с личностью Дэвида Чаума, который в 1993 году создал первую электронную платежную систему eCash) [195]. В 2002 году была создана электронная платежная система Яндекс.Деньги (в 2020 году название было изменено на «ЮMoney»), в 2007 – QIWI. Яндекс.Деньги и QIWI стали наиболее популярными в России электронными платежными системами (наряду с международной электронной платежной системой WebMoney). Так, по состоянию на конец 2018 года в системе Яндекс.Деньги было зарегистрировано около 46 млн электронных кошельков. В системе QIWI в 2019 году было зафиксировано 20 млн человек активных пользователей [203]. Рост популярности электронных платежных систем актуализировал вопрос правового регулирования деятельности данных сервисов и разработки консолидированного нормативно-правового акта, регламентирующего вопросы организации и функционирования электронных платежных систем. Таковым стал принятый 27 июня 2011 года Федеральный закон № 161-ФЗ «О национальной платежной системе», в который, помимо прочего, были включены правовые нормы,

регулирующие порядок осуществления переводов и использования электронных денежных средств, а также установлены требования к операторам электронных денежных средств. Также в законе был зафиксирован ряд определений основополагающих понятий в сфере электронных платежных систем. Так, под электронными денежными средствами в законе понимаются «денежные средства, которые предварительно предоставлены одним лицом (лицом, предоставившим денежные средства) другому лицу, учитывающему информацию о размере предоставленных денежных средств без открытия банковского счета (обязанному лицу), для исполнения денежных обязательств лица, предоставившего денежные средства, перед третьими лицами и в отношении которых лицо, предоставившее денежные средства, имеет право передавать распоряжения исключительно с использованием электронных средств платежа» [32]. Электронное средство платежа в законе определено, как «средство и (или) способ, позволяющие клиенту оператора по переводу денежных средств составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств» [32].

Появление новых средств платежа и перевода денежных средств предоставило злоумышленникам дополнительные возможности в части их использования в целях ОД/ФТ в качестве новых способов размещения, расслоения и интеграция преступного капитала [259]. Это привело к необходимости трансформации механизма мониторинга ПОД/ФТ в части учета рисков, связанных с использованием электронных платежных систем и мобильных платежей в целях ОД/ФТ. Так, отмечаем, что с принятием ранее упомянутого Федерального закона «О национальной платежной системе» были установлены лимиты на переводы электронных денежных средств в случае осуществления идентификации клиента в соответствии с требованиями Закона № 115-ФЗ и неосуществления идентификации клиента (во втором случае их значения были установлены значительно меньше) [32]. Позднее была добавлена возможность упрощенной идентификации клиента с

установлением соответствующих пороговых границ переводов электронных денежных средств. Федеральным законом от 28 июня 2013 года № 134-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия незаконным финансовым операциям» в список субъектов Закона № 115-ФЗ были включены «операторы связи, имеющие право самостоятельно оказывать услуги подвижной радиотелефонной связи», к которым позже были добавлены «также операторы связи, занимающие существенное положение в сети связи общего пользования, которые имеют право самостоятельно оказывать услуги связи по передаче данных» [27]. Федеральными законами от 3 июля 2019 года № 173-ФЗ «О внесении изменений в Федеральный закон «О национальной платежной системе» и отдельные законодательные акты Российской Федерации» и от 2 августа 2019 года № 264-ФЗ «О внесении изменений в Федеральный закон «О национальной платежной системе» и Федеральный закон «О Центральном банке Российской Федерации (Банке России)» в целях предотвращения использования анонимных кошельков в электронных платежных системах для финансирования терроризма, незаконного оборота наркотиков, а также в иных противоправных целях была установлена обязанность осуществлять идентификацию клиента-физического лица (за некоторыми исключениями) в случае пополнения таких кошельков без использования банковского счета [28; 29; 188].

Помимо роста популярности электронных денежных средств рубеж 2000-х годов и 2010-х годов отмечен появлением и такого вида виртуальных валют, как криптовалюты. «В 2009 году создателем криптовалюты Bitcoin Сатоши Накамото и группой его соратников были сгенерированы первые 50 монет новой криптовалюты. В этом же году был зафиксирован первый случай обмена криптовалюты на фиатные деньги [104]. В 2010 году была запущена первая криптовалютная биржа – BitcoinMarket [117]. К середине 2010-х годов криптовалюты получили популярность в Российской Федерации (при этом, еще в 2014 году глава Федеральной службы Российской Федерации по контролю за оборотом наркотиков Виктор Иванов сообщал об использовании в России

организованными преступными группировками, осуществляющими незаконный оборот наркотиков, Bitcoin при осуществлении взаиморасчетов)» [57; 73; 235, с. 4].

«В связи с ростом популярности криптовалют (в том числе, среди представителей преступной среды) появилась необходимость отслеживать операции, осуществляемые с их использованием. Развитие технологий искусственного интеллекта в Российской Федерации способствовало появлению возможностей для создания отечественного аппаратно-программного комплекса, предназначенного для отслеживания криптовалютных транзакций с использованием искусственного интеллекта. Таковым стал «Прозрачный блокчейн», разработка которого началась в 2020 году» [235, с. 4–5]. Также в 2020 году Указанием Банка России от 20 октября 2020 г. № 5599-У «О внесении изменений в Положение Банка России от 2 марта 2012 года № 375-П «О требованиях к правилам внутреннего контроля кредитной организации в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» в список признаков, указывающих на необычный характер операции (сделки), которые используются Росфинмониторингом для выявления операций, предположительно связанных с ОД/ФТ, были включены операции, связанные с оборотом цифровой валюты [47]. Федеральным законом № 222-ФЗ от 8 августа 2024 года «О внесении изменений в отдельные законодательные акты Российской Федерации» в список субъектов антиотмывочного законодательства были включены лица, осуществляющие майнинг криптовалют, а также лица, организующие деятельность майнинг-пула (майнинг-пулом является «объединение усилий нескольких майнеров для совместного выполнения вычислительных задач по добыче криптовалюты» [192]) [26].

«Помимо криптовалют к 2017 году популярность набрали криптотокены – цифровые объекты, основанные на технологии блокчейн, подтверждающие право их владельца на получение различного рода активов или долю владения капиталом организации [297]. Криптотокены принято разделять на три вида:

– инвестиционные токены (security tokens), которые подтверждают право на долю владения компанией, либо на возврат переданных эмитенту средств с определёнными процентами;

– утилитарные токены (utility tokens), которые предоставляют их владельцу право на получение определённого объёма товаров, работ или услуг;

– стейблкоины (stablecoins), которые предоставляют своему держателю право на получение суммы, привязанной к рыночной цене определённой валюты, криптовалюты или биржевого товара [59].

Передача прав на криптотокены от эмитентов к покупателям осуществляется посредством процедуры первичного размещения, называемой initial coin offering (ICO)» [235, с. 5; 297].

В 2020 году в Российской Федерации был принят Федеральный закон от 31 июля 2020 года № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» [36]. В рамках данного закона в российское правовое пространство были введены понятия «цифровые финансовые активы» (далее – ЦФА) и «цифровая валюта». Под ЦФА в законе понимаются «цифровые права, включающие денежные требования, возможность осуществления прав по эмиссионным ценным бумагам, права участия в капитале непубличного акционерного общества, право требовать передачи эмиссионных ценных бумаг, которые предусмотрены решением о выпуске цифровых финансовых активов в порядке, установленном настоящим Федеральным законом, выпуск, учет и обращение которых возможны только путем внесения (изменения) записей в информационную систему на основе распределенного реестра, а также в иные информационные системы» [36]. Цифровая валюта в законе раскрывается, как «совокупность электронных данных (цифрового кода или обозначения), содержащихся в информационной системе, которые предлагаются и (или) могут быть приняты в качестве средства платежа, не являющегося денежной единицей Российской Федерации, денежной единицей иностранного государства и (или) международной денежной или расчетной единицей, и (или) в качестве инвестиций

и в отношении которых отсутствует лицо, обязанное перед каждым обладателем таких электронных данных, за исключением оператора и (или) узлов информационной системы, обязанных только обеспечивать соответствие порядка выпуска этих электронных данных и осуществления в их отношении действий по внесению (изменению) записей в такую информационную систему ее правилам» [36]. Таким образом, в российское правовое поле были введены криптотокены и криптовалюты [235]. Также в соответствии с вышеуказанным законом вносились изменения в Закон № 115-ФЗ, согласно которым субъектами антиотмывочного законодательства стали «операторы информационных систем, в которых осуществляется выпуск цифровых финансовых активов, и операторы обмена цифровых финансовых активов» [34].

В 2022 году в России получили лицензии Банка России первые компании – операторы обмена ЦФА. Также в 2022 году была заключена первая сделка с цифровым финансовым активом, по которой Росбанк приобрел цифровой токен на металл палладий на блокчейн-платформе «Атомайз». Эмитентом токена стал GPF Investments [65]. Согласно данным рейтингового агентства АКРА, объем рынка ЦФА в Российской Федерации по состоянию на конец 2023 года составил около 60 млрд рублей [187]. По оценкам аналитиков агентства к 2026 году рынок ЦФА в умеренно-оптимистичном сценарии может достичь 500 млрд рублей.

Наряду с бумом криптовалют и криптотокенов с середины 2010-х начинается рост интереса к технологии блокчейн. Исследователи связывают начало активного продвижения технологии блокчейн в Российской Федерации с заявлением, сделанным председателем руководства «Сбербанка» Германом Грефом на деловой встрече с Президентом Российской Федерации Владимиром Владимировичем Путиным, состоявшейся в январе 2016 года, о том, что блокчейн может существенно обновить механизмы государственного регулирования и схемы управления финансами [225]. Уже в 2016 году Банк России объявил о разработке и тестировании национальной блокчейн-сети для передачи финансовых сообщений под названием «Мастерчейн», основанной на платформе Ethereum [119]. В том же году Внешэкономбанк объявил поиск подрядчика для создания прототипа системы

«Цифровой контракт», также базирующейся на технологии блокчейн. Функционал системы должен был включать надежное хранение введенных текстов документов с перспективой контроля и анализа договорных сумм и сроков [142]. Несмотря на снижение популярности технологии блокчейн в бизнес-среде она продолжает находить свое применение в государственном секторе [124]. Примером этому является введение в Российской Федерации в 2023 году цифровой формы национальной российской валюты – цифрового рубля [191]. Функционал цифрового рубля также непосредственно связан с механизмом мониторинга ПОД/ФТ, что подробнее будет рассмотрено далее.

С учетом вышеприведенного меры по развитию механизма мониторинга ПОД/ФТ в Российской Федерации в условиях цифровизации экономики можно систематизировать в контексте внедряемых цифровых новшеств. Также возможно классифицировать внедряемые нововведения по ранее упомянутым группам организационно-технологических факторов трансформации механизма мониторинга ПОД/ФТ в условиях цифровизации экономики.

Классификация мер по развитию российского механизма мониторинга ПОД/ФТ в контексте внедряемых нововведений, а также факторов, способствующих внедрению изменений в механизм мониторинга ПОД/ФТ Российской Федерации, приведена в таблице 2.

Классификация внедряемых нововведений по ранее упомянутым группам организационно-технологических факторов трансформации механизма мониторинга ПОД/ФТ в условиях цифровизации экономики приведена в таблице 3.

Таблица 2 – Классификация мер по развитию российского механизма мониторинга ПОД/ФТ в контексте внедряемых нововведений, а также факторов, способствующих внедрению изменений в механизм мониторинга ПОД/ФТ

Технология/нововведение, внедряемое в ходе цифровизации экономики	Фактор, способствующий трансформации	Меры
1	2	3
Развитие инфокоммуникационных технологий и средств связи	Повышение скорости обмена информацией и увеличение объема передаваемых в единицу времени данных, что способствует повышению оперативности реагирования на операции, связанные с ОД/ФТ, а также скорости обмена информацией между субъектами всех уровней механизма мониторинга ПОД/ФТ	Разработка и внедрение ЕИС в сфере ПОД/ФТ, начиная с 2006 года; Создание и развитие систем обмена информацией в рамках деятельности Группы «Эгмонт» и СРПФР СНГ; Внедрение кредитными организациями программных комплексов в сфере ПОД/ФТ, начиная с 2010-х годов; Запуск в 2013 году Росфинмониторингом Личного кабинета для подотчетных организаций и лиц; Открытие Росфинмониторингом Личного кабинета правоохранительных органов в 2021 году; Создание МЦОР в 2023 году
Электронный документооборот	Возможность осуществления дистанционного мониторинга за соблюдением законодательства в сфере ПОД/ФТ в связи с наличием возможности удаленной проверки отчетной документации	Внедрение дистанционных форм надзора при осуществлении Банком России и Росфинмониторингом контрольно-надзорной деятельности в сфере ПОД/ФТ в 2020 году
Искусственный интеллект	Повышение аналитических возможностей в части обработки поступающей информации в целях выявления признаков ОД/ФТ в совершаемых операциях и сделках	Использование кредитными организациями программных комплексов, основанных технологиях искусственного интеллекта, для выявления подозрительных операций; Применение в деятельности Росфинмониторинга технологий машинного обучения в целях выявления признаков, который могут указывать на связь операций и сделок с ОД/ФТ

Продолжение таблицы 2

1	2	3
Искусственный интеллект (продолжение)	Повышение аналитических возможностей в части обработки поступающей информации в целях выявления признаков ОД/ФТ в совершаемых операциях и сделках	Разработка Росфинмониторингом программного комплекса, предназначенного для отслеживания криптовалютных транзакций с использованием искусственного интеллекта «Прозрачный блокчейн» в 2020 году; Обзор проблем и возможностей, связанных, в том числе, с использованием искусственного интеллекта в целях ПОД/ФТ в отчете ФАТФ «Возможности и проблемы новых технологий в сфере ПОД/ФТ» от 2021 года [69]
Биометрическая идентификация	Снижение времени, необходимого для осуществления процедур надлежащей проверки клиентов	Объединение ЕСИА, используемой, в том числе, для предоставления удаленного доступа к банковским услугам, с ЕБС в 2019 году; Обзор проблем и возможностей, связанных, с использованием биометрии в целях ПОД/ФТ в отчете ФАТФ «Возможности и проблемы новых технологий в сфере ПОД/ФТ» от 2021 года [69]
Интернет-банкинг	Использование интернет-банкинга в качестве средства ОД/ФТ, позволяющего быстрее осуществлять переводы денежных средств между участниками нелегальных схем	Разработка Банком России рекомендаций для кредитных организаций по управлению рисками, связанными с использованием интернет-банкинга в целях ОД/ФТ, а также рекомендаций по отказе в выполнении распоряжений клиентов, направляемых с использованием ДБО, в случае выявления признаков подозрительности
Мобильные платежи	Использование мобильных платежей в качестве средства ОД/ФТ, не охваченного требованиями антиотмывочного законодательства	Включение операторов связи в список субъектов Закона № 115-ФЗ в 2013 году; Разработка ФАТФ Руководства по применению риск-ориентированного подхода «Предоплаченные карты, мобильные платежи и онлайн-платежи» от 2013 года [164]

Продолжение таблицы 2

1	2	3
Электронные платежные системы	Использование электронных платежных систем в качестве средства ОД/ФТ, позволяющего избежать идентификации участников операций	Установление в принятом Федеральном законе «О национальной платежной системе» лимитов на переводы электронных денежных средств в случае осуществления идентификации клиента в соответствии с требованиями Закона № 115-ФЗ и неосуществления идентификации клиента в 2011 году [32]; Опубликование отчета ФАТФ «Виртуальные валюты. Ключевые определения и потенциальные риски в сфере ПОД/ФТ» от 2014 года [141]; Введение законодательного запрета на пополнение анонимных электронных кошельков без использования банковского счета в 2019 году; Издание типологического проект ЕАГ «Легализация (отмывание) преступных доходов от киберпреступлений, а также финансирование терроризма за счет указанной преступной деятельности, в том числе с использованием электронных денег или виртуальных активов и инфраструктуры их провайдеров» от 2022 года [101]
Криптовалюты	Использование криптовалют в качестве средства ОД/ФТ, не охваченного требованиями антиотмывочного законодательства, а также функционала ряда криптовалют (и инструментов, применяемых при осуществлении транзакций) в целях сокрытия отправителя/получателя виртуальных активов	Включение в 2018 году в Рекомендацию 15 ФАТФ мер по регулированию деятельности провайдеров услуг виртуальных активов

Продолжение таблицы 2

1	2	3
Криптовалюты (продолжение)	Использование криптовалют в качестве средства ОД/ФТ, не охваченного требованиями антиотмывочного законодательства, а также функционала ряда криптовалют (и инструментов, применяемых при осуществлении транзакций) в целях сокрытия отправителя/получателя виртуальных активов	Опубликование ФАТФ отчета «Виртуальные валюты. Ключевые определения и потенциальные риски в сфере ПОД/ФТ» от 2014 года, Руководства по применению риск-ориентированного подхода ФАТФ «Виртуальные активы и провайдеры услуг в сфере виртуальных активов» от 2019 года, а позднее Обновленного руководство по применению риск-ориентированного подхода «Виртуальные активы и провайдеры услуг в сфере виртуальных активов» от 2021 года и иных документов в части оценки рисков, связанных с использованием криптовалют в целях ОД/ФТ [135; 141; 163]; Разработка Росфинмониторингом программного комплекса, предназначенного для отслеживания криптовалютных транзакций с использованием искусственного интеллекта «Прозрачный блокчейн» в 2020 году; Внесение в перечень признаков, указывающих на необычный характер операции (сделки), операций, связанных с оборотом цифровых валют в 2020 году; Издание типологического проекта ЕАГ «Легализация (отмывание) преступных доходов от киберпреступлений, а также финансирование терроризма за счет указанной преступной деятельности, в том числе с использованием электронных денег или виртуальных активов и инфраструктуры их провайдеров» от 2022 года [101]; Включение лиц, осуществляющих майнинг криптовалют, а также лиц, организующих деятельность майнинг-пула, в список субъектов Закона № 115-ФЗ в 2024 году

Продолжение таблицы 2

1	2	3
Криптотокены	Возможность использования такого нового финансового инструмента, как криптотокены в качестве средства ОД/ФТ, не охваченного требованиями антиотмывочного законодательства	Принятие Федерального закона от 31 июля 2020 года № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации», регламентирующего выпуск и оборот ЦФА [36]; Включение операторов информационных систем, в которых осуществляется выпуск ЦФА, и операторов обмена ЦФА в список субъектов Закона № 115-ФЗ в 2020 году

Источник: составлено автором.

Таблица 3 – Классификация внедряемых нововведений по группам организационно-технологических факторов трансформации механизма мониторинга ПОД/ФТ в условиях цифровизации экономики

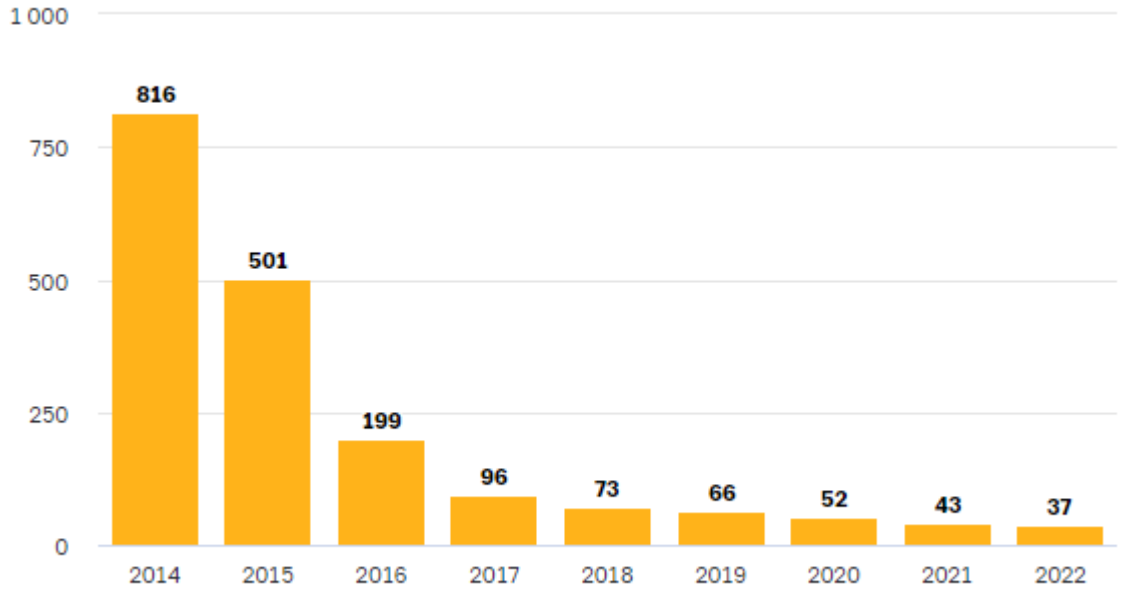
Технология/нововведение, внедряемое в ходе цифровизации экономики	Группа организационно-технологических факторов цифровизации экономики, влияющих на механизм мониторинга ПОД/ФТ		
	На микроуровне	На национальном уровне	На наднациональном уровне
1	2	3	4
Развитие инфокоммуникационных технологий и средств связи	а1; а2; а3; б3	а1; а2; а3; б3	а1; а2; а3; б3
Электронный документооборот	-	а3	-
Искусственный интеллект	а1	а1	а1
Биометрическая идентификация	а3	а3	а3
Интернет-банкинг	б1; б3	б1; б3	б1; б3
Мобильные платежи	б1	б1	б1
Электронные платежные системы	б1	б1	б1
Криптовалюты	б1	б1; б2	б1; б2
Криптотокены	б1	б1	-

Источник: составлено автором.

Следовательно, можно отметить, что большинство внедряемых цифровых новаций приводят к принятию мер по трансформации механизма мониторинга ПОД/ФТ на всех уровнях механизма мониторинга ПОД/ФТ. Меры на микроуровне механизма мониторинга ПОД/ФТ зачастую выражаются в выработке новых и адаптации существующих практик финансового мониторинга к внедряемым новшествам (как в части учета рисков ОД/ФТ, связанных с внедрением нововведений, а также приведения процесса внутреннего контроля в соответствие с изменениями законодательства, так и посредством использования преимуществ новых технологий в целях повышения эффективности осуществления процедур механизма мониторинга ПОД/ФТ на микроуровне). Меры на национальном уровне механизма мониторинга ПОД/ФТ преимущественно выражаются в адаптации нормативно-правовой основы механизма мониторинга ПОД/ФТ и практической деятельности органов финансового контроля и Росфинмониторинга к внедряемым цифровым новшествам (а также использовании возможностей внедряемых нововведений в целях развития национального механизма мониторинга ПОД/ФТ и повышения качества проводимых финансовых расследований). На наднациональном уровне меры, в основном, сводятся к выработке на основе изучения передовых национальных практик в сфере ПОД/ФТ рекомендаций по минимизации рисков и использованию возможностей, которые несут новые технологии в сфере ПОД/ФТ.

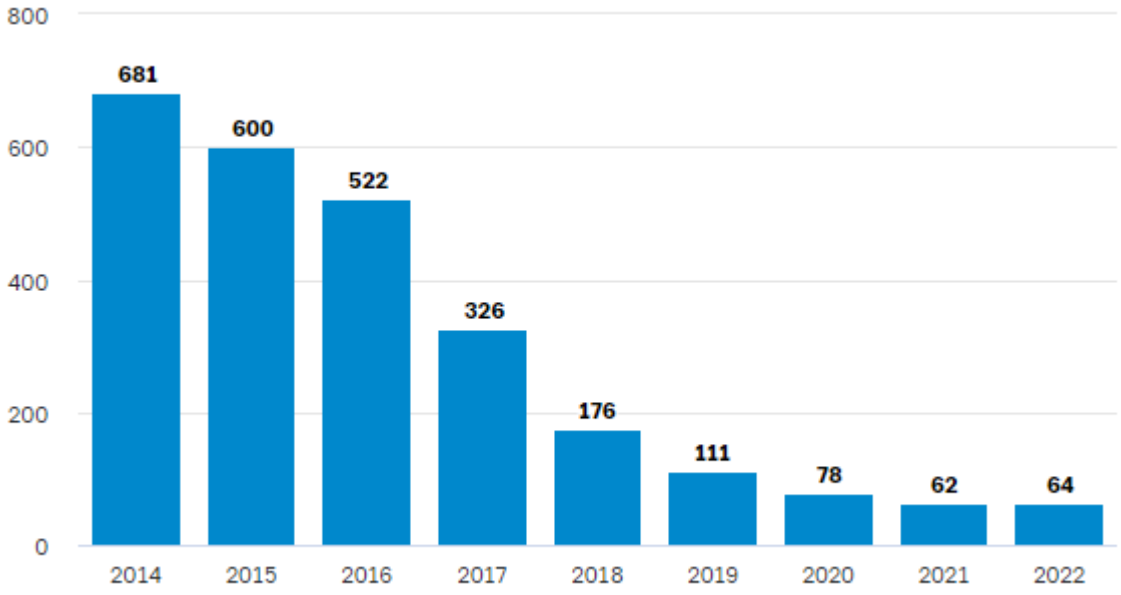
В качестве показателя эффективности российского механизма мониторинга ПОД/ФТ можно рассмотреть озвученные на встрече директора Росфинмониторинга Чиханчина Ю.А. с Президентом Российской Федерации Путиным В.В. 29 октября 2021 года, в ходе которой было отмечено возрастание стоимости теневых услуг, связанных с обналичиванием и выводом денежных средств за границу, с 1-1,5% до 20% и 40% (в случае с криптовалютами) [70].

Показателями эффективности российского механизма мониторинга ПОД/ФТ также можно считать объемы обналичивания и вывода денежных средств за границу по подозрительным основаниям, которые публикует Банк России. Данные представлены на рисунках 22; 23.



Источник: составлено [153].

Рисунок 22 – Объемы вывода денежных средств за рубеж в банковском секторе, в млрд рублей



Источник: составлено [153].

Рисунок 23 – Объемы обналичивания денежных средств в банковском секторе, в млрд рублей

Как следует из графиков, наблюдается тенденция устойчивого снижения вывода денежных средств и обналичивания в банковском секторе. Исключение наблюдается лишь в 2022 года в отношении миграции капитала за рубеж, что может быть обусловлено сложившейся международной коньюнктурой.

Таким образом, российский механизм мониторинга ПОД/ФТ заключается в направлении субъектами Закона № 115-ФЗ в адрес уполномоченного органа сообщений об ОПОК, подозрительных операциях и деятельности, а также об иных случаях, предусмотренных Законом № 115-ФЗ (в том числе о принятии мер по замораживанию денежных средств и иного имущества, принадлежащего или контролируемого лицами, причастными к террористической деятельности, о случаях отказов в заключении договоров, о случаях отказов в осуществлении операций и о случаях разрыва договоров с клиентами), с последующим анализом данных сообщений и передачей информации финансовой разведкой в правоохранительные и иные государственные органы.

Стоит отметить, что основными направлениями в части которых предпринимаются меры по развитию механизма мониторинга ПОД/ФТ являются: повышение эффективности взаимодействия между государственными ведомствами, между Росфинмониторингом и организациями и лицами, отправляющими в соответствии с Законом № 115-ФЗ информацию в уполномоченный орган, взаимодействия между ПФР различных стран, а также усиление аналитических возможностей, как кредитных организаций, так и Росфинмониторинга в части выявления, отслеживания и определения лиц, причастных к ОД/ФТ.

2.3 Изучение трансформации способов отмывания доходов, полученных преступным путем, и финансирования терроризма в условиях цифровизации экономики

Цифровизация экономики сопровождается появлением не только новых стимулов для экономического роста, но и новыми вызовами для мировой экономики и экономик национальных государств. Одним из таких вызовов является возможность использования новаций цифровой экономики для легализации преступных доходов и финансирования терроризма. Преступный элемент генетически склонен к использованию новинок в своей деятельности, так

как это может обеспечить ему скрытность своих действий и повысить уровень преступно получаемых доходов. Так, на встрече директора Росфинмониторинга с Президентом Российской Федерации 9 марта 2023 года было озвучено использование злоумышленниками государственных программ «туристический кэшбэк» и «Пушкинская карта», запущенных в 2020 и 2021 годах соответственно, злоумышленниками в целях хищения бюджетных средств. На данной же встрече были отмечены и вызовы, порождаемые цифровой экономикой. Директор Росфинмониторинга Чиханчин Ю.А. сообщил о нарастании объемов использования криптовалют. «По данным ведомства оборот криптовалют может превышать 630 тысяч биткойнов. Также глава российской финансовой разведки сообщил о том, что на мониторинге у службы находятся более 25 тысяч участников криптовалютных операций» [68; 235, с. 7].

Сопровождающим цифровизацию экономики новым способам отмывания преступных доходов и финансирования терроризма (в первую очередь, связанным с использованием криптовалют) уделяется значительное внимание в научных работах [220; 221; 228; 249; 255; 266]. Так, по мнению Хисамовой З.И. активному использованию информационно-телекоммуникационных технологий в целях ОД/ФТ способствовало их «быстрое развитие, высокая функциональность и распространенность» [266, с. 84]. М.М. Долгиева отмечает распространенность незаконного сбыта наркотических средств за криптовалюту [221]. Тогда как в работе Мурадян С.В. указывается на использование криптовалют в связке с более широким спектром предикатных преступлений: «наркоторговля, незаконный оборот оружия, легализация денежных средств, дистанционные хищения и вымогательство» [249, с. 197].

Согласно докладу Банка России «Криптовалюты: тренды, риски, меры», опубликованному в январе 2022 года, «использование криптовалют больше свойственно преступлениям наркотической направленности. Наиболее активно злоумышленниками используется криптовалюта Bitcion, позволяющая создать криптокошелек без помощи посредников в виде криптобирж. Также экспертами было отмечено использование техники разделения криптовалютного перевода на

множество мелких транзакций с использованием различных криптокошельков» [110; 235, с. 8]. Программу, осуществляющую данную технику называют, «миксер» [179]. «Суть данной программы заключается в том, что она позволяет разорвать связь между отправителем и получателем за счет того, что транзакция отправителя разбивается на несколько частей, которые затем смешиваются с аналогичными частями переводов других пользователей программы, после чего криптовалюта направляет в адрес различных криптокошельков «миксера». На конечном этапе процесса криптовалюта поступает на криптокошелек получателя в заданном размере (за исключением комиссии «миксера») из различных выбранных в случайном порядке криптокошельков. В целях сокрытия личности преступников также применяются анонимные криптовалюты, позволяющие частично или полностью скрыть данные транзакции (адрес отправителя/получателя, сумму транзакции и др.). К анонимным криптовалютам относят следующие: Dash, Monero, Zcash, SmartCash, Komodo, Pivx, Navcoin, Horizen и Verge (при этом, наибольшая степень анонимности свойственна Monero)» [5; 235, с. 8].

Согласно Национальной оценки рисков легализации (отмывания) доходов, полученных преступным путем (далее – НОР ОД), от 2022 года виртуальные активы (в соответствии с определением ФАТФ виртуальные активы – это «цифровое выражение ценности, которое может цифровым образом обращаться или переводиться и может быть использовано для целей осуществления платежей или инвестиций», при этом к виртуальным активам не относятся цифровые разновидности фиатных валют и ценных бумаг [120]) в рамках отмывания доходов могут использоваться для [131]:

– «для оплаты при осуществлении преступной деятельности с последующим выводом в фиатные валюты;

– для приобретения движимого и недвижимого имущества в юрисдикциях, в которых расчеты с использованием виртуальных активов разрешены;

– для «расслоения» преступных доходов по различным криптокошелькам и средствам платежа, а также для «разрыва» связи с доходами, полученными преступным путем;

– для сохранения анонимности владельца» [235, с. 7].

«В НОР ОД также отмечается, что наиболее часто виртуальные активы в целях легализации доходов, полученных преступным путем, использовались транснациональной организованной преступностью, контролирующей наркотрафик. При этом, для приобретения и сбыта наркотических средств использовались ресурсы сети Интернет» [235, с. 7]. Стоит отметить, что бесконтактный способ незаконной продажи наркотических средств, с которым непосредственно связано использование криптовалют, берет свое начало с 2014 года. С 2018 года начинается распространение криптовалют, как средства оплаты при осуществлении незаконного оборота наркотиков [5]. Бесконтактный способ сбыта наркотических средств осуществляется с использованием ресурсов трех видов:

– торговых площадок в закрытом сегменте сети Интернет («Даркнет»);

– интернет-мессенджеров (из которых наибольшее распространение у наркопотребителей приобрел Telegram);

– сайтов магазинов в сети Интернет в доменной зоне «.biz».

При этом, сам процесс сбыта происходит следующим образом. Покупатель регистрируется на сервисе, осуществляющем продажу незаконных субстанций. Затем клиент нелегального сервиса выбирает наркотическое вещество, а также район его получения. После этого криптовалюта списывается со счета клиента, а самому покупателю приходит ссылка, в которой содержится информация о местонахождении тайника [5]. Схожая схема применяется в чат-ботах Telegram [249]. Далее полученные средства перечисляются в качестве зарплаты на криптокошельки членов организованного преступного сообщества, а также конвертируются в фиатные валюты. Для этого криптовалютными обменниками осуществляются транзакции с использованием P2P-переводов через счета, открытые в российских кредитных организациях и зачастую зарегистрированные на подставных лиц, на указанные клиентом платежные средства (например, банковские карты) в размере, эквивалентном объему виртуальных активов [131].

Характерный пример с точки зрения использования криптовалюты в целях создания «разрыва» между преступно полученными доходами и используемыми денежными средствами имел место в случае с пользователем криптобиржи Localbitcoins. Фигурант создал на криптобирже несколько криптовалютных кошельков, после чего он вступил в переписку с трейдерами, осуществляющими продажу биткоинов за рубли на QIWI-кошельках. Полученные реквизиты QIWI-кошельков злоумышленник предоставлял лицам, приобретающим наркотические средства. Полученную криптовалюту фигурант аналогичным образом конвертировал в рубли [206].

Использованию электронных кошельков («специальное программное обеспечение, доступ к которому клиент получает непосредственно или через веб-сайт оператора электронных денежных средств в сети Интернет, осуществляемый с использованием компьютеров, мобильных устройств, иных технических устройств, позволяющих клиенту оператора по переводу денежных средств составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов» [132]) в целях отмывания преступных доходов уделяется внимание в НОР ОД, где отмечается, что электронные кошельки используются для разрыва и усложнения цепочки платежей, осуществляемых с использованием других платежных инструментов. В связи с введением ограничений на использование анонимных электронных кошельков, в последнее время получили распространение электронные кошельки, оформленные на подставных лиц [131].

«В НОР ОД отмечается, что наибольшее распространение в целях ОД получили такие криптовалюты, как Bitcoin, Monero, Etherium. Данные криптовалюты в 2021 году были указаны заместителем директора Росфинмониторинга Неглядом Г.Ю., в отношении которых были зафиксированы факты финансирования терроризма» [162; 235, с. 7].

Риски использования виртуальных активов и электронных кошельков целях финансирования терроризма отмечены в Национальной оценке рисков финансирования терроризма (далее – НОР ФТ), опубликованной в декабре

2022 года [132]. И если риск использования виртуальных активов в целях ФТ отмечен, как умеренный, то риск эксплуатации электронных кошельков градуирован, как высокий. В НОР ФТ указывается, что электронные кошельки могут использоваться в целях ФТ, как для перемещения денежных средств внутри страны, так и за ее пределы.

Схожие оценки содержатся в отчете по реализации типологического проекта ЕАГ «Легализация (отмывание) преступных доходов от киберпреступлений, а также финансирование терроризма за счет указанной преступной деятельности, в том числе с использованием электронных денег или виртуальных активов и инфраструктуры их провайдеров» от 2022 года [115]. В отчете отмечается, что информация об осуществлении сбора денежных средств с использованием виртуальных валют и электронных средств платежа размещается мессенджерах (в том числе, Telegram) и социальных сетях. Полученные денежные средства снимаются на территории стран с повышенным уровнем террористической активности после совершения ряда операций, направленных на «расслоение» поступивших средства, в том числе вывод денежных средств через несколько уровней карт, а также разделение суммы на ряд частей между не идентифицированными кошельками. На территории Российской Федерации были отмечены случаи использования в целях ФТ таких электронных платежных систем, как «Western Union», «Webmoney», «Qiwi», «Золотая корона», «Юнистрим», «Яндекс.Деньги».

Рост объем отмывания преступных доходов с использованием криптовалют отмечают также эксперты американской аналитической компании Chainalysis в докладе «О преступлениях, совершаемых с помощью криптовалюты» за 2022 год [295]. Так, эксперты выяснили, что объем криптовалюты, направленных с IP-адресов, связанных с преступной деятельностью, в 2022 году вырос на 68% по сравнению с 2021 годом и достиг 23,8 млрд долларов США. При этом, как следует из графика, начиная с 2015 года наблюдается хоть и неустойчивая, но очевидная тенденция роста объемов преступных доходов, легализуемых с использованием криптовалют, что отражено на рисунке 24.

Источник: составлено [295].

Рисунок 24 – Общий объем криптовалюты, используемой для отмывания доходов, за 2015-2022 годы, млрд долларов

Однако, стоит отдельно отметить, что к преступной деятельности эксперты Chainalysis также относят обход санкций, в связи с чем отечественный подход к квалификации доходов в качестве преступных несколько отличается от представленного Chainalysis.

Согласно данным аналитической компании, миксеры применялись в отношении 8% от общей суммы криптовалютных средств, направленных с IP-адресов, связанных с преступной деятельностью, что демонстрируется на рисунке 25.

За 2022 год в миксеры поступило средств на общую сумму 7,8 млрд долларов США, из которых 24% поступило с IP-адресов, связанных с преступной деятельностью, что превышает аналогичное значение за 2021 год, составлявшее 21%.

Также в Chainalysis отметили рост использования нелегальных сервисов (в отношении которых у экспертов Chainalysis существуют подозрения в причастности к ОД), через которые в 2022 году было легализовано средств на общую сумму 6 млрд долларов США, что отражено на рисунке 26.

Источник: составлено [295].

Рисунок 25 – Средства, полученный миксерами в разрезе источников за 2016-2022 годы, млрд долларов

Источник: составлено [295].

Рисунок 26 – Сумма средств, перемещенных через нелегальные сервисы за 2019-2022 годы, млрд долларов

Таким образом, можно отметить рост объемов денежных средств, легализация которых осуществляется в криптовалюты. В Российской Федерации наиболее распространенным к таким способам ОД предикатными преступлениями, являются связанные с незаконным оборотом наркотиков. Также возможна комбинация злоумышленниками способов ОД, совершаемых с криптовалютами и

электронными кошельками. Наблюдается рост рисков, связанных с использованием криптовалют в целях финансирования терроризма.

Также стоит отметить, что ряд угроз, не стоящих остро на момент написания исследования могут актуализироваться в дальнейшем. К таковым, например, относится использование технологий искусственного интеллекта в целях алгоритмизации процесса ОД/ФТ, а также применение smart-контрактов в качестве способа легализации денежных средств и финансирования терроризма (о данных угрозах будет упомянуто в дальнейшем).

В совокупности вышеуказанные факторы приводят к формированию следующих требований для механизма мониторинга ПОД/ФТ в условиях цифровизации экономики:

– налаживание регулирования оборота цифровых валют с точки зрения применения к обороту данных активов требований антиотмывочного законодательства;

– отработка практики отслеживания криптовалют и иных ЦФА, используемых в целях ОД/ФТ, в рамках расследования совершенных преступлений, выявления и привлечения к ответственности лиц, причастных к преступным деяниям;

– с учетом роста скорости проведения финансовых операций и оборачиваемости денежных средств (чему способствует повышение объемов безналичных платежей и внедрение цифровых валют) требуется повышение оперативности осуществления мониторинга ПОД/ФТ, в том числе по направлению в Росфинмониторинг ФЭС об ОПОК и подозрительных операциях;

– имплементация в механизм мониторинга ПОД/ФТ технологий цифровой экономики в целях снижения издержек субъектов Закона № 115-ФЗ на соответствие требованиям антиотмывочного законодательства (стоит отметить, что в условиях усиливающихся мировых тенденций по ужесточению денежно-кредитной политики сокращение издержек на соблюдение антиотмывочного законодательства может стать одним из ключевых факторов, способствующих стабильности финансового сектора);

– обеспечение необходимой динамичности в развитии механизма мониторинга ПОД/ФТ в целях реагирования на вызовы и угрозы, порождаемые внедрением новых технологий цифровой экономики в деятельность хозяйствующих субъектов;

– повышение эффективности механизма мониторинга ПОД/ФТ в рамках исполнения своего основного назначения – предотвращения отмывания преступных доходов и финансирования терроризма, а также привлечения к ответственности лиц, причастных к данным преступным деяниям.

Применительно к вышеуказанным требованиям в национальном механизме мониторинга ПОД/ФТ можно выделить следующие недостатки:

– отсутствие операторов оборота цифровых валют в списке субъектов Закона № 115-ФЗ, а также неразрешенность вопроса регулирования деятельности иностранных криптовалютных бирж;

– отсутствие в Положении Банка России от 15 декабря 2014 г. № 445-П «О требованиях к правилам внутреннего контроля некредитных финансовых организаций в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» признаков подозрительности в отношении операций с цифровыми финансовыми активами, что затрудняет процесс внедрения требований ОД/ФТ в деятельность операторов информационных систем, в которых осуществляется выпуск ЦФА, и операторов обмена ЦФА, которые относятся к некредитным финансовым организациям;

– длительный срок передачи информации об операциях, подлежащих обязательному контролю, и подозрительных операциях в Росфинмониторинг (до трех рабочих дней, что означает, что фактически срок может растянуться до пяти дней, если в период попадут выходные дни, а также на более длительный срок, в случае, если период будет включать праздничные дни). При этом, срок предоставления СПО с момента совершения операции может быть еще больше, в силу того, что срок в три рабочих дня в случае СПО отсчитывается с момента принятия окончательного решения о признании операции клиента подозрительной

(в соответствии с информационным письмом Банка России от 21.02.2005 г. № 7 «Обобщение практики применения Федерального закона «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» [96]);

– достаточно невысокий процент материалов национального подразделения финансовой разведки, по которым возбуждаются уголовные дела (составлено на основе результатов, полученных совместно с Капустиной Н.В. [231]). Так, согласно годовому отчету Росфинмониторинга в 2022 году ведомством было проведено более 6,3 тыс. финансовых расследований в кредитно-финансовой сфере, тогда как возбуждено уголовных дел по материалам Росфинмониторинга было около 1300 (около 22% от проведенных финансовых расследований) [140].

Выводы по 2 главе

В рамках анализа сущности и генезиса российского механизма мониторинга ПОД/ФТ во 2 главе рассмотрен процесс становления международного регулирования в сфере ПОД/ФТ, послужившего базисом для развития отечественного механизма мониторинга ПОД/ФТ, а также процесс развития национального механизма мониторинга ПОД/ФТ.

Международную основу механизма мониторинга ПОД/ФТ составляют Венская конвенция ООН 1988 года, Международная конвенция ООН о борьбе с финансированием терроризма 1999 года и Палермская конвенция ООН 2000 года. Однако, содержательная составляющая механизма мониторинга ПОД/ФТ раскрывается в Рекомендациях ФАТФ, а также в Вольфсбергских принципах. Важность Рекомендаций ФАТФ для стран-участниц организаций обусловлена, как накопленным опытом организации в части выстраивания механизмов мониторинга ПОД/ФТ, так и де-факто обязательностью исполнения Рекомендаций в силу наличия таких процедур, как проведение взаимной оценки и включение стран, не исполняющих Рекомендации ФАТФ, в «черный» и «серый» списки организации,

чье негативное влияние на экономическую безопасность государств рассматривалось ранее.

Российский механизм мониторинга ПОД/ФТ основывается на нормах права, закрепленных в Законе № 115-ФЗ, и принятых в соответствии с ним нормативно-правовых актах. Центральным звеном российского механизма мониторинга ПОД/ФТ является Росфинмониторинг, который получает от субъектов Закона № 115-ФЗ сообщения о подозрительных операциях и сообщения о подозрительной деятельности, сообщения об операциях, подлежащих обязательному контролю, а также сообщения в иных случаях, предусмотренных Законом № 115-ФЗ [11]. Контрольно-надзорные функции за субъектами Закона № 115-ФЗ в части предоставления необходимой информации Росфинмониторингу и обеспечения функционирования системы внутреннего контроля за операциями, которые могут быть связаны с ПОД/ФТ, осуществляют помимо самого Росфинмониторинга Банк России, Федеральная пробирная палата, Роскомнадзор, ФНС России, саморегулируемые организации аудиторов, адвокатские палаты субъектов Российской Федерации и нотариальные палаты субъектов Российской Федерации в отношении очерченного в Законе № 115-ФЗ круга поднадзорных субъектов [11]. После получения сообщений и их аналитической обработки Росфинмониторинг уполномочен направлять информацию о выявленных случаях ОД/ФТ в правоохранительные и налоговые органы. Предоставление информации в органы государственной власти Росфинмониторингом осуществляется, как по собственной инициативе, так и на основе поступающих в его адрес запросов. Также Росфинмониторинг правомочен направлять собственные запросы в адрес ряда субъектов Закона № 115-ФЗ в целях предоставления ими информации об операциях клиентов, а также об бенефициарных владельцах клиентов.

Кроме того, Законом № 115-ФЗ предусмотрено замораживание средств лиц, включенных в Перечень террористов и экстремистов, публикуемый Росфинмониторингом, а также лиц, в отношении которых принято соответствующее решение МВК по ФТ. Таким лицам запрещается осуществление любых операций, но физическим лицам может быть назначено ежемесячное

гуманитарное пособие в размере, не превышающем 10 000 рублей. Заморозке подлежат денежные средства, находящиеся на счетах юридических лицах, контролируемых лицами, в отношении которых принято решение о замораживании денежных средств, о чем сообщается в адрес Росфинмониторинга, который либо принимает решение о признании приостановления операций обоснованным, либо принимает решение о признании приостановления операций необоснованным.

Также у организаций, осуществляющих операции с денежными средствами и иным имуществом, есть право отказать в совершении операции при наличии подозрений в том, что операция совершается в целях ОД/ФТ [34]. Кредитные организации вправе отказаться от заключения договора в случае наличия подозрений, что целью заключения договора является ОД/ФТ, а также вправе расторгнуть договор банковского счета с клиентом в случае принятия в течение календарного года двух и более решений об отказе в совершении операции [34]. Помимо того, что вышеуказанные меры сами по себе являются объектами мониторинга, так как информация о них передается в Росфинмониторинга, так и представляют собой способы реализации механизма мониторинга ПОД/ФТ на микроуровне.

Еще одной составляющей механизма мониторинга ПОД/ФТ является проведение оценки рисков на предмет причастности к ОД/ФТ организациями, осуществляющими операции, при приеме клиентов на обслуживание. При этом, в Законе № 115-ФЗ устанавливается обязанность по периодическому пересмотру данной оценки [34]. В целях оценки рисков юридических лиц и индивидуальных предпринимателей может быть использована система «Знай своего клиента» Банка России. В отношении клиентов, которым присвоен высокий уровень риска, Законом № 115-ФЗ устанавливается ряд ограничений на осуществление финансовых операций.

В процедуре проведения оценки рисков клиентов с установлением ограничений для лиц, которым присвоен высокий уровень риска, процедуре блокировке средств лиц, причастных к терроризму и экстремизму, процедуре отказа организации, осуществляющей операции с денежными средствами и иным

имуществом, от совершения операции при наличии подозрений на причастность к ОД/ФТ (а также отказа кредитной организации от заключения договора с клиентом) наиболее ярко проявляется экономическая сущность реализации механизма мониторинга ПОД/ФТ, который направлена не только (как в случае, с СПО, СПД и ОПОК) на привлечение лиц, причастных к отмыванию преступных доходов и финансированию терроризма к уголовной ответственности, но и на недопущение проникновения преступных капиталов в легальный экономический оборот, последствия чего для экономической безопасности государства подробно рассмотрены в первой главе. Именно пресекательная функция механизма мониторинга ПОД/ФТ (которая несомненно реализуется и посредством привлечения лиц, причастных к ОД/ФТ, к уголовной ответственности с использованием направленной Росфинмониторингом в адрес правоохранительных органов информации на основе полученных сообщений от субъектов Закона № 115-ФЗ), выражающаяся в процессе его реализации, оказывает, по нашему мнению, наибольшее влияние на недопущение негативного эффекта от проникновения преступного капитала в законный экономический оборот и осуществления операций, направленных на ОД/ФТ, на состояние национальной экономики. В связи с этим, актуальным является повышение оперативности направления сообщений о подозрительных операциях, ОПОК, а также иных сообщений в адрес Росфинмониторинга (что позволит подразделению финансовой разведки расширить возможности по пресечению незаконных финансовых потоков), а также увеличение скорости принятия решений о приостановлении операций в случае наличия признаков ОД/ФТ, что может быть реализовано за счет частичной автоматизации процедур, а также повышения эффективности процесса оценки рисков клиентов на основе анализа разносторонних данных о них и их деятельности (для чего могут быть применены такие технологии цифровой экономики, как Big Data и искусственный интеллект).

В ходе анализа российской практики трансформации механизма мониторинга ПОД/ФТ установлена взаимосвязь между внедрением тех или иных нововведений цифровой экономики в деловую практику и развитием самого

механизма мониторинга ПОД/ФТ путем включения в него либо контрмер на риски, порождаемые цифровизацией экономики, либо самих технологий цифровой экономики, как инструментов повышения эффективности механизма мониторинга ПОД/ФТ. Данный вывод применим к технологиям искусственного интеллекта, блокчейн, биометрической идентификации, электронного документооборота, интернет-банкинга, мобильных платежей, электронных платежей, которые изначально стали проникать в деятельность хозяйствующих субъектов, после чего нашли уже свое применение в рамках механизма мониторинга ПОД/ФТ. При этом, отмечаем, что большинство внедряемых нововведений приводят к принятию мер по трансформации механизма мониторинга ПОД/ФТ на всех уровнях механизма мониторинга ПОД/ФТ. Однако, по нашему мнению, если на микроуровне и национальном уровне данные меры выражаются в непосредственной модернизации механизма мониторинга ПОД/ФТ, влекущей развитие его количественных и качественных характеристик, то применяемые на наднациональном уровне меры носят преимущественно рекомендательный характер и основаны на анализе передовых практик, сформированных в рамках национальных систем ПОД/ФТ.

Глава 3

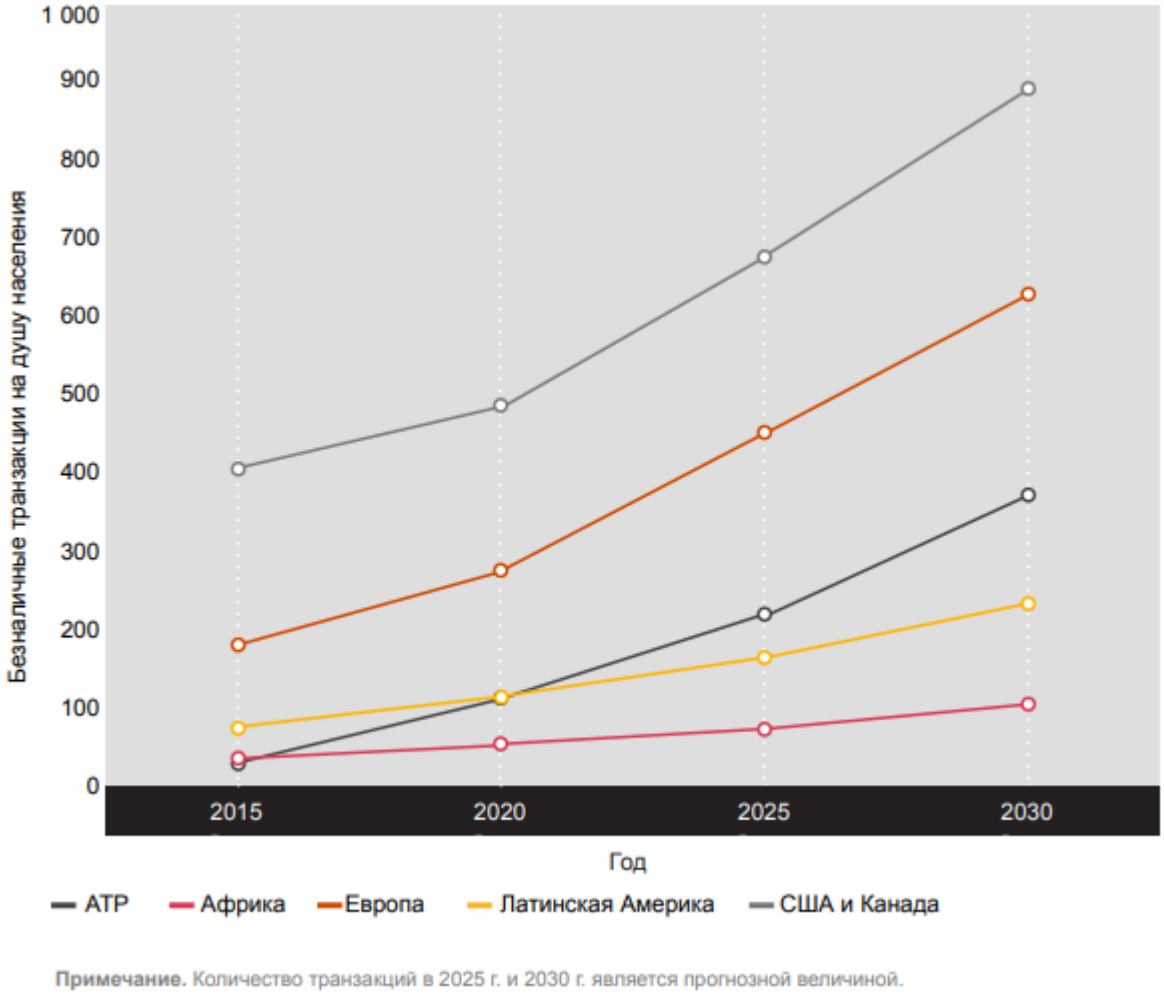
Перспективы трансформации механизма мониторинга противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма в условиях цифровизации экономики

3.1 Анализ влияния цифровизации экономики на эффективность механизма мониторинга противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма

Развитие цифровых технологий способствовало росту объемов безналичных операций. Так, в отчете консалтинговой компании PWC «Навигация в мире платежей» указывается, что если в 2020 году количество безналичных транзакций составляло 1,035 млрд, то к 2025 году ожидается рост на 82% до 1,882 млрд транзакций, а к 2030 году количество безналичных операций по мнению экспертов может достичь 3,026 млрд, что отражено на рисунке 27 [129]. Эксперты отметили две тенденции в трансформации платежной инфраструктуры: эволюция средств платежа (включая внедрение системы быстрых платежей и электронных кошельков) и революция способов платежа (в том числе, внедрение криптовалют и цифровых фиатных валют).

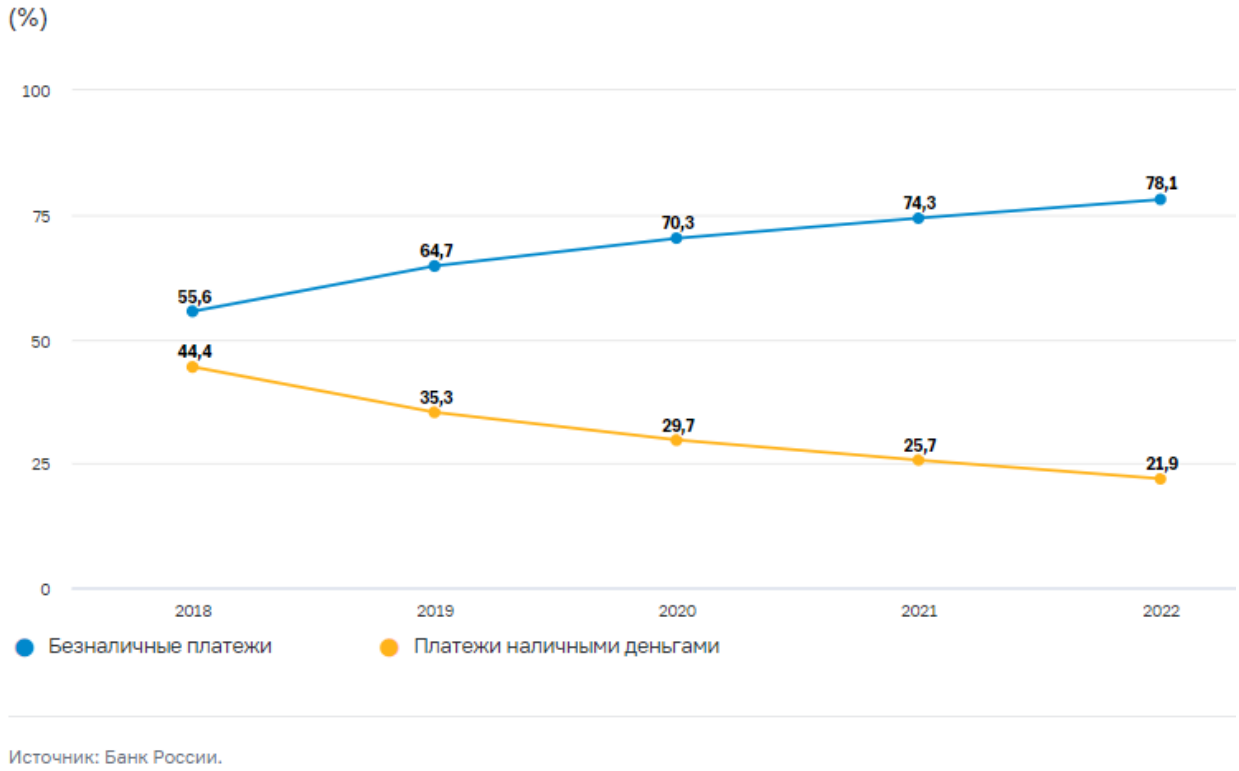
При этом, по темпам роста безналичных транзакций лидирующие позиции занимает Российская Федерация. Так, согласно исследованию Boston Consulting Group, с 2010 года по 2018 год число карточных операций в Российской Федерации увеличилось в 30 раз, а по количеству платежей Россия заняла первое место в Европе [184]. Тогда как в отчете консалтинговой компании BCG «Глобальный рынок платежных услуг 2021: ставки на рост» отмечается, что по показателю платежей по картам на душу населения Россия за период с 2010 года по 2021 год сократила отставание от лидера рейтинга – Норвегии – с 40 раз до 1,5 раза [170]. Эксперты спрогнозировали дальнейший рост платежей в России, в связи с чем за

период 2021 – 2031 гг. Российская Федерация должна выйти в лидеры рейтинга и превышать своих преследователей по количеству транзакций на 12%, а по их сумме на 9%. Рост числа и объемов безналичных операций с одной стороны повышает возможности механизма мониторинга ПОД/ФТ, так как этому сопутствует снижение объемов операций с наличными денежными средствами, а с другой стороны создает на него дополнительную нагрузку и предъявляет новые требования к программному обеспечению, осуществляющему анализ операций на предмет выявления признаков ОД/ФТ. Связь снижения доли платежей наличными денежными средствами с ростом доли безналичных платежей представлена на рисунке 28.



Источник: составлено [129].

Рисунок 27 – График роста объема безналичных платежей



Источник: составлено Банком России [102].

Рисунок 28 – Доля безналичных платежей за товары и услуги в розничном обороте

В части вызова цифровизации экономики для механизма мониторинга ПОД/ФТ многими учеными и экспертами рассматриваются криптовалюты [221; 228; 249; 250; 255]. Криптовалюты получили широкое распространение в качестве средства сбережения и даже оплаты. Так, рыночная капитализация криптовалют по состоянию на конец июня 2023 года превышала 1 трлн долларов [287]. Как было отмечено выше, криптовалюты также широко используются в качестве инструмента легализации преступных доходов и финансирования терроризма. По данным занимавшего в то время пост главы Европола Роба Вэйнрайта по состоянию на февраль 2018 года через криптовалюты отмывалось около 4% всех преступно полученных доходов в размере по меньшей мере 5,5 млрд евро [283]. По данным аналитического портала Chainalysis в 2022 году с криптовалютных адресов, принадлежащих злоумышленникам, было отправлено 23,8 млрд долларов, что на 68% больше, чем в 2021 году.

При этом, при рассмотрении конкретных характеристики криптовалют, позволяющих их использовать в качестве инструмента ОД/ФТ выделяются следующие характеристики:

– быстрота операций;

– анонимность пользователей;

– дефицит данных об операциях;

– затруднительность установления фактов использования криптовалют и отслеживания транзакций;

– отсутствие ограничений по сумме операций [255].

Здесь стоит отметить, что проблема ПОД/ФТ в случае с криптовалютами имеет два аспекта: юридический и технический. Юридический аспект проблемы охватывает вопросы, связанные с установлением правового регулирования деятельности криптобирж, в чьи обязанности должно входить проведение процедур идентификации клиента, а также передача информации об отправителе и получателем корреспондентам и надзорным органам (что, например, предусмотрено Рекомендацией 15 ФАТФ). Технический аспект проблемы связан с необходимостью отслеживания операций, совершающихся с относительно высокой скоростью (хотя стоит отметить, что скорость транзакций, например, в Bitcoin не столь высокая и может занимать от нескольких минут до нескольких часов в период пиковых нагрузок [172]), а также с преодолением техник, используемых злоумышленниками для затруднения отслеживания операций (например, с использованием миксеров). Еще одним важным аспектом, связанным с криптовалютами, является невозможность или крайняя ограниченность возможностей по заморозке операций с криптовалютами в силу особенности технологии Blockchain, не предполагающей возврата. В связи с этим, на первый план выходят технологии, позволяющие повысить эффективность механизма мониторинга ПОД/ФТ за счет усиления аналитических возможностей финансовых организаций, УНФПП и государственных органов. Одной из таких технологий является технология искусственного интеллекта.

Ранее уже отмечалось использование Росфинмониторингом технологий искусственного интеллекта (далее – ИИ) в целях отслеживания криптовалютных транзакций. Технологии ИИ находят свое применение и среди банковского сектора. Так, в феврале 2021 года о завершении автоматизации процессов ПОД/ФТ

заявили представители Росбанка [157]. Автоматизированная система имеет функционал выявления подозрительных операций, проведения финансовых расследований, а также использует алгоритмы машинного обучения для оценки уровня риска клиента. Внедрение автоматизированной системы, по словам представителя банка, позволило организации справиться с увеличением объемов финансовых операций без найма дополнительного персонала. При этом, искусственный интеллект применяется российскими банками не только для выявления операций, направленных на отмывание доходов, но и для выявления подозрительных операций, которые могут быть связаны с мошенничеством. Так, еще в 2017 году председатель правления Сбербанка Станислав Кузнецов сообщил, что специалистам Сбербанка удалось выявить схему хищения денежных средств из банкоматов с использованием систем фрод-мониторинга (система, осуществляющая анализ транзакций с целью выявления связанных с мошенничеством посредством построения математической модели финансовой активности клиента и сравнения с ней проводимых операций), в которой применяются технологии искусственного интеллекта [99]. При описании данной системы заместитель председателя правления Сбербанка Анатолий Попов в 2019 году привел следующие показатели работы системы: система фрод-мониторинга способна проверять 200 млн операций в сутки по более чем тысяче параметров. Применение системы позволило за период с июля 2018 года по май 2019 года предотвратить кражу денежных средств на сумму около 2 млрд рублей [92]. Алгоритмы искусственного интеллекта используются в антифрод-системе Почта Банка [165]. О внедрении искусственного интеллекта в деятельность банка в целях выявления мошеннических операций с банковскими картами сообщили в 2021 году представители ВТБ [71].

Аналогичные тенденции наблюдаются за границей. В июне 2023 года компания Google заявила о запуске облачного сервиса под названием Anti Money Laundering AI, использующего технологии машинного обучения в целях выявления транзакций, связанных с ОД/ФТ. В качестве отличительной черты продукта отмечено осуществление оценки подозрительности операции не на основе

предопределенных критериев, а за счет комплексного анализа уровня риска клиента на основе заданных сотрудниками организаций риск-индикаторов и типологий [301]. Продукты на основе искусственного интеллекта применяются в целях ПОД/ФТ также английским банком HSBC, бразильским Banco Bradesco и датским банком Lunar. При этом, HSBC внедрение искусственного интеллекта в свою деятельность по ПОД/ФТ (которое началось еще в 2018 году [298]) позволило сократить количество СПО, поступающих от системы мониторинга операций, на 60%, при увеличении количества сообщений, не содержащих ложных срабатываний, в 2-4 раза [301]. Подразделение финансовой разведки США FinCEN применяет систему искусственного интеллекта под названием FinCEN Artificial Intelligence System (FAIS, с английского языка Система искусственного интеллекта FinCEN), начиная с 1993 года, когда она использовалась для выявления признаков подозрительности в операциях с денежными средствами. К настоящему моменту возможности системы искусственного интеллекта FinCEN позволяют осуществлять поиск сведений в отношении частных лиц и организаций по 60 государственным и коммерческим базам данных, а также проводить анализ разрозненных сведений об одном объекте, содержащихся в различных учреждениях. Также сообщалось о проведении FinCEN работы по модернизации собственной системы искусственного интеллекта, чтобы ее функционал позволял автоматически распознавать заполненные от руки финансовые бланки и осуществлять дешифровку неправильно введенных имен, аббревиатур и других параметров [243].

Наиболее распространенными в мире программными решениями в области ПОД/ФТ являются Attivio, BAE Systems AML Regulatory Compliance, Exiger, FICO TONBELLER, Fiserv, IdentityMind, NICE Actimize, SAS [205]. В подавляющем большинстве данных программных комплексов применяются технологии искусственного интеллекта для выявления подозрительных операций.

В статье Баринова В.Р. и Бариновой Н.В. со ссылкой на исследователя Лащенко Р.А. в качестве преимущества программных комплексов ПОД/ФТ, разработанных с использованием ИИ, по сравнению с менее интеллектуальными

конкурентами отмечается то, что в традиционном программном обеспечении системы слежения выявляют типологии, которые достаточно легко обходятся. Это приводит к настройке систем таким образом, что блокируется достаточно большой массив операций. Это, в свою очередь, повышает нагрузку на сотрудников организации и, в целом, на механизм мониторинга ПОД/ФТ. В связи с этим Баринов В.Р. и Баринова Н.В. указывают, что программное обеспечение, разработанное с использованием технологий ИИ, имеет значительные перспективы, так как способно выявлять данные, недоступные для традиционного ПО.

Потенциал применения ИИ в целях выявления подозрительных операций, как в рамках традиционной банковской системы, так и в случае с виртуальными активами, отмечен также в работе Прасолова В.И. и Фешиной С.С. [255]. Применительно к криптовалютам особую актуальность технологии ИИ будут иметь, видимо, применительно к отслеживанию анонимных криптовалют, таких как Monero и ZCash. Вопросу их отслеживанию уделяется внимание не только со стороны финансовой разведки России, но и государственных органов других стран. «Так, в 2018 году Министерство внутренней безопасности США (Department of Homeland Security) запустило проект, связанный с отслеживанием анонимных криптовалют [288]. В рамках данного проекта в 2020 году аналитическая компания CipherTrace получила патенты на технологию, позволяющую отслеживать криптовалюту Monero с использованием статистических и вероятностных методов, а также создала соответствующее программное обеспечение [197]. Также в 2020 году сообщалось о старте пилотной программы Налоговой службы США (Internal Revenue Service), направленной на поиск программных инструментов для отслеживания транзакций, совершаемых с использованием анонимных криптовалют [292]. В качестве возможного решения рассматривалось ПО Coinbase Analytics, применяющее технологии ИИ для отслеживания операций» [235, с. 9; 291].

Однако, стоит отметить и обратную сторону применения технологий ИИ в контексте ПОД/ФТ. Так, Прасолов В.И. и Фешина С.С. отмечают возможность

использования нейронных сетей в целях создания механизмов мониторинга обхода требований ПОД/ФТ [255]. В настоящее время получили распространение программы-боты (специализированное программное обеспечение, выполняющее в автоматизированном режиме какие-либо действия), управляющие криптовалютой на основе заданных алгоритмов [185]. При этом, на классических финансовых рынках алгоритмическая торговля уже давно получила широкое распространение. Так, по данным английской компании по управлению активами Jupiter Asset Management по состоянию на 2018 год, 80% биржевой торговли в США контролировалось машинами [290]. Алгоритмическая торговля на финансовых рынках и в случае криптовалют может осуществляться двумя способами:

– классическим, предполагающим совершение роботом операций в соответствии с заданными правилами реагирования на то или иное развитие ситуации на рынке;

– с использованием искусственного интеллекта, способным анализировать ситуацию на фондовой и криптовалютной биржах, предсказывать поведение ее участников и выполнять иные задачи по управлению активами.

Следовательно, программа бот с применением технологий ИИ не только способна оценивать динамику активов и торговых операций, но и управлять активами в соответствии со складывающейся обстановкой на рынке. Соответственно, не стоит исключать создания программного обеспечения на основе технологий ИИ, которое содействовало бы злоумышленникам в совершении операций, направленных на отмывание преступных доходов или финансирование терроризма (при этом, такая ситуация возможна, как в случае с фондовым рынком, так и рынком криптовалют). Особая угроза такого ПО для эффективности механизма мониторинга ПОД/ФТ заключается в возможности использования в обратном направлении функционала ИИ по выявлению подозрительных операций (то есть, на основе знания признаков подозрительности операций таким образом осуществлять операции, чтобы они не фиксировались службами финансового мониторинга банков и иных субъектов антиотмывочного законодательства), а также возможностью маскировки операций в соответствии со

складывающейся ситуацией на рынке, или (в случае наличия значительных ресурсов) за счет создания на фондовом или криптовалютном рынках обстановки, способствующей сокрытию операций, направленных на ОД/ФТ.

Также в научных источниках отмечается возможность использования smart-контрактов (программное обеспечение с использованием, в ряде случаев, технологий ИИ, обеспечивающее выполнение сделки при достижении предопределенных сторонами условий) в целях ОД/ФТ [255]. Отдельный интерес в связи с этим представляют NFT (non-fungible token, с англ. невзаимозаменяемый токен – «цифровой объект с криптографической подписью, подтверждающей его уникальность; NFT могут, как сами по себе быть предметом торговли, например, в случае создания уникального художественного произведения в цифровом виде, так и цифровым представлением активов» (процитировано из статьи, подготовленной в соавторстве с Шевляковым Е.В. [271]), при торговле которыми также активно используются смарт-контракты. В опубликованном в феврале 2022 года отчете Министерства финансов США отмечаются случаи ОД/ФТ с использованием NFT, наиболее популярным способом чего является продажа и покупка NFT одной и той же организацией в целях создания записи о транзакции в блокчейн с последующей продажей NFT стороннему покупателю [126]. В качестве факторов риска ОД/ФТ с использованием NFT Минфин США отметило возможность совершения быстрых трансграничных операций, анонимность участников сделок и возможность обмена активами без посредников. В Российской Федерации проблема использования NFT в целях ОД/ФТ усугубляется также тем, что они не подпадают ни под определение ЦФА, ни под определение цифровой валюты, в связи с чем отмечается отсутствие у NFT в Российской Федерации правового статуса, что, соответственно, затрудняет работу, связанную с отслеживанием использования данного актива в целях ОД/ФТ [114; 210].

При этом, ряд авторов отмечают, что технология блокчейн помимо вышеприведенных уязвимостей с точки зрения ОД/ФТ обладает также потенциалом в области противодействия данным деяниям. Так, по мнению директора по информационным технологиям компании Standard Chartered Анжу

Патвардан блокчейн позволяет сделать финансовые операции прозрачными и отслеживаемыми [8]. Аналогичного мнения придерживается Ю Лай Чан в своей исследовательской диссертации «Отмывание доходов в ходе торговой деятельности: общая методология. Являются ли смарт-контракты в рамках технологии блокчейн возможным решением?», в которой отмечается возможность мгновенного получения финансовой документации при использовании технологии блокчейн [306]. Применительно к тематике противодействия ОД/ФТ в рамках торговых операций блокчейн позволяет обеспечить прослеживаемость всей торговой цепочки. Кроме того, по мнению автора технология блокчейн поможет повысить эффективность процедур НПК за счет наличия в цепочке всей необходимой финансовой и сопровождающей документации, что позволит банковским аналитикам в ходе оценки наличия признаков ОД/ФТ использовать всю доступную в блокчейн информацию вместо отрывочных сведений, полученных из открытых и иных источников. В то же самое время, у технологии блокчейн с точки зрения ПОД/ФТ есть ряд серьезных недостатков. Так, как отмечается в вышеприведенном исследовании Ю Лай Чана, при осуществлении транзакций в технологии блокчейн отсутствует посредник (так называемая, «доверенная сторона», роль которой в классической финансовой системе играют банки и операторы денежных переводов). Таким образом, становится невозможным осуществление такой меры ПОД/ФТ, как приостановление подозрительных операций (операция в технологии блокчейн считается необратимой или практически необратимой, что, однако, зависит от конкретной реализации технологии блокчейн). В случае со смарт-контрактами роль посредника в определенном смысле выполняет само ПО, в автоматизированном режиме отслеживающее выполнение контракта, в которое могут быть запрограммированы алгоритмы блокирования операций в случае выявления признаков ОД/ФТ. Однако, в данном случае, эффективность такой меры ПОД/ФТ, как приостановление операции, будет целиком зависеть от качества алгоритма проверки, содержащегося в смарт-контракте, а также от качества выборки данных, на которых данный алгоритм будет проходить обучение (при условии применения в смарт-контракте

искусственного интеллекта). Кроме того, необходимость проверки операций на наличие признаков ОД/ФТ до момента совершения операции в блокчейн будет также негативно сказываться на скорости совершения операций.

Однако, в отчете ФАТФ «Возможности и проблемы новых технологий в сфере ПОД/ФТ» указывается на наличие потенциала применения технологий распределенного реестра (технологий блокчейн) для ускорения процесса НПК, так как будет возможна автоматизация процедуры в рамках функционала смарт-контрактов [64]. Кроме того, возможно применение технологии блокчейн для обмена информации между финансовыми организациями, УНФПП и государственными органами в целях совершенствования процедур НПК. Так, в Китае блокчейн применяется финансовыми организациями для обмена розыскными списками и индикаторами опасности. В отчете ФАТФ приводится также пример инициативы нескольких частных компаний, осуществленной при поддержке надзорных органов, заключающейся в применении технологии блокчейн для проведения процедуры идентификации личности клиента, которая может, соответственно, применяться при НПК. Применение блокчейн для осуществления НПК может иметь ряд преимуществ, таких как ускорение процедуры НПК за счет использования цифровых устройств и автоматизации процесса, а также повышение качества процедуры НПК благодаря созданию децентрализованного реестра данных, необходимых для проверки личности клиента.

При этом, повышение скорости и качества НПК возможно не только с использованием блокчейн. Применяются иные цифровые решения для совершенствования процедур НПК. Так, в Бразилии ведущие финансовые организации применяют технологии машинного обучения при проведении оценки рисков клиентов, для выявления подставных компаний и осуществления мониторинга клиента на основе регистрационной и финансовой информации. Отмечается также положительное влияние использования финансовыми организациями Бразилии технологий машинного обучения в рамках финансового мониторинга на снижение количества ложноположительных сигналов

автоматизированных систем ПОД/ФТ [64]. Наблюдается мировая тенденция цифровизации процесса идентификации клиентов, что выражается в осуществлении обмена в электронном виде между государственными органами и финансовыми организациями данными, позволяющими идентифицировать пользователя, а также в расширении использования биометрической информации в качестве дополнительного способа верификации личности [64].

Так, в Индии внедрена система eKYC, позволяющая в электронном виде осуществить проверку личности пользователя с использованием кодов Aadhaar, выдаваемых Агентством Индии по уникальной идентификации (UIDAI). Согласно замыслу системы eKYC, клиент предоставляет свой код Aadhaar с согласием на использование персональных данных поставщику финансовых услуг, который отправляет этот номер в UIDAI, в ответ на что получает данные, необходимые для проверки личности клиента, в том числе имя, адрес, номер телефона, пол и другую информацию [302]. Взаимодействие между финансовыми организациями и UIDAI осуществляется при помощи специализированного интерфейса прикладного программирования (API) системы eKYC [302].

Также в Индии функционирует Центральный реестр НПК, управляемый Центральным реестром секьюритизации, восстановления активов и регистрации обеспечительных интересов Индии (CERSAI) и представляющий собой централизованное хранилище записей клиентов финансового сектора, сформированных при прохождении процедур НПК. Функционирование реестра позволяет клиентам финансовых организаций не предоставлять вторично идентификационные документы после успешного прохождения процедуры НПК при обращении в иные финансовые организации (при условии, что финансовая организация, осуществлявшая НПК подключена к данному реестру) [280].

Аналогичный eKYC сервис с 2016 года функционирует в Сингапуре под названием MyInfo. Сервис содержит данные из различных государственных учреждений и позволяет клиентам осуществлять денежные переводы, открывать банковские счета и совершать иные финансовые операции без необходимости

предоставления документов в рамках процедур НПК в связи с получением таковых финансовыми организациями в электронном виде с использованием сервиса [303].

Основными преимуществами вышеприведенных систем является сокращение времени необходимого для осуществления процедур НПК, расходов на осуществление данных процедур, а также повышение их качества за счет использования данных государственных учреждений. Так, по оценкам экспертом Всемирного банка применение системы eKYC позволило снизить среднюю стоимость верификации клиентов с 23 долларов США до 0,15 долларов США [300]. Кроме того, особую значимость такие системы продемонстрировали во время пандемии коронавируса, предоставив возможность пользователям удаленно получать доступ к финансовым услугам [64]. В то же время, использование систем подобных eKYC порождает риски, связанные с обеспечением защиты персональных данных, в случае компрометации подобных систем, что вызывает соответствующие опасения у их пользователей [302].

Схожие опасения в части безопасности персональных данных имеют место в отношении другого набирающего обороты способа прохождения процедур НПК – использования биометрической информации [241]. Схоже и основное достоинство данного метода – возможность удаленной идентификации.

С 2018 года в Российской Федерации действует ЕБС, созданная по инициативе Банка России и Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации. С 2020 года ЕБС имеет статус государственной информационной системы. ЕБС предполагает осуществление процедуры идентификации личности человека на основе предоставленных им заранее образцов своего голоса и изображения лица. Сбор биометрических данных осуществляется в отделениях ряда банков. Идентификация может осуществляться, как в отделении банка, так и с использованием дистанционных банковских услуг [270].

При этом, биометрическая информация не ограничивается образцами голоса и изображениями лица. Так, в соответствии со ст. 11 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» под биометрическими данными

понимаются «сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность» [33]. К таковым помимо вышеперечисленных можно также отнести отпечатки пальцев, результаты ДНК-анализа, рисунки радужной оболочки глаза и вен, особенности поведения человека в тех или иных ситуациях [270].

Соответственно, существует и разнообразие в вариациях биометрической идентификации. Так, в июле 2023 года на криптовалютной бирже Binance поступила в обращение криптовалюта Worldcoin, разработанная компанией Tools for Humanity. Worldcoin предполагает прохождение владельцем криптовалюта процесса получения ключа идентификации World ID, для чего пользователю необходимо отсканировать свою радужную оболочку глаза в специально оборудованных в ряде стран пунктах сбора биометрических данных. По замыслу создателей криптовалюты процедура биометрической идентификации позволит отличить людей от искусственного интеллекта [128]. Стоит отметить, что разработчики данной криптовалюты не являются первопроходцами в области биометрической идентификации своих пользователей. С 2017 года функционирует криптовалюта под названием AML Bitcoin, для использования которой необходимо пройти процедуру цифровой идентификации, состоящую в предоставлении документов, удостоверяющих личность и биометрической информации (лица, радужной оболочки глаз или отпечатков пальцев) [116].

Особая актуальность биометрической идентификации для криптовалютных бирж связана с удаленным характером их деятельности и невозможностью физического приема всех своих клиентов. В то же время, в научных источниках указывается на уязвимость биометрической идентификации к атакам с использованием основанной на искусственном интеллекте технологии deef-fake, позволяющей на основе образцов лица и голоса синтезировать видео- и аудио-изображения [245]. Стоит отметить, что уже был отмечен случай использования технологии deep-fake в рамках мошеннической деятельности – в 2019 году мошенниками был синтезирован голос руководителя одной из компаний, от имени которого руководителю нижестоящей организации была адресована просьба о

переводе 200 000 фунтов стерлингов поставщику из Венгрии, после чего полученные средства были выведены через цепочку переводов [127].

Цифровизация процесса идентификации клиента не сводится исключительно к цифровизации процесса сбора документов, удостоверяющих личность, и биометрической информации о человеке. В условиях роста популярности технологий ДБО (по данным Банка России дистанционным доступом к банковским счетам в мае 2021 года пользовались 75,4% взрослого населения России по сравнению с 55,2% в мае 2019 года, при этом по состоянию на май 2021 года 52,6% взрослого населения пользовались интернет-банкингом, 69,8% - мобильным банкингом [98]) возникает необходимость идентификации устройств, с которых пользователи осуществляют финансовые операции. Согласно Правилам составления кредитными организациями в электронной форме сведений и информации, предусмотренных статьями 7, 7.5 Федерального закона «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», формализованные электронные сообщения, направляемые в Росфинмониторинг кредитными организациями в отношении подозрительных операций, ОПОК, и приостановленных операций должны содержать IP-адрес и MAC-адрес оборудования плательщика [149]. При этом, ФАТФ к идентификаторам цифровых устройств помимо вышеуказанных относит также номер мобильного телефона, Сим-карту, координаты спутниковых навигационных систем [289].

Также стоит отметить влияние, оказываемое цифровыми валютами центральных банков на эффективность механизма мониторинга ПОД/ФТ. Цифровые валюты центральных банков представляют собой цифровые активы, выпускаемые центральными банками, на основе технологии блокчейн и являются частным случаем стейблкоина (цифровой актив, обеспеченный одним из традиционных и ликвидных видов активов) [265]. По сравнению с криптовалютами цифровые валюты положительно отличаются меньшей волатильностью и отсутствием анонимности, при этом сохраняя такие преимущества технологии блокчейн, как, например, возможность внедрения смарт-контрактов.

С точки зрения ПОД/ФТ цифровые валюты центральных банков, как государственный аналог криптовалют, обладают такими достоинствами, как деанонимизация проводимых финансовых операций и возможность отслеживания осуществляемых с использованием цифровых валют центральных банков операций (например, внедряемый Китаем цифровой юань, согласно заявлению Центрального банка КНР, предполагает при необходимости осуществление контроля за транзакциями [88]). Так, Бюро общественной безопасности провинции Синьми КНР в 2021 году (через год после начала тестового использования цифрового юаня) сообщило о выявлении первого случая использования цифрового юаня в целях отмывания доходов мошенниками, которые после хищения денежных средств выводили их с использованием цифрового юаня за границу. В ходе расследования было арестовано 11 человек, причастных к совершению преступления. Комментируя данное событие, эксперты отметили скорость осуществления расследования преступления с использованием цифрового юаня, отличающуюся в положительную сторону по сравнению с традиционной валютой [63]. В то же время в научных источниках отмечаются операционные сложности (в том числе, в части осуществления мер ПОД/ФТ), которые могут возникнуть у центральных банков государств в случае перехода от модели взаимодействия с коммерческими банками к взаимодействию с многопользовательской аудиторией [88; 265]. Указывается на сложность осуществления контроля за трансграничными цифровыми валютами, используемыми для международных платежей (так, в 2021 году о запуске пилотного проекта цифрового евро объявил Европейский центральный банк) [196; 265]. Также в экспертном сообществе звучат опасения в части использования цифровых валют в целях тотального контроля за финансовыми операциями граждан и ограничения экономической свободы. Так, в посвященном цифровым валютам центральных банков докладе Института Катона, опубликованном в апреле 2023 года, отмечаются, помимо прочего, такие риски цифровых валют, как возможность ограничения финансовых операций в отношении отдельных лиц или товаров, а также централизованное хранение информации о совершаемых финансовых операциях, что делает системы такого

хранения перспективными целями для злоумышленников. По результатам своего доклада эксперты пришли к выводам, что цифровые валюты центральных банков могут нести риски для стабильности финансовой системы и рекомендовали Конгрессу США законодательно запретить их выпуск [279].

С учетом вышеприведенного можно привести следующую классификацию рисков эффективного функционирования механизма мониторинга ПОД/ФТ, связанных с цифровизацией экономики:

а) «Актуальные риски ОД/ФТ:

1) использование криптовалют в целях ОД/ФТ (в первую очередь, данный риск связан с отсутствием устойчивых механизмов идентификации владельцев криптовалют, с функционированием криптовалют с повышенной степенью конфиденциальности операций), а также иных цифровых активов, в отношении которых отсутствуют устойчивые практики ПОД/ФТ (таких как NFT);

2) увеличение скорости осуществления денежных переводов, а также повышение темпов торговли на фондовом рынке (в результате внедрения алгоритмической торговли), что предъявляет повышенные требования к программным системам ПОД/ФТ в части хранения информации и скорости анализа операций на наличие признаков ОД/ФТ;

3) использование искусственного интеллекта в целях разрыва цепочки криптовалютных операций между плательщиком и получателем.

б) Потенциальные риски ОД/ФТ:

1) использование технологий искусственного интеллекта в целях алгоритмизации процесса ОД/ФТ (составлено на основе результатов, полученных совместно с Шевляковым Е.В. [271]);

2) применение smart-контрактов в целях ОД/ФТ в качестве средства сокрытия улик совершения финансовых операций в отсутствие на то экономических оснований (составлено на основе результатов, полученных совместно с Шевляковым Е.В. [271]);

3) использование технологии «deepfake» и вредоносного программного обеспечения в целях обхода биометрических средств идентификации клиента» [235, с. 8–9].

Также можно привести список преимуществ цифровизации экономики, за счет которых возможно повышение эффективности механизма мониторинга ПОД/ФТ:

а) рост процентной доли безналичных финансовых операций в общем объеме платежей способствует снижению оборота наличных денежных средств, что повышает прозрачность финансовой системы;

б) применение технологий искусственного интеллекта для отслеживания криптовалют (в том числе, криптовалют с повышенной степенью анонимности операций), а также для повышения результативности работы программных комплексов ПОД/ФТ, что позволяет за счет использования технологий машинного обучения выявлять ранее не зафиксированные схемы ОД/ФТ и снижать количество ложноположительных срабатываний;

в) использование биометрической идентификации и иных методов удаленного подтверждения личности в качестве средства проведения НПК в отсутствие личного контакта с клиентом (в том числе, клиентом криптовалютной биржи);

г) внедрение государствами и надгосударственными образованиями цифровых валют, что способствует замещению анонимных криптовалют, повышает возможности проведения финансовых расследований, а также позволяет заблокировать использование выделенных денежных средств на нецелевые нужды;

д) использование технологий искусственного интеллекта при осуществлении мер НПК, в том числе, за счет автоматизации процесса сбора информации о клиенте из открытых источников и государственных баз данных.

Отмечаем, что вышеприведенная классификация рисков и преимуществ цифровизации экономики в контексте влияния на эффективность механизма мониторинга ПОД/ФТ отличается от классификаций рисков ОД/ФТ, представленных в НОР ОД и НОР ФТ, своим акцентом на влиянии именно

технологий цифровой экономики на эффективность противодействия ОД/ФТ, а также включением в себя потенциальных рисков ОД/ФТ.

В вышеупомянутом отчете ФАТФ «Возможности и проблемы новых технологий в сфере ПОД/ФТ» также содержится список возможностей цифровых технологий в части их применения в механизме мониторинга ПОД/ФТ, а также классификация трудностей, которые могут возникнуть при внедрении новых технологий в механизм мониторинга ПОД/ФТ. Так, к числу преимуществ новых технологий для надзорных органов отнесены возможности:

– «осуществлять надзор за большим количеством учреждений;

– лучше выявлять и понимать риски, связанные с отдельными учреждениями различных секторов;

– в режиме реального времени осуществлять мониторинг соблюдения стандартов ПОД/ФТ и принимать меры в случае их несоблюдения;

– более эффективно взаимодействовать с подотчетными учреждениями и выполнять запросы о дополнительной информации;

– хранить, обрабатывать более объемные наборы надзорных данных и направлять сообщения о них;

– обмениваться информацией с другими компетентными органами» [64].

Тогда как среди преимуществ для частного сектора приведены возможности:

– «более эффективно выявлять, лучше понимать риски ОД/ФТ и более эффективно управлять ими;

– обрабатывать и анализировать более объемные наборы данных быстрее, оперативнее и точнее;

– применять более эффективные методы приема на обслуживание (цифровые);

– обеспечить проведение аудита, подотчетность и в целом хорошее управление;

– снизить затраты и максимально использовать людские ресурсы в более сложных областях ПОД/ФТ;

– повысить качество направляемых сообщений о подозрительной деятельности» [64].

Трудности и проблемы, возникающие в связи с разработкой и внедрением новых технологий, в отчете ФАТФ разделены на три вида:

– регулятивные трудности и проблемы (проблемы, связанные с отсутствием у надзорных органов необходимых технических знаний и умений, позволяющих им «понять новые технологии и надлежащим образом осуществлять надзор за их использованием» [64]);

– операционные трудности и проблемы (проблемы, связанные с адаптацией деятельности надзорных органов и субъектов антиотмывочного законодательства к новым технологиям, в том числе, затруднения, которые встречают надзорные органы в процессе внедрения новых технологий);

– нежелательные последствия и возможность противозаконного использования (проблемы, связанные с ошибками функционирования программно-аппаратных систем, созданных с использованием новых технологий, а также с возможностью компрометации данных систем).

Несмотря на то, что классификация ФАТФ избыточно описывает, возможности и проблемы, связанные с внедрением в надзорную деятельность и деятельность поднадзорных субъектов цифровых технологий, она оставляет за пределами своего внимания аспекты, связанные с возможностью использования технологий цифровой экономики злоумышленниками в целях обхода существующих и будущих требований механизма мониторинга ПОД/ФТ.

Кроме того, представленная в исследования классификация рисков и преимуществ цифровизации экономики в контексте влияния на эффективность механизма мониторинга ПОД/ФТ в силу того, что позволяет проанализировать дуалистичное (использование технологий цифровой экономики как для снижения, так и для повышения эффективности механизма мониторинга ПОД/ФТ) влияние цифровизации экономики, по нашему мнению, может быть представлена в разрезе ранее упомянутых групп организационно-технологических факторов трансформации механизма мониторинга ПОД/ФТ в условиях цифровизации

экономики, а также уровней механизма мониторинга, на которых действие данных групп факторов потребует принятия мер по трансформации механизма мониторинга ПОД/ФТ. В таблице 4 представлена классификация рисков эффективного функционирования механизма мониторинга ПОД/ФТ и преимуществ цифровизации экономики в контексте повышения эффективности механизма мониторинга ПОД/ФТ в разрезе групп организационно-технологических факторов трансформации механизма мониторинга ПОД/ФТ в условиях цифровизации экономики и уровней механизма мониторинга ПОД/ФТ.

Таблица 4 – Классификация рисков эффективного функционирования механизма мониторинга ПОД/ФТ и преимуществ цифровизации экономики в контексте повышения эффективности механизма мониторинга ПОД/ФТ в разрезе групп организационно-технологических факторов трансформации механизма мониторинга ПОД/ФТ в условиях цифровизации экономики и уровней механизма мониторинга ПОД/ФТ

Наименование риска эффективного функционирования механизма мониторинга ПОД/ФТ/ преимущества цифровизации экономики в контексте повышения эффективности механизма мониторинга ПОД/ФТ	Группа организационно-технологических факторов трансформации механизма мониторинга ПОД/ФТ в условиях цифровизации экономики		
	На микроуровне	На национальном уровне	На наднациональном уровне
1	2	3	4
«Использование криптовалют в целях ОД/ФТ, а также иных цифровых активов, в отношении которых отсутствуют устойчивые практики ПОД/ФТ» [235, с. 8]	б1	б1; б2	-
«Увеличение скорости осуществления денежных переводов, а также повышение темпов торговли на фондовом рынке, что предъявляет повышенные требования к программным системам ПОД/ФТ в части хранения информации и скорости анализа операций на наличие признаков ОД/ФТ» [235, с. 8]	б3	б3	-
«Использование искусственного интеллекта в целях разрыва цепочки криптовалютных операций между плательщиком и получателем» [235, с. 8]	-	б2	-
«Использование технологий искусственного интеллекта в целях алгоритмизации процесса ОД/ФТ» [235, с. 8]	б2	б2	-

Продолжение таблицы 4

1	2	3	4
«Применение smart-контрактов в целях ОД/ФТ в качестве средства сокрытия улик совершения финансовых операций в отсутствие на то экономических оснований» [235, с. 8]	-	б1	-
«Использование технологии «deepfake» и вредоносного программного обеспечения в целях обхода биометрических средств идентификации клиента» [235, с. 9]	б2	б2	-
Рост процентной доли безналичных финансовых операций в общем объеме платежей способствует снижению оборота наличных денежных средств, что повышает прозрачность финансовой системы	а1; а3	а1; а3	-
Применение технологий искусственного интеллекта для отслеживания криптовалют, а также для повышения результативности работы программных комплексов ПОД/ФТ, что позволяет за счет использования технологий машинного обучения выявлять ранее не зафиксированные схемы ОД/ФТ и снижать количество ложноположительных срабатываний	а1	а1	-
Использование биометрической идентификации и иных методов удаленного подтверждения личности в качестве средства проведения НПК в отсутствие личного контакта с клиентом	а3	а3	-
Внедрение государствами и надгосударственными образованиями цифровых валют, что способствует замещению анонимных криптовалют, повышает возможности проведения финансовых расследований, а также позволяет заблокировать использование выделенных денежных средств на нецелевые нужды	-	а1; а2	а1; а2

Продолжение таблицы 4

1	2	3	4
Использование технологий искусственного интеллекта при осуществлении мер надлежащей проверки клиентов, в том числе, за счет автоматизации процесса сбора информации о клиенте из открытых источников и государственных баз данных	1а	1а	-

Источник: составлено автором.

Риск использования криптовалют, а также иных цифровых активов, в отношении которых отсутствуют устойчивые практики ПОД/ФТ, в целях ОД/ФТ сводится не только к факторам трансформации механизма мониторинга ПОД/ФТ, связанным с появлением новых технологий, не охваченных требованиями антиотмывочного законодательства (что, по нашему мнению, требует выработки соответствующих мер реагирования как на национальном уровне механизма мониторинга ПОД/ФТ в части разработки нормативно-правового регулирования, так и на микроуровне в рамках адаптации практики процедур комплаенс к новым технологиям), но и к факторам использования технологий цифровой экономики в целях воспрепятствования осуществлению и реализации механизма мониторинга ПОД/ФТ в связи с возможностью использования анонимных криптовалют и криптовалютных миксеров с целью обхода требований антиотмывочного законодательства. Вторая группа факторов требует, в первую очередь, выработки мер противодействия на национальном уровне в связи с тем, что решение задачи отслеживания анонимных криптовалют и противодействия работе криптовалютных миксеров требует значительных вложений ресурсов (как в части денежных средств, так и человеческого капитала) и, как показывает практика, вырабатывается преимущественно под руководством государственных органов. Аналогичная потребность в выработке мер реагирования на национальном уровне механизма мониторинга ПОД/ФТ в силу высокой ресурсоемкости существует в отношении риска использования искусственного интеллекта в целях разрыва цепочки криптовалютных операций между плательщиком и получателем.

Однако, риск использования технологий искусственного интеллекта в целях алгоритмизации процесса ОД/ФТ может потребовать выработки мер противодействия в равной мере на двух уровнях механизма мониторинга ПОД/ФТ (микроуровне и национальном уровне), так как алгоритмизация процесса ОД/ФТ может основываться и на использовании уже имеющихся финансовых инструментов, интегрированных в механизм мониторинга ПОД/ФТ. Однако, опасность алгоритмизации ОД/ФТ заключается в том, что она может привести к усложнению схем ОД/ФТ (так как составление сложных схем станет доступным не только профильным специалистам, но и всем пользователям соответствующего программного обеспечения), а также к ускорению процессов ОД/ФТ, что может потребовать от субъектов антиотмывочного законодательства дополнительных ресурсных вложений в системы внутреннего контроля для выявления усложняющихся схем ОД/ФТ. На аналогичных уровнях механизма мониторинга ПОД/ФТ требуется выработка мер противодействия на риск использования технологии «deepfake» и вредоносного программного обеспечения в целях обхода биометрических средств идентификации клиента, так как разработка решения общегосударственного характера, а также опубликование рекомендаций по минимизации риска осуществляется на национальном уровне, тогда как реализация данного решения и внедрение рекомендаций будет осуществляться на микроуровне в силу того, что идентификация клиентов осуществляется субъектами микроуровня механизма мониторинга ПОД/ФТ.

Риск применение smart-контрактов в целях ОД/ФТ в качестве средства сокрытия улик совершения финансовых операций, в свою очередь, требует выработки мер трансформации, в первую очередь, на национальном уровне механизма мониторинга ПОД/ФТ, так как в случае расширения практики использования smart-контрактов именно на данном уровне потребуется разработка нормативно-правового регулирования их оборота (в том числе, в части учета рисков использования smart-контрактов для ОД/ФТ).

Рассматривая перечисленные в классификации преимущества цифровизации экономики, за счет которых возможно повышение эффективности механизма

мониторинга ПОД/ФТ, стоит отметить, что рост процентной доли безналичных финансовых операций в общем объеме платежей, использование биометрической идентификации и иных методов удаленного подтверждения личности в качестве средства проведения НПК, применение технологий искусственного интеллекта для отслеживания криптовалют, для повышения результативности работы программных комплексов ПОД/ФТ, а также для осуществления мер НПК приведет к трансформации механизма мониторинга ПОД/ФТ, как на микроуровне, так и на национальном уровне. При этом, использование искусственного интеллекта будет способствовать повышению аналитических возможностей субъектов механизма мониторинга ПОД/ФТ, внедрение биометрической идентификации и иных методов удаленного подтверждения личности в качестве средства проведения НПК – повышению скорости осуществления процедур надлежащей проверки клиентов, рост процентной доли безналичных финансовых операций в общем объеме платежей – как повышению аналитических возможностей механизма мониторинга ПОД/ФТ, так и росту скорости передачи информации об осуществляемых операциях в рамках механизма мониторинга ПОД/ФТ.

В части наднационального уровня механизма мониторинга ПОД/ФТ в классификации не было учтено влияние рисков и преимуществ цифровизации экономики на наднациональный уровень механизма мониторинга ПОД/ФТ, приводящее к выработке ФАТФ и РГТФ соответствующих рекомендаций, так как оно может иметь место в отношении всех перечисленных рисков и преимуществ цифровизации экономики. Соответственно, на наднациональном (и на национальном) уровне механизма мониторинга ПОД/ФТ отмечено только влияние групп факторов, связанных с повышением аналитических возможностей (в силу расширения функционала отслеживания операций), и расширением возможностей по хранению информации и ее обработке (в силу применения технологии Блокчейн), при внедрении государствами и надгосударственными образованиями цифровых валют.

Влияние цифровизации на эффективность механизма мониторинга ПОД/ФТ через призму его контрольного компонента возможно продемонстрировать на

примере контроль-надзорной деятельности, осуществляемой Банком России и Росфинмониторингом в отношении своих поднадзорных субъектов.

Согласно годовому отчету, в 2022 году Банк России провел мероприятия дистанционного надзора в отношении 353 кредитных организаций (94,6% от общего числа) [84]. В рамках контактного надзора было проведено 16 проверок кредитных организаций и 10 некредитных финансовых организаций (далее – НФО). В 2021 году таких проверок было проведено 46 в отношении кредитных организаций и 36 в отношении НФО [83]. В 2020 году было проведено в рамках контактного надзора 48 проверок кредитных организаций и 17 НФО, в 2019 году – 59 проверок кредитных организаций и 21 НФО, в 2018 году – 146 кредитных организаций и 32 НФО, в 2017 году – 200 кредитных организаций и 73 НФО, в 2016 году – 557 проверок кредитных организаций, в 2015 году – 626 кредитных организаций (статистика по проверкам НФО на предмет соблюдения требований антиотмывочного законодательства в годовых отчетах ЦБ РФ появляется с 2017 года) [77; 78; 79; 80; 81; 82]. График количества проверок, проведенных Банком России в отношении поднадзорных субъектов представлен на рисунке 29.

Источник: составлено автором на основе годовых отчетов Банка России за период 2015-2022 годов [77; 78; 79; 80; 81; 82; 83; 84].

Рисунок 29 – График количества проверок, проведенных Банком России

График в отношении проверок НФО начинается с 2017 года в связи с отсутствием информации в годовых отчетах Банка России о количестве проводимых ранее проверок в отношении НФО. Статистика надзора демонстрирует тенденции к снижению количества контактных проверок, проводимых Банком России. На смену данным проверкам приходит дистанционный надзор в сочетании с контактными проверками, проводимыми в соответствии с риск-ориентированным подходом.

Дистанционный надзор предполагает прохождение проверки только в случае наличия у Банка России информации о совершении поднадзорным субъектом действий, противоречащих требованиям Закона № 115-ФЗ. В остальных случаях дистанционный надзор выражается в требовании предоставить документы по организации системы внутреннего контроля организации, а также данные по ФЭС, направленным в Росфинмониторинга, и сведения о принятых мерах по замораживанию/блокированию денежных средств лиц, включенных в перечни Росфинмониторинга и Совета Безопасности ООН. В случае выявления нарушения составляется мотивированное заключение о наличии признаков административного правонарушения, предусмотренного ст. 15.27 КоАП РФ [138].

Характерно, что снижение количества проверок, согласно статистике Банка России, не приводит к снижению эффективности механизма мониторинга ПОД/ФТ, а имеет скорее обратный эффект. Так, отмечаем, что на ранее приведенных рисунках 22 и 23 демонстрируются тенденции снижения объемов выводимых за рубеж по подозрительным основаниям денежных средств, а также объемов обналичивания денежных средств, что совпадает с тенденциями по снижению количества контактных проверок и переходу к дистанционному надзору. По результатам проведенных нами расчетов, коэффициент корреляции между объемом выводимых за рубеж денежных средств и количеством проверок кредитных организаций составляет 0,89, что указывает на сильную корреляцию между переменными. Также установлено, что коэффициент корреляции между количеством проверок кредитных организаций и объемом обналичиваемых по подозрительным основаниям через банковский сектор денежных средств

составляет 0,98. Методика определения коэффициента корреляции и корреляционные поля представлены в приложении А.

Высокие значения корреляции между числом проверок и объемом обналичивания / вывода денежных средств могут объясняться одним из двух способов:

– Снижение количества проверок не приводит к негативному эффекту для контрольно-надзорной деятельности, а внедрение риск-ориентированного подхода позволило уделять большее внимание субъектам, наиболее уязвимым к ОД/ФТ (также может иметь место эффект очищения сектора банковских услуг от недобросовестных субъектов).

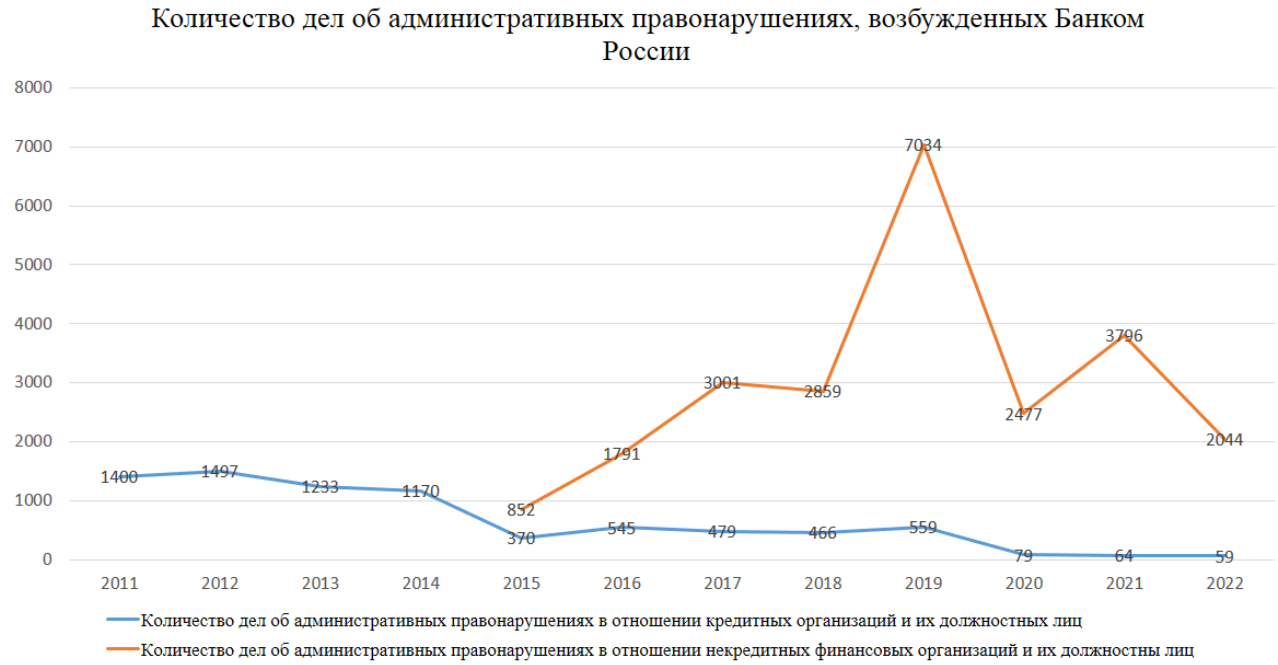
– Снижение количества проверок приводит к снижению эффективности контрольно-надзорной деятельности, в результате чего снижаются объемы выявляемых подозрительных финансовых потоков.

Для определения верности той или другой точки зрения следует обратиться к иным параметрам, которые могут охарактеризовать эффективность контрольно-надзорной деятельности. К одному из таких параметров можно отнести статистику по возбужденным Банком России делам об административных правонарушениях, предусмотренных статьей 15.27 Кодекса Российской Федерации об административных правонарушениях (КоАП РФ) («Неисполнение требований законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» [27]) в отношении кредитных организаций и их должностных лиц, а также некредитных финансовых организаций и их должностных лиц.

Статьей предусматривается административная ответственность за неисполнение требований антиотмывочного законодательства, связанных с направлением ФЭС о подозрительных операциях и ОПОК, составлением правил внутреннего контроля, блокированием денежных средств, а также иных требований Закона № 115-ФЗ.

График со статистикой приведен на рисунке 30. График с количеством дел об административных правонарушениях в отношении НФО и их должностных лиц

начинается с 2015 года в связи с тем, что контрольно-надзорные полномочия в отношении НФО были получены Банком России в 2013 году в связи с упразднением Федеральной службы по финансовым рынкам и в 2013-2014 годах данные организации не учитывались в статистике Банка России. Также отмечаем, что график с количеством дел об административных правонарушениях в отношении кредитных организаций и их должностных лиц начинается с 2011 года в связи с тем, что в 2011 году на Банк России была возложена обязанность по рассмотрению дел об административных правонарушениях, предусмотренных статьей 15.27 КоАП РФ, связанных с неисполнением кредитными организациями и должностными лицами кредитных организаций (с 2013 года также НФО и их должностными лицами) требований законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма [74; 76].



Источник: составлено автором на основе годовых отчетов Банка России за период 2011-2022 годов [74; 75; 76; 77; 78; 79; 80; 81; 82; 83; 84; 85].

Рисунок 30 – График количества дел об административных правонарушениях, возбужденных Банком России, по ст. 15.27 КоАП РФ

Коэффициент корреляции между числом контактных проверок кредитных организаций и количеством возбужденных Банком России дел об административных правонарушениях в отношении кредитных организаций и их

должностных лиц по ст. 15.27 КоАП РФ равен 0,48 (что указывает на наличие слабой корреляции между переменными). Коэффициент корреляции между числом контактных проверок некредитных финансовых организаций и количеством возбужденных Банком России дел об административных правонарушениях в отношении некредитных финансовых организаций и их должностных лиц по ст. 15.27 КоАП РФ равен – 0,05 (что указывает на отсутствие корреляции между переменными).

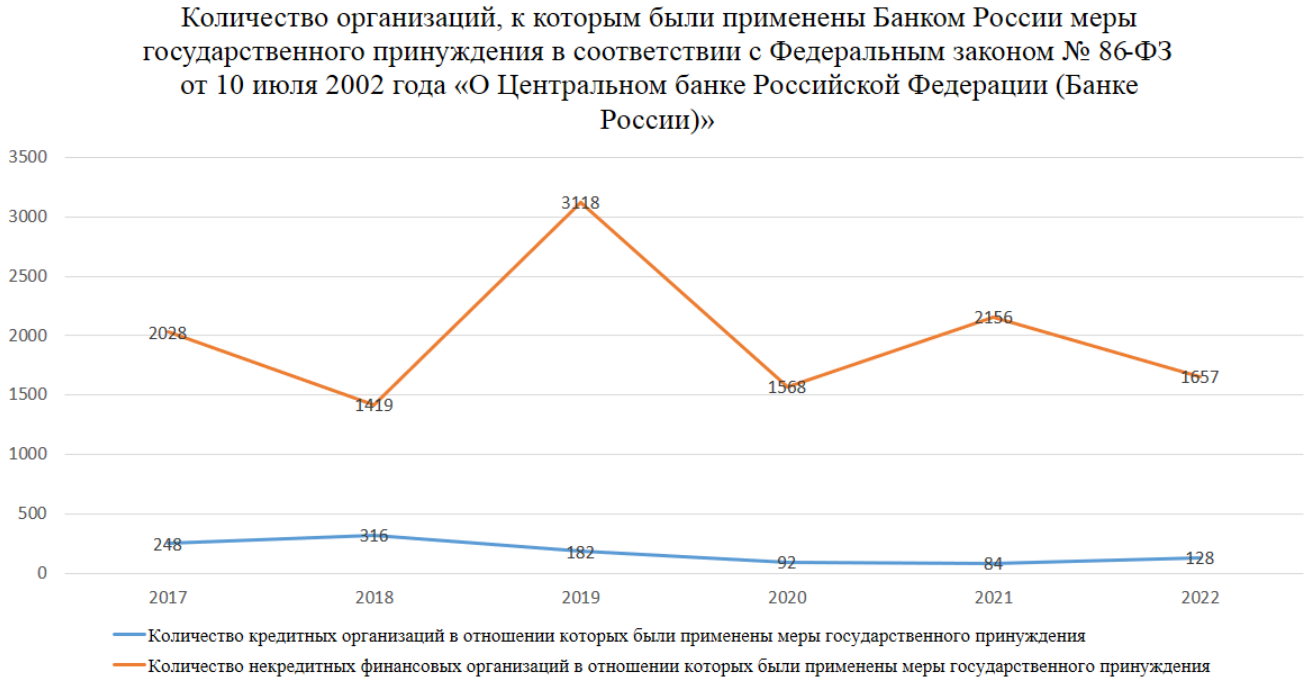
Для получения более всесторонней картины в качестве еще одного параметра оценки эффективности контрольно-надзорной деятельности возможно проанализировать статистику применения мер государственного принуждения Банком России в отношении кредитных организаций и некредитных финансовых организаций в соответствии со статьями 74 и 76.5 Федерального закона № 86-ФЗ от 10 июля 2002 года «О Центральном банке Российской Федерации (Банке России)», приведенную на рисунке 31 (статистика приводится за период с 2017 года, так как до этого Банком России использовалась в годовых отчетах методика подсчета мер принудительного характера, тогда как с 2017 года используется методика подсчета числа организаций, в отношении которых были вынесены меры) [35].

Коэффициент корреляции между числом контактных проверок кредитных организаций и количеством кредитных организаций, к которым были применены Банком России меры государственного принуждения, равен 0,81. Коэффициент корреляции между числом контактных проверок некредитных финансовых организаций и количеством некредитных финансовых организаций, к которым были применены Банком России меры государственного принуждения, по нашим расчетам, равен 0,05.

Таким образом, в случае с кредитными организациями имеется достаточно высокий коэффициент корреляции, тогда как в случае с некредитными финансовыми организациями корреляция отсутствует.

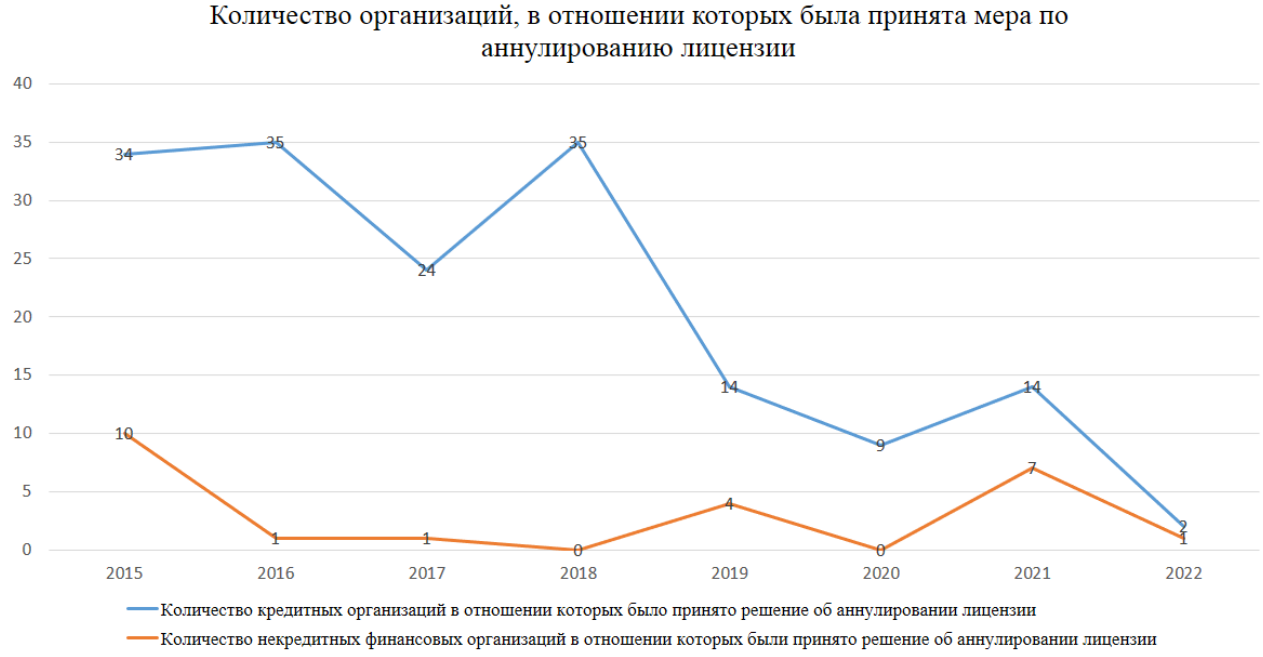
Также возможно проанализировать корреляцию между числом контактных проверок и количеством случаев отзыва лицензий у кредитных организаций и

некредитных финансовых организаций в связи с нарушением ими законодательства Российской Федерации (в том числе, требований ПОД/ФТ), которая представлена на рисунке 32.



Источник: составлено автором на основе годовых отчетов Банка России за период 2017-2022 годов [79; 80; 81; 82; 83; 84].

Рисунок 31 – Количество организаций, к которым были применены Банком России меры государственного принуждения в соответствии с Федеральным законом № 86-ФЗ от 10 июля 2002 года «О Центральном банке Российской Федерации (Банке России)»



Источник: составлен автором на основе годовых отчетов Банка России за период 2015-2022 годов [77; 78; 79; 80; 81; 82; 83; 84].

Рисунок 32 – Количество организаций, у которых Банком России были аннулированы лицензии за нарушения требований законодательства Российской Федерации (в том числе в сфере ПОД/ФТ)

Коэффициент корреляции между числом контактных проверок кредитных организаций и количеством кредитных организаций, у которых Банком России была отозвана лицензия, равен 0,78. Коэффициент корреляции между числом контактных проверок некредитных финансовых организаций и количеством некредитных финансовых организаций, у которых Банком России была отозвана лицензия, равен 0,03.

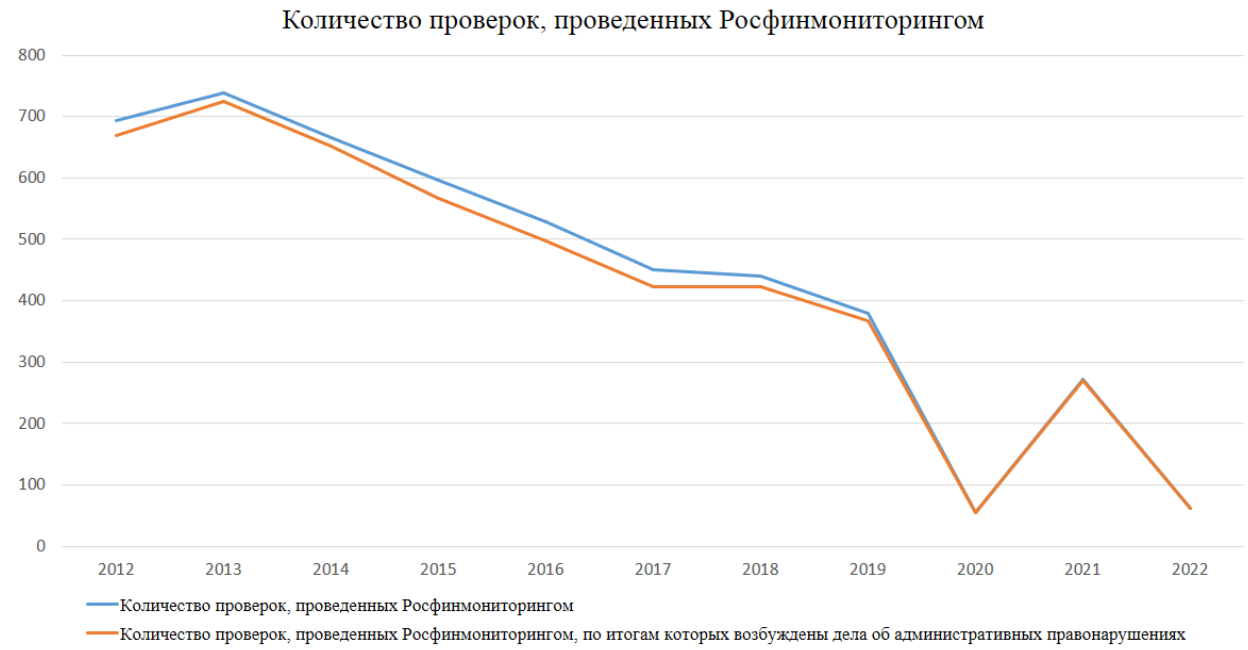
Соответственно, имеет место совпадение с предыдущими значениями коэффициентов корреляции, когда в случае с кредитными организациями корреляция наблюдается, а в случае с некредитными финансовыми организациями корреляция отсутствует.

Методика определения коэффициента корреляции и корреляционные поля представлены в приложении А.

Таким образом, можно отметить, что снижение числа проверок в отношении некредитных финансовых организациях не взаимосвязано с количеством мер государственного принуждения, применяемых Банком России в отношении НФО. В отношении кредитных организациях, такая корреляция хоть и наблюдается, однако, она меньше и неустойчивее по сравнению с корреляцией между числом проверок и такими показателями эффективности механизма мониторинга ПОД/ФТ, как объем выводимых за границу денежных средств и объем обналичивания денежных средств. Соответственно, нельзя сделать вывод, что снижение обналичивания денежных средств и вывода капитала за рубеж по подозрительным основаниям связано с ухудшением качества надзора, осуществляемого в дистанционном формате. Наоборот, дистанционный формат надзора вкупе с общим сокращением числа неблагонадежных участников сектора банковских услуг мог способствовать снижению объемов подозрительных финансовых потоков.

Развитие дистанционной и консультативной форм надзора осуществляет также Росфинмониторинг. Так, 85% проведенных ведомством в 2022 году проверок пришлось на камеральные проверки [134]. Статистика количества проверок, проведенных Росфинмониторингом, демонстрирует схожие тенденции к

снижению, что отражено на рисунке 33. Отмечаем, что в связи с тем, что статистика по количеству возбужденных Росфинмониторингом дел об административных правонарушениях в отчетах ведомства не представлена, сравнение статистики Росфинмониторинга со статистикой Банка России не представляется возможным.



Источник: составлен автором на основе статистики проверок Росфинмониторинга за период 2012-2022 годов [175].

Рисунок 33 – Количество проверок, проведенных Росфинмониторингом

Характерно, что доля проверок, проведенных Росфинмониторингом, в которых выявляются правонарушения, от общего числа проверок регулярно приближается к показателю 100%. При этом, рисунок демонстрирует то, что со снижением числа проверок, проводимых Росфинмониторингом, повысилась их точечность, о чем говорят практически идентичные графики общего количества проверок и количества проверок, по итогам которых были возбуждены дела по административным правонарушениям, начиная с 2019 года.

Основными причинами допущенных нарушений в 2022 году, согласно данным Росфинмониторинга, являлись:

– «невнесение (несвоевременное внесение) соответствующих изменений во внутренние документы контролируемых лиц, разрабатываемых в целях ПОД/ФТ, т.е. привело к несоответствию правил внутреннего контроля требованиям законодательства о ПОД/ФТ;

– невыполнение отдельных требований по идентификации клиентов (их представителей, выгодоприобретателей и бенефициарных владельцев) контролируемых лиц;

– несвоевременное проведение систематической проверки (не реже чем один раз в три месяца) клиентов на наличие принятия мер по замораживанию (блокированию) денежных средств или иного имущества» [134].

При этом, Росфинмониторинг значительное внимание уделяет профилактической работе в целях предупреждения нарушения законодательства о ПОД/ФТ. Особую роль в этом играет информационное взаимодействие с поднадзорными субъектами, осуществляемое через Личный кабинет. Так, по итогам 2022 года число поднадзорных лиц, использующих функционал Личного кабинета, увеличилось на 3,9 процентных пункта [134].

Таким образом, влияние цифровизации экономики на эффективность механизма мониторинга ПОД/ФТ неоднозначно. С одной стороны, инновационные технологии, неразрывно связанные с цифровой экономикой, создают дополнительные риски в сфере ПОД/ФТ, снижают эффективность применяемых мер и требуют введения новых. Так, открытым остается вопрос отслеживания и деанонимизации операций, совершаемых с использованием криптовалют, отмечаются риски использования технологий искусственного интеллекта для обхода действующих требований механизма мониторинга ПОД/ФТ. В то же самое время, технологии цифровой экономики открывают новые возможности в сфере ПОД/ФТ, как в части обмена информацией при осуществлении процедур НПК, так и в части отслеживания операций (как в традиционной финансовой системе, так и криптовалютных операций), а также применения новых форм надзора за соблюдением нормативно-правовых требований в сфере ПОД/ФТ. При этом, отдельные инновации, такие как цифровые валюты центральных банков, могут значительно поменять весь облик механизма мониторинга ПОД/ФТ за счет предоставления возможности отслеживания всей цепочки передачи конкретной цифровой монеты, а также за счет применения целевых мер, направленных на ограничение операций с ней в отношении отдельно взятых активов и лиц.

Характерно, что все основные технологии, сопровождающие цифровизацию, дуалистичны с точки зрения ПОД/ФТ. Развитие средств инфокоммуникаций, цифровой банкинг, блокчейн, искусственный интеллект не являются однозначно «плохими» или «хорошими» с точки зрения ПОД/ФТ, а создают возможности, как для усиления механизма мониторинга ПОД/ФТ, так для его обхода. Соответственно, можно сказать, что имеет место «гонка вооружений» между преступниками с одной стороны и правоохранительными органами и финансовыми разведками с другой в части получения наибольших преимуществ от внедрения указанных технологий. Это порождает необходимость доработки, а местами и значительной модернизации существующего механизма мониторинга ПОД/ФТ, разработки такой его модели, которая могла бы способствовать минимизации рисков цифровой экономики и эффективному использованию ее преимуществ.

3.2 Перспективы совершенствования национального механизма мониторинга противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма

В феврале 2022 года Центральный банк Российской Федерации объявил о начале процедуры тестирования платформы цифрового рубля [183]. Цифровой рубль представляет собой третью форму рубля после наличной и безналичной. Концепция цифрового рубля предполагает открытие цифрового кошелька на платформе Банка России. На данной же платформе будут осуществляться операции с цифровым рублем [182]. Осуществление операций с цифровым рублем для граждан предполагается без взимания комиссия, комиссия для операций юридических лиц по планам ЦБ РФ не должна превышать 0,3% [190]. Однако, концепция цифрового рубля не предполагает открытие накопительных счетов. Цифровой рубль обладает рядом преимуществ для граждан, делового сообщества и финансового рынка России, в целом. Так, цифровой рубль предоставляет возможность осуществления финансовых операций без подключения к сети Интернет. Также снизится финансовая нагрузка на пользователей цифрового рубля

за счет снижения комиссий, взимаемых при осуществлении денежных переводов. Внедрение цифрового рубля позволит более широко использовать смарт-контракты в коммерческой практике с задействованием фиатных валют в отличие от высоковолатильных криптовалют. Однако, в качестве одного из главных преимуществ цифровой валюты отмечается возможность государства контролировать операции, осуществляемые с использованием данного вида валюты, в целях противодействия незаконным финансовым потокам [260].

Возможность контроля за операциями с использованием цифрового рубля связана с тем, что сам цифровой рубль представляет собой определенный уникальный цифровой код, что позволяет по цифровому следу отслеживать путь каждого цифрового рубля [180]. Кроме того, в цифровой рубль предполагается внедрить возможность «окрашивания» тех или иных средств, выделяемых на специфические нужны (например, субсидий) [89]. Это позволит противодействовать схемам, связанным с нецелевым расходованием бюджетных средств. Также стоит отметить, что сама по себе возможность «окрашивания» цифрового рубля с запретом нецелевого использования выделенных на специфические цели денежных средств не станет непреодолимым препятствием на пути хищения бюджетных средств, так как останется возможным осуществление финансовых операций по подложным основаниям (например, как в случае со схемами обналичивания материнского капитала с фиктивной покупкой недвижимости и задействованием микрофинансовых организаций в качестве посредников для обналичивания материнского капитала [3]). Однако, цифровой рубль позволит отслеживать перемещение выделенных на целевые нужды денежных средств, что поспособствует облегчению процесса осуществления расследования преступлений, связанных с ОД/ФТ (по крайней мере, до момента их обналичивания).

Оператором платформы цифрового рубля является Банк России. В соответствии с этим, обязанность по соблюдению требований антиотмывочного законодательства в части операций с цифровым рублем также предполагается возложить на ЦБ РФ, так как только у него есть полная информация обо всех таких

операциях [93]. Однако, по прогнозам экспертов Банк России будет вынужден делегировать полномочия по идентификации клиентов кредитным организациям и другим субъектам Закона № 115-ФЗ, так как сам не обладает необходимыми компетенциями в данной сфере. В связи с ожидаемым включением Банка России в круг лиц, на которых законодательством возлагается обязанность по контролю за финансовыми операциями в целях выявления подозрительных операций и ОПОК, а также за соблюдением иных требований Закона № 115-ФЗ, можем отметить, что изменения коснутся и структуры механизма мониторинга ПОД/ФТ таким образом, что Банк России одновременно станет и органом, осуществляющим контроль (надзор) за соблюдением требований Закона № 115-ФЗ, и подотчетным субъектом. Также возложение на Банк России новых обязанностей потребует от него соответствующих вложений в персонал и информационную инфраструктуру в целях создания подразделений, осуществляющих мониторинг финансовых операций на предмет наличия признаков ОД/ФТ.

Еще одним актуальным направлением развития механизма мониторинга ПОД/ФТ является включение в сферу его охвата оборота криптовалют. Оборот ЦФА и цифровых валют в ограниченном виде законодательно был разрешен в Российской Федерации с принятием Федерального закона № 259-ФЗ от 31.07.2020 «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» [36]. В соответствии с данным законом список субъектов противодействия отмыванию преступных доходов был расширен за счет включения в него операторов информационных систем, в которых осуществляется выпуск ЦФА, и операторы обмена ЦФА. Соответственно, на данные субъекты стали распространяться требования антиотмывочного законодательства, в том числе по осуществлению надлежащей проверки клиентов и направлению ФЭС в Росфинмониторинг. Федеральным законом № 222-ФЗ от 8 августа 2024 года «О внесении изменений в отдельные законодательные акты Российской Федерации» в список субъектов антиотмывочного законодательства были включены лица, осуществляющие майнинг криптовалют, а также лица, организующие деятельность майнинг-пула

[26]. Однако, российским механизмом мониторинга ПОД/ФТ не охватываются операторы оборота цифровых валют. Кроме того, является актуальным вопрос о регулировании деятельности криптовалютных бирж, зарегистрированных за пределами Российской Федерации. В целях устранения данных пробелов осуществляется работа по установлению государственного регулирования рынка криптовалют в Российской Федерации, а также обсуждаются варианты введения обязанности для операторов обмена цифровых валют, оказывающих услуги для пользователей из Российской Федерации, регистрироваться на территории Российской Федерации [86; 151]. Актуальным является вопрос установления правового режима для NFT, так как невозможность на них распространить имеющиеся в российском законодательстве определения цифрового финансового актива, цифровой валюты и цифрового права выводит их за пределы сферы контроля государственных органов, что чревато использованием активов в целях ОД/ФТ. В контексте введения оборота NFT в сферу действия механизма мониторинга ПОД/ФТ целесообразно было бы расширить существующее определение ЦФА в части включения в него цифровых прав, удостоверяющих право на владение, пользование и распоряжение уникальным цифровым активом.

Также по мере развития практики использования smart-контрактов в деловом обороте (чему может поспособствовать введение в оборот цифровых валют) можно ожидать включения в национальный механизм мониторинга ПОД/ФТ мер, направленных на минимизацию рисков использования smart-контрактов в преступных целях. К таковым мерам можно отнести разрешение использования smart-контрактов при условии осуществления финансовых операций через кредитные организации или провайдеров услуг цифровых финансовых активов (или операторов обмена цифровых валют при условии установления в их отношении обязанности по соблюдению требований Закона № 115-ФЗ), предоставляющих данные в Росфинмониторинг, а также введение обязанности для разработчиков (пользователей) smart-контрактов предоставлять субъектам Закона № 115-ФЗ всю сопроводительную документацию, на основе которой программное обеспечение «умных контрактов» приняло решение о выполнении (или

невыполнении с последующим востребованием денежных средств с поручителей) сторонами своих обязательств (составлено на основе результатов, полученных совместно с Шевляковым Е.В. [271]).

В качестве перспективного направления развития национального механизма мониторинга ПОД/ФТ можно также отметить расширение использования биометрической информации, а также ЕСИА в целях удаленного осуществления процедур надлежащей проверки клиентов. Данный способ НПК будет приобретать большую популярность по мере роста объема банковских услуг, оказываемых в дистанционном формате. Кроме того, удаленные способы НПК имеют решающую роль при введении в правовое поле оборота ЦФА и цифровых валют. В связи с этим, можно ожидать, что решение вопросов борьбы с ОД/ФТ, совершаемых с использование цифровых финансовых активов и цифровых валют, тесно связано с предоставлением клиентам кредитных организаций, операторов оборота цифровых финансовых активов и криптовалютных бирж возможности осуществления удаленной процедуры идентификации и надлежащей проверки клиента, что может быть реализовано, как за счет создания единой межбанковской системы обмены информацией о клиентах кредитных организаций, прошедших процедуру идентификации, использования в целях идентификации биометрической информации и ЕСИА, так и за счет отработки процесса удаленного предоставления клиентом требуемой документации по сделке с принятием необходимых мер по недопущению предоставления фальсифицированных сканов документов или их электронных версий. Стоит отметить, что процедуры удаленной идентификации клиентов также могут найти свое применение в качестве средства борьбы с хищением денежных средств посредством компрометации электронных устройств клиентов кредитных организаций, однако, в таком случае удаленные способы идентификации должны быть разработаны таким образом, чтобы учесть возможность злоумышленников направлять со скомпрометированного устройства команды, подтверждающие исполнение финансовых операций, в том числе (с учетом развития технологии подделки голоса и лица человека deepfake) команды с

задействованием биометрических данных человека (например, подающиеся голосом или в формате видеоконференцсвязи).

Направления развития национального механизма ПОД/ФТ закреплены в Концепции развития национальной системы противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, утвержденной Президентом Российской Федерации 30 мая 2018 года (далее – Концепция развития системы ПОД/ФТ) и представлены на рисунке 34 [106].

При этом, в качестве одной из основных задач по совершенствованию деятельности национальной системы ПОД/ФТ приведено «расширение информационно-технологических возможностей Росфинмониторинга по сбору, своевременной обработке, анализу, хранению и передаче необходимой информации на международном, федеральном и региональном уровнях» [106]. В рамках реализации данной задачи особую роль приобретают технологии искусственного интеллекта и Big Data.

Основные направления развития национальной системы ПОД/ФТ
• формирование государственной политики и нормативно-правовой базы в области противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма; • совершенствование механизма участия в деятельности национальной системы организаций, осуществляющих операции с денежными средствами и иным имуществом, и специалистов, входящих в эту систему; • снижение уровня преступности, связанной с легализацией (отмыванием) доходов, полученных преступным путем, коррупцией, финансированием терроризма и распространения оружия массового уничтожения; • расширение участия Российской Федерации в международном сотрудничестве в сфере противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма на уровне международных организаций и иных профильных структур, а также на межгосударственном уровне; • совершенствование деятельности национальной системы.

Источник: составлено автором на основании материала [106].
Рисунок 34 - Основные направления развития национальной системы ПОД/ФТ

С учетом отмеченных тенденций к расширению роли технологий искусственного интеллекта в сфере ПОД/ФТ можно ожидать дальнейшего

развития программно-аппаратных комплексов на их основе, используемых в антиотмывочных целях. При этом, расширение использования данных комплексов можно ожидать как стороны финансовой разведки, так и со стороны поднадзорных субъектов 115-ФЗ (а также Банка России с учетом его новых полномочий по управлению рисками ОД/ФТ при обороте цифрового рубля). Развитие технологий искусственного интеллекта и Big Data, как в случае субъектов 115-ФЗ, так и в случае государственных органов будет осуществляться в целях расширения их аналитического функционала за счет оптимизации процесса анализа накапливающихся данных, объемы которых имеют тенденции к увеличению, а также алгоритмизации процесса анализа массивов данных, что позволит повысить эффективность средств отслеживания операций (в случае криптовалют) и улучшить качество процесса автоматизированного выявления признаков ОД/ФТ в операции или деятельности клиента (может иметь место, как в случае осуществления надлежащей проверки клиентов, так и в процессе последующего анализа их деятельности). В первую очередь, развитие технологий искусственного интеллекта в сфере ПОД/ФТ будет направлено по вектору отслеживания криптовалютных транзакций (в том числе, с использованием криптовалютных миксеров). Подтверждением этому является повышенный интерес государственных органов разных стран (в том числе и России) к разработке комплексов, позволяющих отслеживать криптовалютные транзакции. При этом, в большинстве таких комплексов до сих пор окончательно не решен вопрос об отслеживании операций, осуществляемых с использованием криптовалют, в которые встроены средства обфускации операций.

Искусственный интеллект может найти свое применение в качестве способа исследования финансовых операций на предмет наличия признаков отмывания доходов, полученных преступным путем, и финансирования терроризма в режиме реального времени. Актуальность анализа финансовых операций в текущем времени связана с вышеотмеченными тенденциями роста безналичных денежных переводов и алгоритмизацией торговли на рынке ценных бумаг. Также можно отметить, что введение в оборот цифровых валют также может привести к росту

скорости совершения финансовых операций. И связано это может быть не столько со скоростью операций в блокчейн (здесь скорее блокчейн может даже уступать традиционным платежным системам, так скорость транзакций, совершаемых с использованием криптовалюты Bitcoin, составляет около семи транзакций/секунду при среднем времени ожидания подтверждения транзакции, составляющем 55 минут, тогда как в платежной системе Visa скорость операций составляет около 24 000 транзакций/секунду при среднем времени ожидания в три секунды [8]), сколько с возможностью комбинированного использования цифровых валют и программных комплексов, позволяющим в автоматизированном режиме отслеживать выполнение сторонами своих обязательств и осуществлять финансовые операции в соответствии с договоренностями сторон (smart-контракты). При этом, по мнению Прошунина М.М, сроки предоставления сообщений об операциях и сделках в будущем будут пересматриваться в пользу их сокращения вплоть до конца рабочего дня даты совершения операции (сделки) [257]. В осуществлении анализа финансовых операций в режиме реального времени в той или иной степени потребуется задействование информационных систем финансового мониторинга. При этом с учетом объема и скорости осуществляемых операций такие системы должны быть в значительной степени интеллектуализированными, чтобы позволить в автоматизированном или полуавтоматизированном режиме выявлять признаки подозрительности в финансовых операциях и сообщать о них операторам информационных систем или сотрудникам органов государственного финансового контроля.

Более того, в научных источниках существует мнение о необходимости установления закрепленного в нормативно-правовых актах требования по внедрению технологий искусственного интеллекта в программные системы субъектов Закона № 115-ФЗ. Так, Прошунин М.М. считает, что в скором будущем может воплотиться в жизнь «самообучающееся программное обеспечение и цифровая аналитика как обязательное нормативное требование к системам, направленным на ПОД/ФТ» [257, с. 5]. Кроме того, Прошунин пишет, что «в конечном итоге может идти речь о создании единого информационно-

аналитического центра на базе Росфинмониторинга, анализирующего финансовые операции в режиме реального времени путем получения доступа к внутренним системам проведения платежей Банка России и кредитных организаций» [257, с. 5]. Также в научных источниках отмечается необходимость установления единообразного и общедоступного подхода к внедрению технологий цифровой экономики (в первую очередь, искусственного интеллекта) в деятельность субъектов Закона № 115-ФЗ [2]. При этом, в выработке такого подхода особая роль отводится Росфинмониторингу.

Таким образом, с учетом цифровизации экономики автором выделены следующие тенденции развития механизма мониторинга ПОД/ФТ Российской Федерации:

– введение цифрового рубля с целью контроля финансовых потоков, выделяемых на целевые нужды, с передачей обязанностей по осуществлению финансового мониторинга за операциями с цифровым рублем Банку России, что потребует от последнего создания соответствующих подразделений и информационной инфраструктуры, а также разработки правовых конструкций, определяющих взаимодействие Банка России и Росфинмониторинга в части исполнения обязанностей, установленных Законом № 115-ФЗ, в отношении операций с цифровым рублем;

– устранение правового пробела, связанного с отсутствием обязанности по соблюдению требований антиотмывочного законодательства у операторов оборота цифровых валют (в том числе, зарубежных криптовалютных бирж), а также неурегулированностью статуса NFT;

– установление дополнительных требований в отношении разработчиков и пользователей ряда технологических инноваций (в частности, smart-контрактов), позволяющих снизить риски использования инноваций в целях ОД/ФТ по мере роста популярности использования инноваций в деловой практике;

– расширение практики осуществления удаленной идентификации с использованием биометрической информации, а также данных, полученных из ЕСИА, клиентов кредитных организаций, операторов выпуска и обмена ЦФА и

операторов оборота цифровых валют. Кроме того, удаленная идентификация получит свое развитие за счет оптимизации процесса обмена данными в отношении клиентов, прошедших НПК, между кредитными организациями, операторами выпуска и обмена ЦФА и операторами оборота цифровых валют (в том числе, возможно развертывание единой системы обмена информацией между вышеуказанными субъектами);

– внедрение в деятельность профильных подразделений субъектов Закона № 115-ФЗ, а также органов финансового контроля технологий искусственного интеллекта и Big Data, позволяющих оптимизировать процесс взаимодействия с растущими объемами информации, накапливающимися в базах данных субъектов и органов, а также в иных источниках (в том числе, в сети Интернет) [2]. При этом, первостепенное внимание будет уделяться развитию программных комплексов (в первую очередь, системы «Прозрачный блокчейн»), позволяющих отслеживать криптовалютные операции и деанонимизировать участников данных операций, в части включения в функционал таких программных комплексов возможности отслеживания операций, совершаемых с использованием криптовалют, в которые встроены средства повышения конфиденциальности транзакций (таких как Dash и Monero). Также развитие технологий искусственного интеллекта может подтолкнуть Росфинмониторинг к внедрению в нормативном (или добровольно-нормативном) порядке юнитов искусственного интеллекта в информационные системы субъектов Закона № 115-ФЗ с целью повышения скорости предоставления ФЭС в подразделение финансовой разведки, а также повышения качестве первичного финансового мониторинга.

3.3 Разработка рекомендаций по совершенствованию механизма мониторинга противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма в условиях цифровизации экономики

Формирование новых и актуализация старых рисков отмывания преступных доходов и финансирования терроризма в результате цифровизации экономики требует соответствующей реакции со стороны, как государственных органов, так и субъектов Закона № 115-ФЗ, являющихся агентами финансового мониторинга. Также необходимо внедрение технологий цифровой экономики в деятельность механизма мониторинга ПОД/ФТ в той части, в которой они могут способствовать повышению эффективности его деятельности, с сопутствующим учетом и минимизацией рисков, возникающих в связи с внедрением данных технологий в механизм мониторинга ПОД/ФТ [53].

Увеличение скорости совершения финансовых операций и расширение масштабов алгоритмической торговли, как уже было отмечено выше, повышают нагрузку на подразделения и должностные лица, отвечающие за соблюдение требований Закона № 115-ФЗ, а также предъявляют повышенные требования к оперативности передачи информации в подразделение финансовой разведки. Применение программно-аппаратных комплексов в целях выявления операций и лиц, связанных с ОД/ФТ, несмотря на возможность ускорения процедур выявления подозрительных операций и ОПОК в информационных системах Закона № 115-ФЗ, а также формирования ФЭС, имеют ряд ограничений, в числе которых:

– необходимость наличия ресурсов (в том числе финансовых и людских) на внедрение данных комплексов в информационную систему организации (так, по оценкам экспертов консалтинговой компании Forrester с увеличением количества нормативных требований затраты на обслуживание решений в сфере ПОД/ФТ возрастут на 15–25% [238]);

– низкая эффективность прямолинейных программно-аппаратных комплексов, в деятельности которых наблюдается значительное количество ошибок первого и второго рода [2];

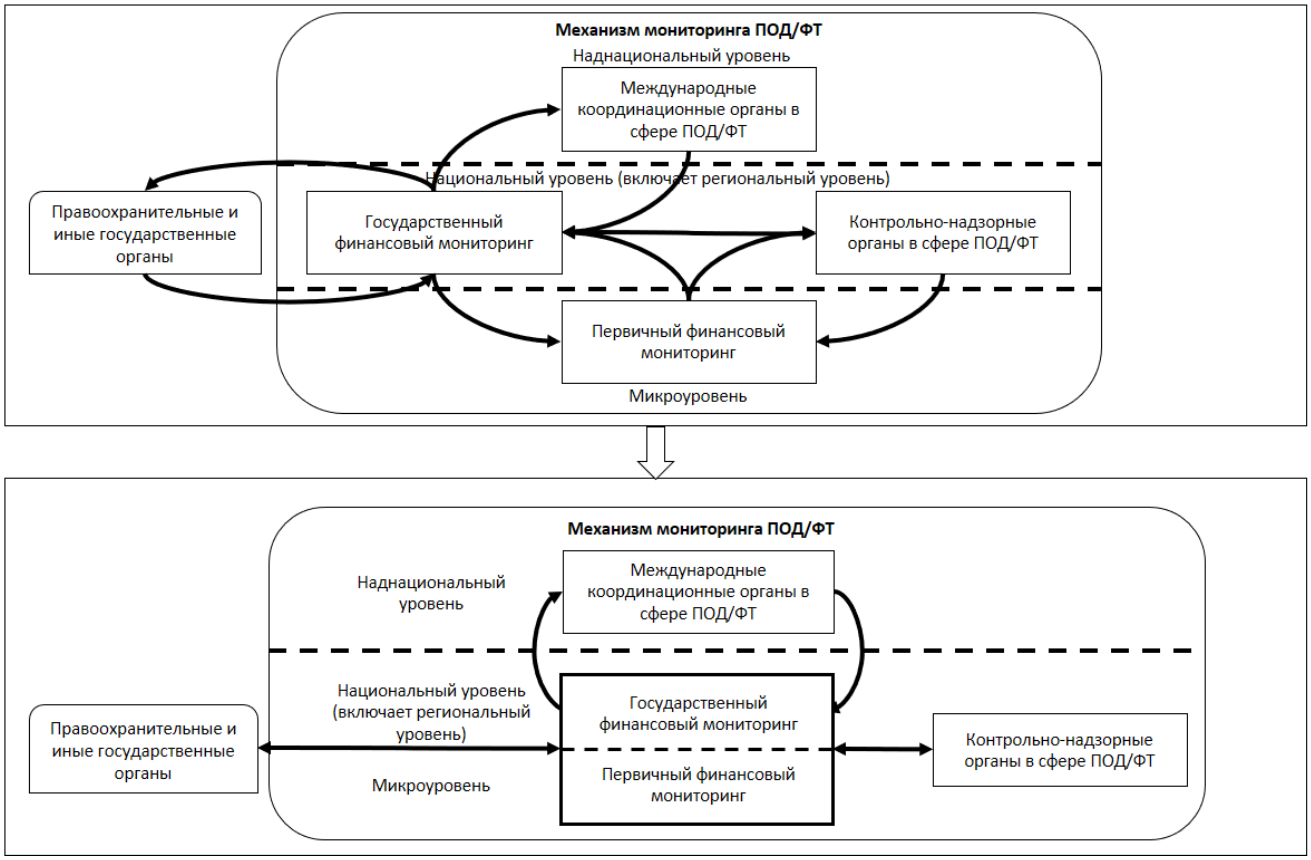
– слабая развитость рынка отечественного программного обеспечения в области автоматизации финансового мониторинга с использованием алгоритмов машинного обучения, в то время как преобладание иностранного ПО на данным рынком создает угрозы для российского механизма мониторинга ПОД/ФТ, как санкционного характера, так и сфере информационной безопасности и сохранности банковской тайны.

Кроме того, данные комплексы, несмотря на автоматизацию процесса формирования ФЭС, неспособны значительно ускорить процесс передачи информации от субъектов Закона № 115-ФЗ в Росфинмониторинг. Для преодоления недостатков механизма мониторинга ПОД/ФТ, перечисленных во второй главе исследования, реагирования на риски, связанные с цифровизацией экономики, необходимо комплексная модификация механизма мониторинга ПОД/ФТ, предполагающая изменение модели его функционирования.

Действующая в настоящий момент модель функционирования механизма мониторинга ПОД/ФТ предполагает выявление субъектами Закона № 115-ФЗ ОПОК и подозрительных операций, а также направление ФЭС о них (а также в иных случаях, предусмотренных Законом № 115-ФЗ) в адрес Росфинмониторинга. После осуществления анализа получаемой информации Росфинмониторинг принимает решение о направлении или ненаправлении информации в правоохранительные и иные государственные органы.

В целях сокращения временного лага, связанного с передачей информации от субъектов Закона № 115-ФЗ (в первую очередь, от кредитных организаций и некредитных финансовых организаций) целесообразно рассмотреть вопрос о модернизации механизма мониторинга противодействия отмыванию доходов, полученных преступным путем, и финансированию терроризма в сторону слияния микроуровня и национального уровня механизма мониторинга ПОД/ФТ. При разработке рекомендаций по совершенствованию механизма мониторинга

ПОД/ФТ в представленном в исследовании подходе не будет учитываться наднациональный уровень механизма мониторинга ПОД/ФТ в связи с тем, что, как было отмечено ранее, принимаемые на данном уровне меры носят преимущественно рекомендательный характер и основаны на анализе передовых практик, сформированных в рамках национальных систем ПОД/ФТ. Схематично данный процесс изложен на рисунке 35.



Источник: составлено автором.

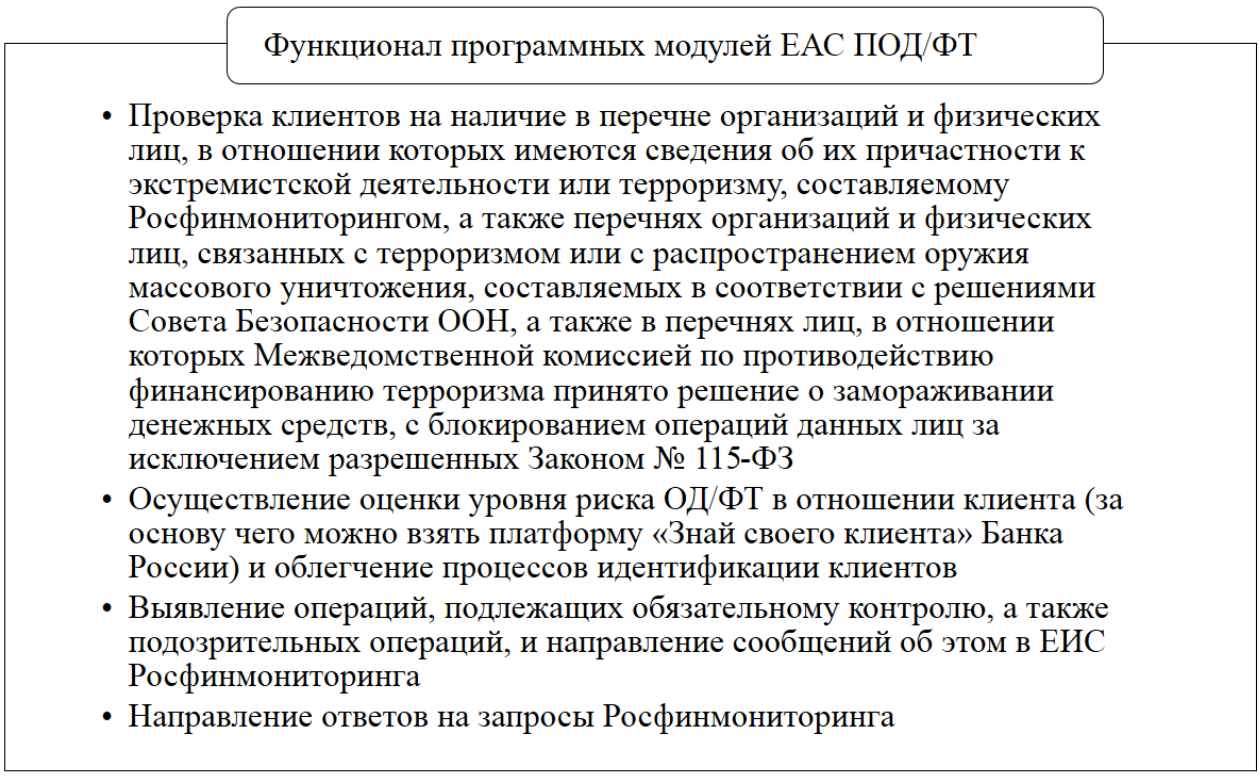
Рисунок 35 - Модернизация механизма мониторинга ПОД/ФТ путем слияния первичного и вторичного финансового мониторинга

Реализация данного подхода возможна за счет внедрения в информационные системы субъектов Закона № 115-ФЗ программных модулей единой программно-аппаратной системы финансового мониторинга, разработка которой возможна по аналогии с системой «Прозрачный блокчейн» в рамках государственно-частного партнерства Росфинмониторинга и крупнейших кредитных организаций Российской Федерации, имеющих значительный опыт разработки, внедрения и применения программно-аппаратных систем выявления противозаконных операций.

Такая система должна представлять собой программно-аппаратный комплекс, предназначенный для автоматизации процесса проведения процедур НПК, выявления подозрительных операций и ОПОК, формирования и направления ФЭС и ответов на запросы Росфинмониторинга в едином стандартизированном виде, а также автоматизированного замораживания денежных средств.

Такой комплекс должен состоять из централизованной системы финансового мониторинга, размещенной в ЕИС в сфере ПОД/ФТ, а также программных модулей, встраиваемых в информационные системы субъектов Закона № 115-ФЗ (далее вышеуказанный программно-аппаратный комплекс будет именоваться Единой автоматизированной системой противодействия отмыванию доходов, полученных преступным путем, и финансированию терроризма, ЕАС ПОД/ФТ). Структура ЕАС ПОД/ФТ представлена в приложении Б.

Программные модули должны представлять собой встраиваемые в информационные системы субъектов Закона № 115-ФЗ программные компоненты, функционал которых описан на рисунке 36.



Источник: составлено автором.
Рисунок 36 - Функционал программных модулей ЕАС ПОД/ФТ

При этом, целесообразно, чтобы функция приостановка операции или деловых отношений с клиентом была предусмотрена данным ПО, но подтверждение на нее необходимо получать от должностных лиц субъектов Закона № 115-ФЗ, в информационную систему которых внедряется программный модуль, так как именно данные субъекты несут гражданско-правовую ответственность за неправомерное ограничение прав своих клиентов (за исключением, согласно представленному в данном исследовании подходу, случаев приостановления операций в отношении лиц, включенных в вышеуказанные перечни Росфинмониторинга и Совета Безопасности ООН, в случае принятия соответствующего решения МВК по ФТ, а также в случае если приостановление операций применяется в отношении юридического лица, которое находится в собственности или под контролем лица, в отношении которых применены меры по замораживанию денежных средств или иного имущества). Информация о принятии мер по замораживанию операций может в автоматизированном режиме направляться в Росфинмониторинг. Информация о принятии решения о расторжении договора, а также о принятии решения в отказе от заключения договора должна вноситься в систему в ручном или автоматизированном режиме.

Автоматизация процесса осуществления процедур НПК посредством встраиваемого модуля Росфинмониторинга имеет по нашему мнению несколько преимуществ, отмеченных на рисунках 37; 38.

Автоматизация процесса выявления подозрительных операций и ОПОК и формирования ФЭС позволит устранить субъективизм персонала субъектов Закона № 115-ФЗ, который рядом авторов отмечается, как одна из ключевых проблем банковского сектора в части осуществления первичного финансового мониторинга [238]. Кроме того, влияние субъективизма тем больше возрастает, чем более дорогими являются автоматизированные комплексы ПОД/ФТ, так как на их внедрение и обслуживание у небольших кредитных организаций не хватает денежных средств. Внедрение в информационные системы субъектов Закона № 115-ФЗ программных модулей ЕАС ПОД/ФТ позволит устранить эту проблему.

Преимущества автоматизации процесса осуществления процедур НПК посредством встраиваемого модуля Росфинмониторинга
• Устраняется временной промежуток между размещением информации на сайте Росфинмониторинга о включении того или иного лица в вышеуказанные перечни и поступлением данной информации сотрудникам субъектов Закона № 115-ФЗ. В случае внедрения в информационную систему субъекта Закона № 115-ФЗ программного модуля ЕАС ПОД/ФТ учет изменений в перечнях возможен практически сразу после принятия соответствующего решения, так как загрузка информации в ЕАС ПОД/ФТ может происходить параллельно с публикацией информации на сайте Росфинмониторинга • Возможность осуществления идентификации личности клиента удаленно в случае прохождения процедуры клиентом в ином субъекте Закона № 115-ФЗ, подключенного к ЕАС ПОД/ФТ. В случае прохождения клиентов процедуры идентификации в одном из субъектов Закона № 115-ФЗ, подключенных к ЕАС ПОД/ФТ, информация о нем попадает в единую базу данных ЕАС ПОД/ФТ, после чего клиент будет иметь возможность не проходить процедуру идентификации при установлении деловых отношений с иными субъектами Закона № 115-ФЗ, подключенными к ЕАС ПОД/ФТ, при условии осуществлении данным клиентом действий, подтверждающих его личность (применяя тот или иной вид аутентификации). При этом, для исключения перегрузки базы данных ЕИС Росфинмониторинга данными клиентов субъектов Закона № 115-ФЗ, полную информацию о клиентах, предоставленную при осуществлении идентификации, целесообразно хранить непосредственно в информационных системах субъектов Закона № 115-ФЗ, в которых клиенты проходили процедуру идентификации, используя технологии построения распределенной базы данных. Хранение и изменение информации может осуществляться с использованием технологии Блокчейн путем генерации нового блока в случае изменения данных клиентов (что требует обеспечения процесса перманентной актуализации данных клиентов при их изменении по заявлению клиента, при выявлении изменений идентификационных данных клиентов сотрудниками субъектов Закона № 115-ФЗ или при поступлении информации от государственных органов)

Источник: составлено автором.

Рисунок 37 - Преимущества автоматизации процесса осуществления процедур НПК посредством встраиваемого модуля Росфинмониторинга (начало)

Преимущества автоматизации процесса осуществления процедур НПК посредством встраиваемого модуля Росфинмониторинга
• Возможность первоначального ранжирования клиентов субъекта Закона № 115-ФЗ в соответствии с уровнем риска ОД/ФТ на основе средневзвешенной оценки клиента со стороны других субъектов Закона № 115-ФЗ, а также данных платформы «Знай своего клиента» (в отношении юридических лиц и индивидуальных предпринимателей), а также возможность автоматизированной оценки клиента/изменения оценки клиента в соответствии с совершаемыми данным клиентом финансовыми операциями, наличием в деятельности клиента признаков, которых могут указывать на его преступный характер или фиктивность • Возможность использования в рамках процедур НПК информации, полученной от государственных органов (в том числе от налоговых при осуществлении НПК в отношении юридических лиц и ИП), запросы в которые могут направляться с использованием ЕАС ПОД/ФТ через Росфинмониторинг или напрямую (в дальнейшем в работе будет использоваться первый вариант в силу наличия необходимой нормативно-правовой базы в виде межведомственных соглашений о взаимодействии (например, Соглашение о сотрудничестве и организации информационного взаимодействия Федеральной службы по финансовому мониторингу и Федеральной налоговой службы от 15.10.2015 года № 01-01-14/22440/ММВ-23-2/77@) которые, однако, тоже потребуется корректировать в части фиксации информации, которая может быть передана субъектам Закона № 115-ФЗ)

Источник: составлено автором.

Рисунок 38 - Преимущества автоматизации процесса осуществления процедур НПК посредством встраиваемого модуля Росфинмониторинга (окончание)

Программный модуль ЕАС ПОД/ФТ позволит также автоматизировать процесс направления запросов в субъекты Закона № 115-ФЗ и получения ответов от них, что исключит (или минимизирует) участие в направлении ответов на

данные запросы персонала субъектов Закона № 115-ФЗ, позволит сократить риск утечки информации о проявлении интереса подразделением финансовой разведки в отношении того или иного клиента, а также устранить документооборот, опосредующий направление запросов в отношении субъектов Закона № 115-ФЗ. Кроме того, это позволит стандартизировать формат ответов на запросы, направляемые в Росфинмониторинг, исключив различия между сообщениями, предоставляемыми разными кредитными организациями и иными субъектами Закона № 115-ФЗ. При этом, единый формат таких сообщений будет формироваться аналитиками Росфинмониторинга, что позволит разработать наиболее приемлемую и удобную для них форму получения информации.

Внедрение ЕАС ПОД/ФТ значительно отразится и на осуществлении процесса контроля и надзора за соблюдением нормативно-правовых требований в области ПОД/ФТ. Контроль и надзор в отношении субъектов Закона № 115-ФЗ, внедривших в свои информационные системы программные модули ЕАС ПОД/ФТ, будет схож с осуществлением налогового мониторинга.

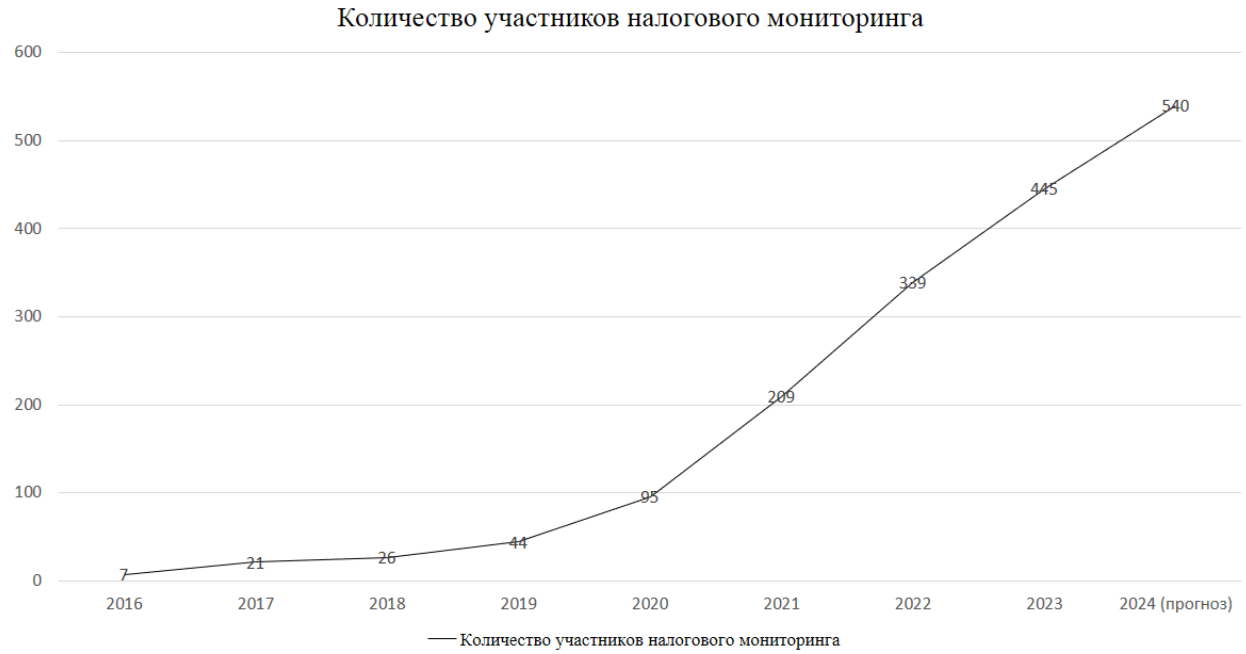
Налоговый мониторинг – это форма налогового контроля, введенная в Налоговой кодекс Российской Федерации в 2016 году в качестве раздела V.2 [30]. Налоговый мониторинг предполагает осуществление налогового контроля за счет получения удаленного доступа к информационной системе налогоплательщика, а также его бухгалтерской и налоговой отчетности. Данная форма налогового контроля позволяет снизить объем истребуемых у налогоплательщика документов и снизить административную нагрузку на бизнес. Кроме того, основной задачей налогового мониторинга является превенция налоговых правонарушений, а не наказание за них, что нашло свое отражение в создании правового института мотивированного мнения, предоставляемого по запросу налогоплательщика или по инициативе налогового органа, содержащего позицию налогового органа по вопросам правильности исчисления и уплаты налогов, сборов и страховых взносов. При этом, во время проведения налогового мониторинга камеральные налоговые проверки не проводятся, выездные налоговые проверки проводятся в случае

невыполнения мотивированного мнения налогового органа, а также в случаях, указанных в п. 5.1 ст. 89 Налогового кодекса Российской Федерации.

Несмотря на наличие определенных требований для налогоплательщиков, желающих перейти на налоговый мониторинг, в части минимальной суммы уплаченных налогов, объема полученных доходов и совокупной стоимости активов (указаны в пункте 3 статьи 105.26 Налогового кодекса Российской Федерации) количество организаций, присоединившихся к налоговому мониторингу растет. Так, в 2023 году налоговый мониторинг проводится в отношении 445 компаний, обеспечивающих в совокупности 41% налоговых поступлений в федеральный бюджет (при этом, в 2022 году таких компаний насчитывалось 339, в 2021 году – 209, в 2020 году – 95, 2019 году – 44, 2018 году – 26, 2017 году – 21, 2016 году – 7) [60; 125; 152; 202]. Налоговые органы ожидают дальнейшего увеличения участников налогового мониторинга, по их оценкам в 2024 году к налоговому мониторингу планируют присоединиться еще 95 компаний [55]. График роста числа участников налогового мониторинга приведен на рисунке 39.

Связана данная тенденция, в том числе, со снижением административной нагрузки на налогоплательщиков после их перехода на налоговый мониторинг. Так, в 2018 году на налоговый мониторинг перешла компания ПАО «Аэрофлот», что по итогам первого полугодия 2018 года позволило ей сократить расходы на налоговое администрирование на 7% [202]. По состоянию на январь 2023 года по данным ФНС России за весь период проведения налогового мониторинга ФНС России составила 189 мотивированных мнений на сумму 282,7 млрд рублей, при этом, не было зафиксировано ни одного случая выездной налоговой проверки по результатам неисполнения мотивированного мнения налогового органа [55].

Несомненно, налоговый мониторинг позволяет сократить не только издержки хозяйствующих субъектов, связанных с осуществление налогового контроля, но и расходы ФНС России на осуществление камеральных и выездных налоговых проверок. Внедрение ЕАС ПОД/ФТ может иметь схожий эффект в части финансового мониторинга.



Источник: составлено автором на основании материалов [60; 125; 152; 202].
Рисунок 39 – График роста количества участников налогового мониторинга

Как отмечено ранее, в надзорной деятельности Банка России и Росфинмониторинга наблюдаются тенденции к уменьшению количества контактных проверок и осуществлению надзора в отношении большей части поднадзорных субъектов в дистанционной форме. Однако, несмотря на то, что дистанционный надзор снижает издержки поднадзорных субъектов, связанных с проведением в отношении них проверок, а также снижает административную нагрузку, он создает издержки в части ответов на запросы контрольных органов, включающих в себя всю направляемую в Росфинмониторинг информацию, что предполагает дублирование действий с точки зрения поднадзорного субъекта.

Внедрение ЕАС ПОД/ФТ позволит, помимо прочего, исключить такое дублирование, в случае включения в функционал ЕАС ПОД/ФТ единого информационного пространства контрольно-надзорных органов в сфере ПОД/ФТ, в котором они смогут в режиме реального времени контролировать направляемые их поднадзорными субъектами ФЭС в адрес Росфинмониторинга. Таким образом, поднадзорные субъекты будут избавлены от необходимости дублирования направляемых сообщений. Аналогично возможно организовать взаимодействие в части предоставления документов, характеризующих организацию внутреннего

контроля в субъекте на предмет соблюдения требований ПОД/ФТ. При выявлении нарушений в процессе анализа документаций и ФЭС, содержащихся в ЕАС ПОД/ФТ, органы, осуществляющие контрольно-надзорную деятельность, могут также привлечь к ответственности виновных субъектов и их должностных лиц, а также принять решение о проведении выездной проверки.

Однако, с учетом автоматизации процесса финансового мониторинга за счет внедрения в информационные системы субъектов Закона № 115-ФЗ программных модулей ЕАС ПОД/ФТ необходимость проведения проверок очевидно сократится, как это имело место в случае с налоговым мониторингом. Основаниями для этого являются следующие моменты:

– государственные органы в сфере ПОД/ФТ получат непосредственный доступ к информационной системе субъектов Закона № 115-ФЗ, а также будут иметь возможность в режиме реального времени изучать направляемые субъектами сообщения;

– контроль за наличием признаков ОД/ФТ в операциях будет осуществлять программный модуль с использованием технологий искусственного интеллекта, он же будет выявлять ОПОК, а также с помощью него будет осуществляться идентификация клиентов;

– сократится число требований к субъектам Закона № 115-ФЗ, внедривших программные модули ЕАС ПОД/ФТ, так как часть их обязанностей будет выполняться ЕАС ПОД/ФТ в автоматизированном режиме.

В части последнего пункта стоит отметить, что ЕАС ПОД/ФТ не сможет полностью заменить персонал организаций, осуществляющий контроль за соблюдением требований Закона № 115-ФЗ, так как такие действия, как осуществление идентификации клиента, его представителя, бенефициарного владельца и выгодоприобретателя, приостановление подозрительных операций, а также выявление признаков ОД/ФТ в финансовых операциях все равно потребуют действий персонала субъектов Закона № 115-ФЗ. Это означает, что останутся актуальными требования о разработке правил внутреннего контроля и назначения

должностных лиц, ответственных за соблюдение требований антиотмывочного законодательства.

Кроме того, внедрение ЕАС ПОД/ФТ не должно привести к массовому увольнению людей, отвечающих за соблюдение требований Закона № 115-ФЗ и подзаконных актов в сфере ПОД/ФТ. Применение программных модулей ЕАС ПОД/ФТ в крупных кредитных организациях заменит использующиеся ими программные комплексы ПОД/ФТ, что, соответственно, не потребует проведения крупных сокращений персонала. Тогда как внедрение ЕАС ПОД/ФТ в информационные системы кредитных организаций и НФО среднего и малого масштаба также не должно иметь значительные негативные последствия для рынка труда в силу незначительного числа специалистов (средняя численность сотрудников подразделения внутреннего контроля (аудита), включающего в том числе специалистов по ПОД/ФТ, в российских банках согласно исследованию, проведенному в 2008 году Институтом внутренних аудиторов (Institute of Internal Auditors) совместно с консалтинговой компанией PricewaterhouseCoopers, составляет 0,86% от общей штатной численности сотрудников банков [261]), занятых в данной сфере, но может повысить качество предоставляемых ими ФЭС.

Однако, в силу того, что ЕАС ПОД/ФТ автоматизирует часть процедур, совершаемых субъектами Закона № 115-ФЗ и снимет с них ответственность за направление ФЭС об ОПОК, замораживании средств, а также частично за направление СПО (что не должно исключать направление СПО субъектом 115-ФЗ в ручном режиме, в случае выявления его сотрудниками признаков ОД/ФТ в операциях), снизится вероятность получения штрафов за неисполнение требований антиотмывочного законодательства, а имеющиеся ресурсы субъектов Закона № 115-ФЗ, выделенные на обеспечение требований антиотмывочного законодательства, будут перенаправлены на внедрение и обслуживание программных модулей ЕАС ПОД/ФТ, а также на обеспечение соблюдения оставшегося сокращенного списка обязательств по ПОД/ФТ.

Размер штрафа, предусмотренного ст. 15.27 КоАП РФ в отношении должностных лиц организаций находится в пределах от десяти тысяч рублей до

пятидесяти тысяч рублей, в отношении юридических лиц и индивидуальных предпринимателей штраф может составлять от пятидесяти тысяч до одного миллиона рублей в зависимости от состава и тяжести правонарушения. В число санкций ст. 15.27 КоАП РФ входят также дисквалификация должностного лица на срок от одного до трех лет и административное приостановление деятельности юридического лица и ИП на срок до девяноста суток.

Также штрафы кредитным организациям могут быть назначены в соответствии со ст. 74 Федерального закона № 86-ФЗ от 10 июля 2002 года «О Центральном банке Российской Федерации (Банке России)». Так, в ч. 2 данной статьи отмечается, что в случае неисполнения кредитной организацией требований Закона № 115-ФЗ, а также подзаконных нормативных актов, принятых Банком России, Центральный банк Российской Федерации «имеет право взыскивать с кредитной организации штраф в размере до 0,1 процента размера собственных средств (капитала) кредитной организации, но не менее 100 тысяч рублей» [35]. В ч. 4 указанной статьи содержится правовая норма, согласно которой неисполнение кредитной организации предписаний Банка России об устранение нарушений требований Закона № 115-ФЗ, а также подзаконных нормативных актов, принятых Банком России, или в случае, если такие нарушения создали реальную угрозу интересам кредиторов (вкладчиков) кредитной организации Банк России вправе назначить штраф «в размере до 1 процента размера собственных средств (капитала) кредитной организации, но не менее 1 миллиона рублей» [35].

В связи с этим представляет интерес статистика, приведенная в годовых отчетах Банка России в 2015-2022 гг. в части вынесенных штрафов в отношении кредитных организаций и их должностных лиц, а также НФО и их должностных лиц, представленная на рисунках 40; 41.

При этом, согласно данным Судебного Департамента при Верховном Суде Российской Федерации, средняя сумма штрафа по статье 15.27 КоАП РФ в 2022 году составила 165 тыс. рублей, в 2021 году – 100 тыс. рублей, в 2020 году – 85 тыс. рублей, в 2019 году – 116 тыс. рублей, в 2018 году – 102 тыс. рублей, в 2017 году – 89 тыс. рублей,

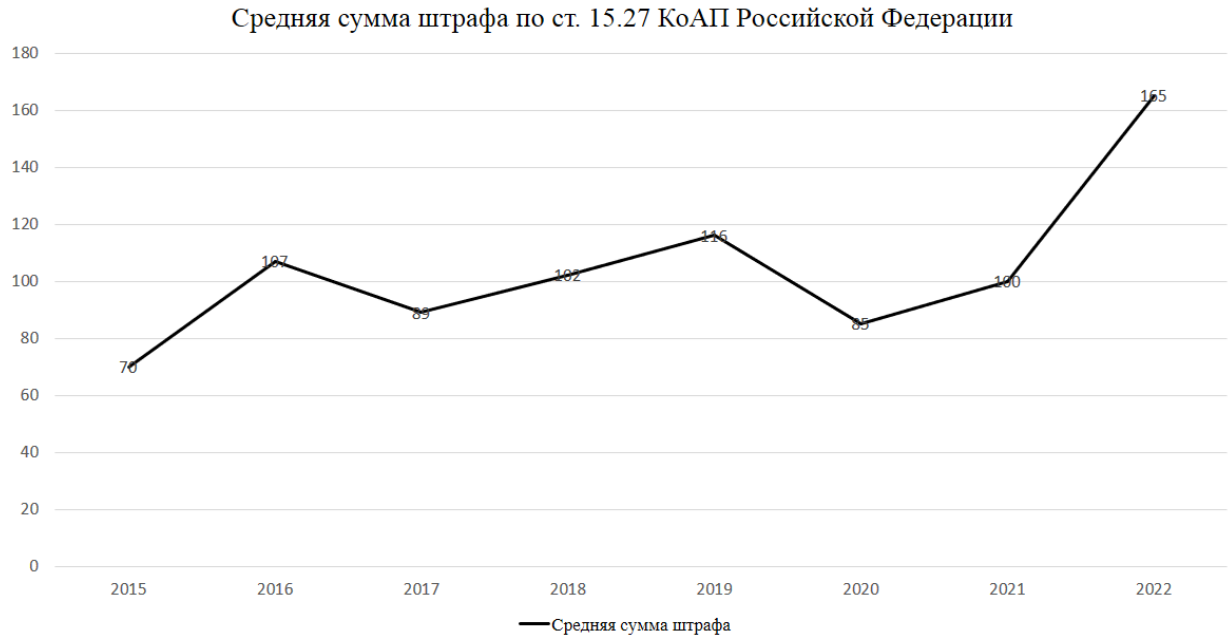
в 2016 году – 107 тыс. рублей, в 2015 году – 70 тыс. рублей [177]. Статистика по штрафам представлена на рисунке 42. Таким образом, среднегодовая сумма штрафа за период 2015-2022 гг. составляет 104 тыс. рублей.

Источник: составлено автором на основе годовых отчетов Банка России за период 2015-2022 годов [77; 78; 79; 80; 81; 82; 83; 84].

Рисунок 40 – Количество штрафов, вынесенных Банком России в соответствии со ст. 15.27 КоАП РФ

Источник: составлено автором на основе годовых отчетов Банка России за период 2017-2022 годов [79; 80; 81; 82; 83; 84].

Рисунок 41 – Количество кредитных организаций, в отношении которых Банком России были применены штрафы в соответствии со ст. 74 Федерального закона № 86-ФЗ от 10 июля 2002 года «О Центральном банке Российской Федерации (Банке России)»



Источник: составлено автором на основании материала [177].
Рисунок 42 – Средняя сумма штрафа по ст. 15.27 КоАП РФ

Внедрение ЕАС ПОД/ФТ, как отмечалось выше, снимет такие обязательства с субъектов Закона № 115-ФЗ, как направление информации об ОПОК, блокирование денежных средств, а также направление информации в Росфинмониторинг по его запросам.

В связи с чем станет неактуальным привлечение к ответственности за правонарушения, предусмотренные:

– частично ч. 2 ст. 15.27 КоАП РФ (неисполнение законодательства в части организации и осуществления внутреннего контроля, повлекшее «непредставление в уполномоченный орган сведений об операциях, подлежащих обязательному контролю, и (или) представление в уполномоченный орган недостоверных сведений об операциях, подлежащих обязательному контролю, а равно непредставление сведений об операциях, в отношении которых у сотрудников организации, осуществляющей операции с денежными средствами или иным имуществом, возникают подозрения, что они осуществляются в целях легализации (отмывания) доходов, полученных преступным путем, или финансирования терроризма» [24]);

– ч. 2.1 ст. 15.27 КоАП РФ («неисполнение законодательства в части блокирования (замораживания) денежных средств или иного имущества либо приостановления операции с денежными средствами или иным имуществом» [24]);

– частично ч. 2.2 ст. 15.27 КоАП РФ («непредставление в уполномоченный орган сведений о случаях отказа по основаниям, указанным в Федеральном законе от 7 августа 2001 года N 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», от заключения (исполнения) договоров банковского счета (вклада) с клиентами и (или) от проведения операций» [24]), так как представление информации в Росфинмониторинг о случаях отказа от заключения договора не всегда возможно автоматизировать;

– частью 2.3 ст. 15.27 КоАП РФ («непредставление в уполномоченный орган по его запросу имеющейся у организации, осуществляющей операции с денежными средствами или иным имуществом, информации об операциях клиентов и о бенефициарных владельцах клиентов, сведений о выгодоприобретателях, ставших ей известными при заключении договора страхования в пользу третьего лица (без проверки их достоверности), либо информации о движении средств по счетам (вкладам) своих клиентов» [24]);

– частично ч. 4 ст. 15.27 КоАП РФ («неисполнение организацией, осуществляющей операции с денежными средствами или иным имуществом, или ее должностным лицом законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, повлекшее установленные вступившим в законную силу приговором суда легализацию (отмывание) доходов, полученных преступным путем, или финансирование терроризма, если эти действия (бездействие) не содержат уголовно наказуемого деяния» [24]).

Таким образом, поднадзорные субъекты снимут риск привлечения к ответственности по двум составам и снизят риск привлечения к административной ответственности по трем составам из восьми составов правонарушений, предусмотренных ст. 15.27 КоАП РФ. Следовательно, по самым грубым подсчетам

(в связи с отсутствием статистики о привлечении к ответственности по тем или иным частям статьи 15.27 КоАП РФ), из среднегодовой суммы штрафа по статье 15.27 КоАП РФ за период 2015-2022 гг. следует вычесть две восьмых части и половину трех восьмых частей (так как ответственность по части 2 статьи 15.27 КоАП РФ снимется только в отношении ОПОК, тогда как отслеживание подозрительных операций останется в обязательствах субъектов Закона № 115-ФЗ, ответственность по ч. 2.2 ст. 15.27 КоАП РФ снимется в отношении отказов от проведения операций), из чего следует, что из среднегодовой суммы штрафа по статье 15.27 КоАП РФ за период 2015-2022 гг. следует вычесть 7/16 частей. Соответственно, среднегодовая сумма штрафа после внедрения ЕАС ПОД/ФТ может составить 58,5 тыс. рублей.

Формула для расчета среднегодовой суммы штрафа по статье 15.27 КоАП РФ после внедрения ЕАС ПОД/ФТ приведена в приложении В.

При этом, данные расчеты не учитывают, что в случае уменьшения числа требований в части выполнения норм Закона № 115-ФЗ, субъекты могут перераспределить имеющиеся ресурсы на соблюдение оставшихся требований, в связи с чем также снизится количество и суммы штрафов по остальным составам ст. 15.27 КоАП РФ.

Также по аналогии с налоговым мониторингом расходы субъектов Закона № 115-ФЗ на выполнение требований антиотмывочного законодательства могут сократиться на семь и более процентов, в связи с тем, что налоговый мониторинг лишь сократил траты организаций, связанные с проведением камеральных и выездных проверок, тогда как расходы субъектов Закона № 115-ФЗ, внедривших в свою деятельность ЕАС ПОД/ФТ, сократятся также за счет снижения количества предоставляемой отчетности и ФЭС.

Текущие расходы субъектов Закона № 115-ФЗ, связанные с функционированием механизма мониторинга ПОД/ФТ, можно представить в виде формулы, приведенной в приложении Г.

При этом, в отношении отдельных видов субъектов Закона № 115-ФЗ уравнение будет изменяться за счет удаления из него элементов, в

отношении которых у них отсутствуют обязательства. Так, у адвокатов, нотариусов, доверительных собственников (управляющих) иностранных структур без образования юридического лица, исполнительных органов личных фондов, имеющих статус международного фонда, лиц, осуществляющих предпринимательскую деятельность в сфере оказания юридических или бухгалтерских услуг, аудиторов и аудиторских организаций отсутствуют обязанности по предоставлению ФЭС об ОПОК, а также по предоставлению ответов на запросы Росфинмониторинга, отсутствует право на отказ от совершения операций, а также на отказ от заключения договора с клиентом в случае наличия подозрений о причастности к ОД/ФТ.

После внедрения ЕАС ПОД/ФТ структура расходов для субъектов Закона № 115-ФЗ, связанных с осуществлением требований антиотмывочного законодательства, должна измениться согласно формуле, представленной в приложении Д.

Соответственно изменениям для субъектов Закона № 115-ФЗ произойдут изменения в деятельности Росфинмониторинга и контрольно-надзорных органов в сфере ПОД/ФТ в результате внедрения ЕАС ПОД/ФТ. Осуществление контрольно-надзорной деятельности облегчится за счет наличия удаленного доступа к информационным системам субъектов Закона № 115-ФЗ, формирования единой базы данных ФЭС поднадзорных субъектов и частичного снятия обязанностей с субъектов Закона № 115-ФЗ за счет передачи их ЕАС ПОД/ФТ, что позволит контрольно-надзорным органам сконцентрироваться на проверке меньшего числа требований.

Несмотря на передачу части обязанностей ЕАС ПОД/ФТ у субъектов Закона № 115-ФЗ все равно останется обязательство по разработке правил внутреннего контроля. Связано это, в первую очередь, с невозможностью полной автоматизации двух процессов – идентификации клиентов и выявления признаков подозрительности в операциях.

Идентификация клиентов требует получения первичных документов от клиентов, а также принятия «обоснованных и доступных в сложившихся

обстоятельствах мер» по определению бенефициарного владельца клиента и его выгодоприобретателя, что полностью автоматизировать в существующих условиях не представляется возможным. В то же время, внедрение ЕАС ПОД/ФТ позволит облегчить процесс идентификации за счет направления запросов к государственным органам при осуществлении процедур идентификации (в том числе в налоговые органы и МВД) в целях проверки достоверности предоставленной информации, а также за счет формирования Единой децентрализованной базы данных клиентов субъектов Закона № 115-ФЗ.

Выявление признаков подозрительности в операциях также нецелесообразно полностью возлагать на ЕАС ПОД/ФТ, так как порой на наличие признаков ОД/ФТ в деятельности клиента может указывать не только наличие формальных признаков в финансовых операциях клиента, но и поведение клиента или его представителей. Также несмотря на развитие технологий искусственного интеллекта в части машинного обучения по совокупности интеллектуальных возможностей программные комплексы искусственного интеллекта не превосходят человеческий интеллект, в связи с чем выявление признаков подозрительности в операциях, требующее порой разностороннего и творческого подхода, должно осуществляться помимо ЕАС ПОД/ФТ также человеком. При этом, появится вероятность дублирования сообщений, направляемых должностными лицами, отвечающими за осуществление внутреннего контроля в организации, и сообщений, направляемых ЕАС ПОД/ФТ, в отношении одной и той же операции. Это требует внедрения в ЕАС ПОД/ФТ механизмов автоматизированного выявления и «склеивания» дубляжей.

Также разработка правил внутреннего контроля и назначение ответственного за соблюдение требований Закона № 115-ФЗ должностного лица необходима в силу того, что по вышеуказанным причинам гражданско-правовой ответственности за несоблюдение условий договора, принятие решения о разрыве договора, а также о приостановлении операции, в которой имеются признаки ОД/ФТ, целесообразно оставить за самим субъектом Закона № 115-ФЗ.

В связи с наличием обязательств субъектов Закона № 115-ФЗ по разработке правил внутреннего контроля, осуществлению идентификации клиентов и выявлению подозрительных операций необходимым останется и осуществление контрольно-надзорной деятельности в отношении данных субъектов. Кроме того, так как при внедрении в информационную систему субъектов ЕАС ПОД/ФТ значительная часть их обязанностей будет возложена на автоматизированную систему, то целесообразно осуществлять надзор за правильностью внедрения и функционирования ЕАС ПОД/ФТ в информационных системах субъектов Закона № 115-ФЗ.

Соответственно, стоит ожидать изменения ст. 15.27 КоАП РФ с включением в нее состава, предусматривающего административную ответственность за отсутствие подключения к ЕАС ПОД/ФТ или за подключение к ЕАС ПОД/ФТ, осуществленное с нарушением правил подключения к ЕАС ПОД/ФТ, которое повлекло или могло повлечь непредставление или неверное представление сведений в уполномоченный орган. При этом, с учетом того, что функционал ЕАС ПОД/ФТ предполагает, как направление ФЭС об ОПОК, так и блокирование денежных средств лиц, причастных к терроризму и экстремизму, ответственность за вышеуказанное правонарушение может ранжироваться в значительном диапазоне в зависимости от тяжести правонарушения (или возможно ввести несколько составов правонарушений в виде разных частей статьи 15.27 КоАП РФ, различающихся по тяжести административного деликта).

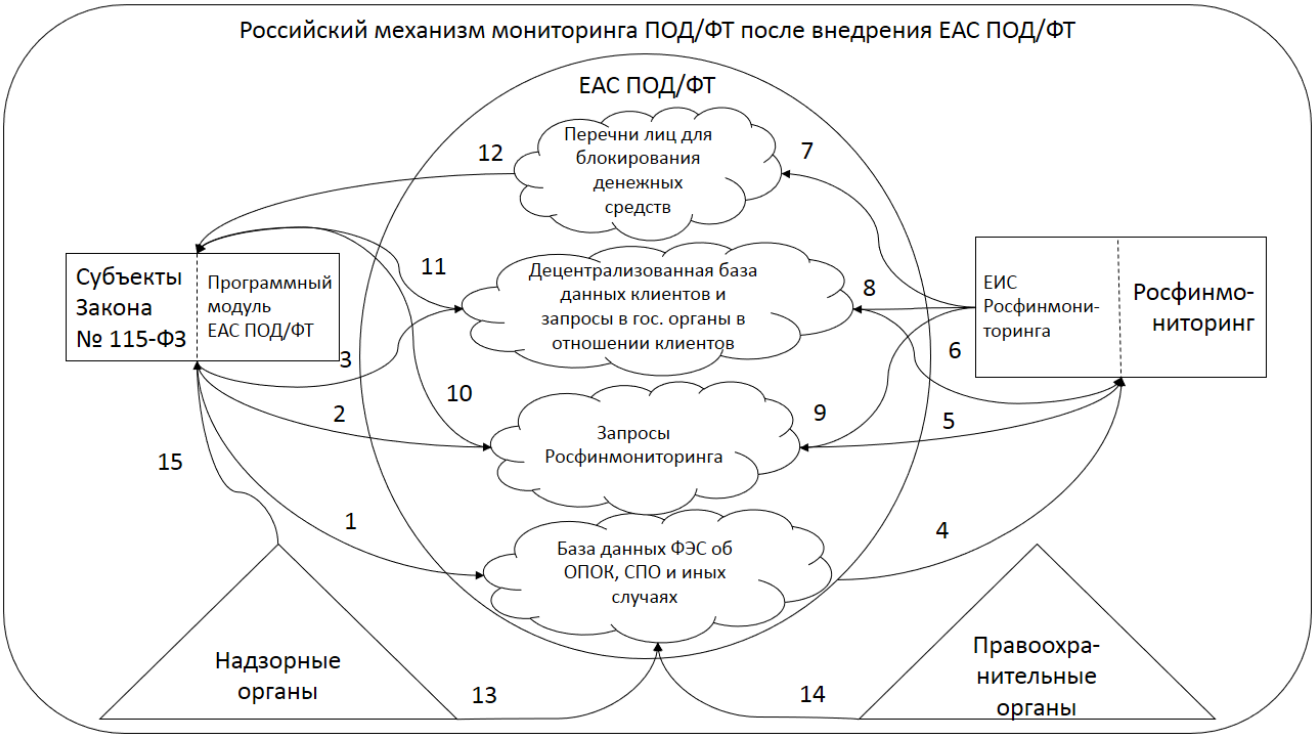
Осуществление контрольно-надзорной деятельности за правильностью внедрения и функционирования ЕАС ПОД/ФТ, а также за иными обязательствами субъектов Закона № 115-ФЗ возможно в текущем формате с преобладанием дистанционного надзора и проведением выездных проверок в случае выявления фактов совершения нарушений.

Внедрение ЕАС ПОД/ФТ целесообразно начинать с кредитных организаций, как занимающих ключевую роль в системе ПОД/ФТ (так как именно они опосредуют наибольший объем финансовых операций), обладающих наибольшими финансовыми и людскими ресурсами среди субъектов Закона

№ 115-ФЗ, а также в значительной степени осуществляющих информатизацию своей деятельности. Также внедрение ЕАС ПОД/ФТ в виде модулей возможно в информационные системы некредитных финансовых организаций, а также организаций федеральной почтовой связи и операторов связи, имеющих право самостоятельно оказывать услуги по передаче данных. Внедрение ЕАС ПОД/ФТ в информационные системы остальных субъектов Закона № 115-ФЗ следует рассматривать, как опциональное решение, которое может быть недоступно в связи с отсутствием необходимой информационной инфраструктуры для внедрения программных модулей ЕАС ПОД/ФТ (что также применимо к кредитным и некредитным финансовым организациям, организациям федеральной почтовой связи и операторам связи, не имеющим необходимых условий для внедрения программных модулей ЕАС ПОД/ФТ).

Кроме того, ЕАС ПОД/ФТ может содержать отдельный подмодуль, отвечающий за взаимодействие Росфинмониторинга с правоохранительными органами. Функционал такого модуля может предусматривать удаленный доступ правоохранительных органов к направляемым ФЭС, что позволит, как оптимизировать документооборот в государственных органах, снизить нагрузку на сотрудников Росфинмониторинга в части ответов на запросы правоохранительных органов, не требующих проведения финансовых расследований или предоставления иной аналитики, так и сократить сроки взаимодействия между ведомствами. Это, в конечном итоге, повысит эффективность межведомственного взаимодействия и будет способствовать росту отдачи от такого взаимодействия в виде значимого результата по обвинительным приговорам и конфискации. Стоит отметить, что отсутствие доступа к базам данных Росфинмониторинга в режиме реального времени выделяется Лебедевым И.А, Ефимовым С.В. и Потехиной В.В. в качестве одного из ключевых недостатков российского механизма мониторинга ПОД/ФТ [244]. При этом, получение правоохранительными органами доступа к данным ЕАС ПОД/ФТ должно найти законодательное закрепление в Законе № 115-ФЗ, так как связано с получением сведений, составляющих банковскую и коммерческую тайну.

Таким образом, претерпит изменение весь механизм мониторинга противодействия отмыванию доходов, полученных преступным путем, и финансированию терроризма. Трансформация механизма мониторинга ПОД/ФТ в результате внедрения ЕАС ПОД/ФТ представлена на рисунках 43–46. Также схема механизма мониторинга ПОД/ФТ после внедрения ЕАС ПОД/ФТ в деятельность субъектов Закона № 115-ФЗ может быть изображена в виде, представленном на рисунке 47.



Источник: составлено автором.

Рисунок 43 – Трансформация механизма мониторинга ПОД/ФТ в результате внедрения ЕАС ПОД/ФТ

В связи с вышеотмеченными тенденциями роста использования криптовалют в целях ОД/ФТ отдельное внимание следует уделить внедрению ЕАС ПОД/ФТ в информационные системы операторов выпуска и обмена ЦФА, также оборота цифровых валют. Наравне с решением вопроса о введение операторов оборота цифровых валют в список субъектов Закона № 115-ФЗ, внедрение программных модулей ЕАС ПОД/ФТ в информационные системы операторов выпуска и обмена ЦФА и операторов оборота цифровых валют позволит повысить эффективность выявления криптовалютных операций и операций с ЦФА, связанных с ОД/ФТ.

Элементы схемы трансформация механизма мониторинга ПОД/ФТ в результате внедрения ЕАС ПОД/ФТ

Номер элемента	Описание элемента
1	ФЭС, направляемые ЕАС ПОД/ФТ и сотрудниками субъектов Закона № 115-ФЗ в Росфинмониторинг
2	Ответы на запросы Росфинмониторинга
3	Запросы в Единую децентрализованную базу данных клиентов субъектов Закона № 115-ФЗ на предмет прохождения тем или иным лицом процедуры идентификации ранее, результатов оценки рисков ОД/ФТ в отношении данного лица, а также при необходимости запросы в государственные органы, в целях проверки сведений, направляемых клиентами. Также под данным элементом следует понимать передачу информации о результатах прохождения процедуры идентификации своих клиентов, их представителей, выгодоприобретателей и бенефициарных владельцев, направляемую субъектами Закона № 115-ФЗ, а также передачу результатов оценки рисков клиента программным модулем ЕАС ПОД/ФТ
4	Передача ФЭС в ЕИС Росфинмониторинга
5	Передача ответов на запросы в ЕИС Росфинмониторинга

Источник: составлено автором.

Рисунок 44 – Описание элементов схемы трансформации механизма мониторинга ПОД/ФТ в результате внедрения ЕАС ПОД/ФТ (начало)

Элементы схемы трансформация механизма мониторинга ПОД/ФТ в результате внедрения ЕАС ПОД/ФТ

Номер элемента	Описание элемента
6	Передача запросов субъектов Закона № 115-ФЗ в государственные органы в целях проверки информации, переданной клиентами
7	Загрузка информации о лицах, в отношении которых принято решение о замораживании денежных средств, в ЕАС ПОД/ФТ
8	Получение Росфинмониторингом результатов идентификации клиентов, их представителей, бенефициарных владельцев и выгодоприобретателей
9	Запросы Росфинмониторинга в адрес субъектов Закона № 115-ФЗ
10	Запросы Росфинмониторинга в адрес субъектов Закона № 115-ФЗ
11	Получение информации о клиентах из Единой децентрализованной базы данных клиентов субъектов Закона № 115-ФЗ, а также ответов от государственных органов
12	Загрузка в локальные информационные системы перечней лиц, в отношении которых принято решение о замораживании денежных средств, и выполнение данных решений программными модулями ЕАС ПОД/ФТ

Источник: составлено автором.

Рисунок 45 – Описание элементов схемы трансформации механизма мониторинга ПОД/ФТ в результате внедрения ЕАС ПОД/ФТ (продолжение)

Элементы схемы трансформация механизма мониторинга ПОД/ФТ в результате внедрения ЕАС ПОД/ФТ

Номер элемента	Описание элемента
13	Получение контрольно-надзорными органами сведений о ФЭС, направленных поднадзорными субъектами Закона № 115-ФЗ в адрес Росфинмониторинга
14	Доступ правоохранительных органов к базе данных ФЭС
15	Получение контрольно-надзорными органами необходимой документации у поднадзорных субъектов

Источник: составлено автором.

Рисунок 46 – Описание элементов схемы трансформации механизма мониторинга ПОД/ФТ в результате внедрения ЕАС ПОД/ФТ (окончание)

Источник: составлено автором.

Рисунок 47 - Структурная схема механизма мониторинга ПОД/ФТ после внедрения ЕАС ПОД/ФТ

В целом, модульность ЕАС ПОД/ФТ теоретически позволяет внедрить программный модуль и в информационную систему Банка России, опосредующую расчеты с использованием цифрового рубля, что, однако, зависит от реализации самой информационной системы цифрового рубля.

Внедрение ЕАС ПОД/ФТ в криптовалютные биржи, требует разработки правил выявления отдельных признаков подозрительности в криптовалютных операциях [235]. Данные признаки подозрительности могут быть сформулированы на основе приведенных во второй главе способов использования цифровых валют

в целях легализации преступных доходов и финансирования терроризма. Разработка признаков подозрительности для криптовалютных операций актуальна не только в контексте внедрения ЕАС ПОД/ФТ. Разработка таких признаков, в целом, необходима в связи с легализацией неторгового оборота цифровых валют в Российской Федерации, законодательных инициатив, направленных на регулирование майнинга криптовалют, а также распространением криптовалют в России [118]. Аналогичная необходимость существует и в отношении цифровых финансовых активов, операторы выпуска и обмена которых уже являются субъектами Закона № 115-ФЗ.

Разработанные признаки могут быть внесены в виде отдельного раздела в Положение Банка России 15 декабря 2014 г. № 445-П «О требованиях к правилам внутреннего контроля некредитных финансовых организаций в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма». Перечень признаков подозрительности для криптовалютных операций и операций с цифровыми финансовыми активами содержится в приложении Е.

Внедрение ЕАС ПОД/ФТ позволит учесть в процессе трансформации механизма мониторинга ПОД/ФТ на микроуровне и национальном уровне все ранее выделенные группы организационно-технологических факторов трансформации механизма мониторинга ПОД/ФТ в условиях цифровизации экономики. Функционал ЕАС ПОД/ФТ в разрезе групп организационно-технологических факторов трансформации механизма мониторинга ПОД/ФТ в условиях цифровизации экономики представлен в таблице 5.

Таким образом, трансформация механизма мониторинга ПОД/ФТ в результате внедрения ЕАС ПОД/ФТ позволит снизить, как издержки субъектов Закона № 115-ФЗ, так и государственных органов (в части сокращения трудозатрат на осуществление надзора и экономии человеко-часов на обеспечение документооборота).

Таблица 5 – Функционал ЕАС ПОД/ФТ в разрезе групп организационно-технологических факторов трансформации механизма мониторинга ПОД/ФТ в условиях цифровизации экономики

Номер группы	Группа организационно-технологических факторов трансформации механизма мониторинга ПОД/ФТ в условиях цифровизации экономики	Функционал ЕАС ПОД/ФТ, позволяющий учесть группу факторов в процессе трансформации механизма мониторинга ПОД/ФТ
1	2	3
Факторы, способствующие развитию механизма мониторинга ПОД/ФТ		
а1	Повышение аналитических возможностей	Автоматизированное направление ФЭС об ОПОК, заблокированных операциях и выявленных ЕАС ПОД/ФТ подозрительных операциях, а также предоставление рекомендаций по блокированию финансовых операций; Автоматизированная подготовка ответов на запросы Росфинмониторинга; Автоматизированное определение уровня риска ОД/ФТ в действиях клиента
а2	Расширение возможностей по хранению информации и ее обработке	Создание Единой децентрализованной базы данных клиентов субъектов Закона № 115-ФЗ и обеспечение хранения и актуализации в ней информации об идентифицированных клиентах
а3	Увеличение скорости обмена информации и объема передаваемых данных	Автоматизированное направление ФЭС об ОПОК, заблокированных операциях и выявленных ЕАС ПОД/ФТ подозрительных операциях; Автоматизированная подготовка ответов на запросы Росфинмониторинга; Направление запросов в базы данных государственных органов; Организация доступа контрольно-надзорных органов к информации о направленных ФЭС и документации об организации системы внутреннего контроля в отношении ПОД/ФТ, а также правоохранительных органов к базе данных ФЭС
Факторы, затрудняющие реализацию механизма мониторинга ПОД/ФТ		
б1	Появление новых технологий, способов, средств платежа и осуществления сделок, а также иных новшеств, влияющих на эффективное функционирование механизма мониторинга ПОД/ФТ, не охваченных требованиями антиотмывочного законодательства	Модульность ЕАС ПОД/ФТ и возможность оперативного расширения области мониторинга за счет донастройки ЕАС ПОД/ФТ с целью выявления операций по добавленным признакам ОПОК и подозрительных операций

Продолжение таблицы 5

1	2	3
б2	Использование технологий цифровой экономики в целях воспрепятствования осуществлению и реализации механизма мониторинга ПОД/ФТ	Внедрение в ЕАС ПОД/ФТ признаков подозрительности в операциях с цифровыми валютами и ЦФА; Автоматизированное направление ФЭС об ОПОК, заблокированных операциях и выявленных ЕАС ПОД/ФТ подозрительных операциях, а также предоставление рекомендаций по блокированию финансовых операций (что должно привести к росту скорости выявления операций и сделок, предположительно связанных с ОД/ФТ, а также к повышению качества аналитики за счет возможности применения искусственного интеллекта для анализа разноформатных наборов данных, что, соответственно, позволит минимизировать негативное влияние алгоритмизации процесса ОД/ФТ)
б3	Повышение требований к скорости осуществления и реализации процедур механизма мониторинга ПОД/ФТ, а также к аналитическим возможностям структурных звеньев механизма мониторинга ПОД/ФТ	Ускорение процесса надлежащей проверки клиентов за счет направления запросов в Единую децентрализованную базу данных клиентов субъектов Закона № 115-ФЗ и государственные органы; Организация доступа контрольно-надзорных органов к информации о направленных ФЭС и документации об организации системы внутреннего контроля в отношении ПОД/ФТ, а также правоохранительных органов к базе данных ФЭС

Источник: составлено автором.

Модификация механизма мониторинга ПОД/ФТ позволит минимизировать такие его недостатки, как длительность получения ФЭС от субъектов Закона № 115-ФЗ, а также получения ответов на запросы Росфинмониторинга. Будет облегчен процесс осуществления контрольно-надзорной деятельности в отношении субъектов Закона № 115-ФЗ, а также ускорится процесс получения необходимой информации правоохранительными органами. Изменение механизма мониторинга ПОД/ФТ, связанное с внедрением в информационные системы субъектов Закона № 115-ФЗ, потребует значительных материальных затрат на начальном этапе на разработку данного программно-аппаратного комплекса, а также на его встраивание в информационные системы субъектов (которые, однако, могут быть снижены за счет реализации механизма государственно-частного

партнерства). Также можно ожидать опасений со стороны частного бизнеса, связанные с внедрением в их информационные системы программных модулей сторонней системы (которые могут быть снижены принятием всех необходимых мер обеспечения безопасности передачи информации между программным модулем ЕАС ПОД/ФТ, облачными хранилищами и ЕИС в сфере ПОД/ФТ). Однако, трансформацию механизма мониторинга ПОД/ФТ путем внедрения ЕАС ПОД/ФТ можно назвать логичным продолжением текущих тенденций развития механизма мониторинга ПОД/ФТ, его дальнейшим этапом развития, в связи с чем, подобное изменение механизма будет так или иначе реализовано, вопрос заключается лишь во временном промежутке и конкретной реализации данного развития, одна из которых и представлена выше в работе.

Выводы по 3 главе

Цифровизация экономики приводит как к расширению возможностей в сфере противодействия отмыванию преступных доходов и финансированию терроризма, так и появлению новых вызовов для существующего механизма мониторинга ПОД/ФТ.

Связанные с цифровизацией экономики риски эффективного функционирования механизма мониторинга ПОД/ФТ, связанные с цифровизацией экономики, и преимущества цифровизации экономики, за счет которых возможно повышение эффективности механизма мониторинга ПОД/ФТ, можно представить в виде следующей классификации:

а) «Актуальные риски ОД/ФТ:

1) Использование криптовалют в целях ОД/ФТ, а также иных цифровых активов, в отношении которых отсутствуют устойчивые практики ПОД/ФТ.

2) Увеличение скорости осуществления денежных переводов, а также повышение темпов торговли на фондовом рынке, что предъявляет повышенные требования к программным системам ПОД/ФТ в части хранения информации и скорости анализа операций на наличие признаков ОД/ФТ.

3) Использование искусственного интеллекта в целях разрыва цепочки криптовалютных операций между плательщиком и получателем.

б) Потенциальные риски ОД/ФТ:

1) Использование технологий искусственного интеллекта в целях алгоритмизации процесса ОД/ФТ.

2) Применение smart-контрактов в целях ОД/ФТ в качестве средства сокрытия улик совершения финансовых операций в отсутствие на то экономических оснований.

3) Использование технологии «deepfake» и вредоносного программного обеспечения в целях обхода биометрических средств идентификации клиента» [235, с. 8–9].

в) Преимущества цифровизации экономики, за счет которых возможно повышение эффективности механизма мониторинга ПОД/ФТ:

1) Рост процентной доли безналичных финансовых операций в общем объеме платежей способствует снижению оборота наличных денежных средств, что повышает прозрачность финансовой системы.

2) Применение технологий искусственного интеллекта для отслеживания криптовалют (в том числе, криптовалют с повышенной степенью анонимности операций), а также для повышения результативности работы программных комплексов ПОД/ФТ, что позволяет за счет использования технологий машинного обучения выявлять ранее не зафиксированные схемы ОД/ФТ и снижать количество ложноположительных срабатываний.

3) Использование биометрической идентификации и иных методов удаленного подтверждения личности в качестве средства проведения НПК в отсутствие личного контакта с клиентом (в том числе, клиентом криптовалютной биржи).

4) Внедрение государствами и надгосударственными образованиями цифровых валют, что способствует замещению анонимных криптовалют, повышает возможности проведения финансовых расследований, а также позволяет заблокировать использование выделенных денежных средств на нецелевые нужды.

5) Использование технологий искусственного интеллекта при осуществлении мер НПК, в том числе, за счет автоматизации процесса сбора информации о клиенте из открытых источников и государственных баз данных.

В результате анализа корреляционной зависимости между объемом совершаемых банками Российской Федерации подозрительных операций, связанных с выводом денежных средств за рубеж, а также с обналичиванием денежных средств, и количеством проведенных Банком России проверок кредитных организаций на предмет соблюдения требований антиотмывочного законодательства установлена взаимосвязь между данными величинами (что выразилось в сокращении количества проверок и уменьшении объема подозрительных операций). Это вкупе с отсутствием явной корреляционной зависимости между количеством проведенных Банком России проверок поднадзорных субъектов на предмет соблюдения требований антиотмывочного законодательства и количеством вынесенных Банком России по результатам проверок мер государственного принуждения, позволяет сделать вывод о том, что внедрение технологий цифровой экономики в контрольно-надзорную деятельность, осуществляемую за субъектами Закона № 115-ФЗ не только не снизило ее эффективность, но и привело к сокращению объема подозрительного финансового потока.

Анализ нормативно-правовых актов, заявлений представителей органов государственной власти, а также исследований в сфере ПОД/ФТ позволил выделить следующие направления развития отечественного механизма мониторинга ПОД/ФТ:

– введение цифрового рубля с целью контроля финансовых потоков, выделяемых на целевые нужды, с передачей обязанностей по осуществлению финансового мониторинга за операциями с цифровым рублем Банку России;

– устранение правового пробела, связанного с отсутствием обязанности по соблюдению требований антиотмывочного законодательства у операторов оборота цифровых валют (в том числе, зарубежных криптовалютных бирж), а также неурегулированностью статуса NFT;

– установление дополнительных требований в отношении разработчиков и пользователей ряда технологических инноваций (в частности, smart-контрактов), позволяющих снизить риски использования инноваций в целях ОД/ФТ по мере роста популярности использования инноваций в деловой практике;

– расширение практики осуществления удаленной идентификации клиентов кредитных организаций, операторов выпуска и обмена ЦФА и цифровых валют с использованием биометрической информации, данных, полученных из ЕСИА, а также за счет оптимизации процесса обмена данными в отношении клиентов, прошедших НПК, между кредитными организациями, операторами выпуска и обмена ЦФА и цифровых валют (в том числе, возможно развертывание единой системы обмена информацией между вышеуказанными субъектами);

– внедрение в деятельность профильных подразделений субъектов Закона № 115-ФЗ, а также органов финансового контроля технологий искусственного интеллекта и Big Data.

С учетом вышеизложенного возможно рассмотреть вопрос о модернизации отечественного механизма мониторинга ПОД/ФТ путем слияния микроуровня и национального уровня механизма мониторинга ПОД/ФТ. Конвергенция двух частей механизма мониторинга ПОД/ФТ позволит значительно усилить экономическую составляющую реализации механизма мониторинга ПОД/ФТ – пресечение нелегальных финансовых потоков с целью недопущения оказания ими негативного влияния на экономическую безопасность государства, за счет сокращения временного лага между совершением незаконной операции и получением соответствующей информации подразделением финансовой разведки, а также иных задержек, связанных с процессом взаимодействия Росфинмониторинга с субъектами первичного финансового мониторинга и выполнением субъектами Закона № 115-ФЗ требований государственного ведомства.

Реализовать подобную модернизацию возможно за счет внедрения в информационные системы субъектов первичного финансового мониторинга программных модулей Единой автоматизированной системой противодействия

отмыванию доходов, полученных преступным путем, и финансированию терроризма. Централизованный компонент такой системы будет размещаться в ЕИС в сфере ПОД/ФТ.

Программные модули ЕАС ПОД/ФТ должны представлять собой встраиваемые в информационные системы субъектов Закона № 115-ФЗ программные компоненты, функционал которых должен включать:

– проверку клиентов на наличие в перечне организаций и физических лиц, в отношении которых имеются сведения об их причастности к экстремистской деятельности или терроризму, составляемому Росфинмониторингом, а также перечнях организаций и физических лиц, связанных с терроризмом или с распространением оружия массового уничтожения, составляемых в соответствии с решениями Совета Безопасности ООН, а также в перечнях лиц, в отношении которых МВК по ФТ принято решение о замораживании денежных средств, с блокированием операций данных лиц за исключением разрешенных Законом № 115-ФЗ;

– осуществление оценки уровня риска ОД/ФТ в отношении клиента (за основу чего можно взять платформу «Знай своего клиента» Банка России) и облегчение процессов идентификации клиентов за счет возможности осуществления идентификации личности клиента удаленно в случае прохождения процедуры клиентом в ином субъекте Закона № 115-ФЗ, подключенного к ЕАС ПОД/ФТ, а также за счет автоматизированного направления запросов в государственные органы;

– выявление операций, подлежащих обязательному контролю, а также подозрительных операций, и направление сообщений об этом в ЕИС в сфере ПОД/ФТ;

– направление ответов на запросы Росфинмониторинга.

Внедрение в информационные системы субъектов первичного финансового мониторинга программных модулей ЕАС ПОД/ФТ позволит Росфинмониторингу сократить временной промежуток между моментом совершения операции, о которой следует проинформировать подразделение финансовой разведки, и

моментом получения службой сообщения о данной операции. Также это может позволить повысить качество сообщений о подозрительных операциях, передаваемых субъектами Закона № 115-ФЗ, не имеющих квалифицированного подразделения, осуществляющего внутренний контроль на предмет выявления операций, связанных с ОД/ФТ. Внедрение ЕАС ПОД/ФТ позволит также сократить время получения и повысить качество ответов на запросы Росфинмониторинга.

Внедрение ЕАС ПОД/ФТ несет преимущества также и для субъектов Закона № 115-ФЗ в связи с тем, что внедрение программных модулей системы позволит субъектам первичного финансового мониторинга сократить издержки, указанные на рисунке 48.

Расходы, которые сократятся у субъектов микроуровня механизма мониторинга ПОД/ФТ в случае внедрения программных модулей ЕАС ПОД/ФТ
• Расходы, связанные с дублированием информации в контрольно-надзорные органы о сообщениях, направленных в адрес Росфинмониторинга. • Расходы, связанные с направлением ФЭС об ОПОК и СПО (частично), замораживании средств лиц, включенных в перечни Росфинмониторинга и Совета Безопасности ООН, а также лиц, в отношении которых принято решение о замораживании их средств Межведомственной комиссией по противодействию финансированию терроризма. • Расходы, связанные с предоставлением информации в Росфинмониторинг. • Расходы, связанные с уплатой штрафов за неисполнение требований антиотмывочного законодательства (в связи с сокращением количества обязанностей, предъявляемых к субъектам Закона № 115-ФЗ, в случае внедрения ЕАС ПОД/ФТ). • Расходы, связанные с облегчением процесса идентификации клиентов в связи с возможностью направления автоматизированных запросов в государственные органы.

Источник: составлено автором.

Рисунок 48 - Расходы, которые сократятся у субъектов микроуровня механизма мониторинга ПОД/ФТ в случае внедрения программных модулей ЕАС ПОД/ФТ

Внедрение программных модулей в информационные системы операторов выпуска и обмена цифровых финансовых активов и операторов оборота цифровых валют требует разработки правил выявления отдельных признаков подозрительности в криптовалютных операциях и операциях, связанных с оборотом криптотокенов (что, однако, актуально и вне связи с внедрением ЕАС ПОД/ФТ).

Данные признаки подозрительности могут быть сформулированы на основе приведенных во второй главе способов использования цифровых валют в целях легализации преступных доходов и финансирования терроризма. Разработанные признаки могут быть внесены в виде отдельного раздела в Положение Банка России 15 декабря 2014 г. № 445-П «О требованиях к правилам внутреннего контроля некредитных финансовых организаций в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

Заключение

В рамках проведенного исследования осуществлен анализ имеющихся экономических и юридических (в силу большей проработанности дефиниций именно в данной области научного познания) доктринальных трактовок понятий «отмывание доходов, полученных преступным путем», «легализация доходов, полученных преступным путем» и «финансирование терроризма», а также содержащихся в российских и международных правовых актах определений данных терминов, на основе чего сформулирован авторский подход к экономической трактовке отмывания преступных доходов. Относительно финансирования терроризма в работе используется определение, применяемое в ст. 3 Федерального закона «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», согласно которому к финансированию терроризма относится «предоставление или сбор средств либо оказание финансовых услуг с осознанием того, что они предназначены для финансирования организации, подготовки и совершения хотя бы одного из преступлений, предусмотренных статьями 205; 205.1; 205.2; 205.3; 205.4; 205.5; 206; 208; 211; 220; 221; 277; 278; 279; 360 и 361 Уголовного кодекса Российской Федерации, либо для финансирования или иного материального обеспечения лица в целях совершения им хотя бы одного из указанных преступлений, либо для обеспечения организованной группы, незаконного вооруженного формирования или преступного сообщества (преступной организации), созданных или создаваемых для совершения хотя бы одного из указанных преступлений» в связи с правовой природой разделения деяний, связанных с финансированием терроризма, и иных деяний, связанных с формированием и распределением фондов денежных средств и иного имущества [34].

Формулирование экономической интерпретации понятия легализации (отмывания) доходов, полученных преступным путем, определило необходимость выработки научно-экономического подхода к определению процесса ПОД/ФТ (без

разделения процесса ПОД от процесса ФТ с учетом отмеченного в работе частичного сходства в методах осуществления противоправных деяний), а также механизма мониторинга ПОД/ФТ. На основе оценки имеющихся определений понятия «механизм ПОД/ФТ» (носящих правовой характер), а также с учетом сформулированного ранее экономического подхода к ОД, было представлено определение ПОД/ФТ с экономической точки зрения и, соответственно, определение механизма ПОД/ФТ, как составной части механизма обеспечения экономической безопасности государства. Опираясь на сформированные в научных источниках определения финансового мониторинга, выделен механизм мониторинга ПОД/ФТ, как составная часть механизма ПОД/ФТ, в рамках которой на основании анализа информации «о проводимых финансовых операциях и заключаемых сделках осуществляется выявление операций, связанных с легализацией (отмыванием) доходов, полученных преступным путем, или финансированием терроризма, результаты чего передаются в правоохранительные и иные государственные органы в целях принятия ими мер, направленных на противодействие легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» [234, с. 6]. С учетом представленного определения сформирована многоуровневая модель функционирования механизма мониторинга ПОД/ФТ с позиции информационного взаимодействия его участников, а также модель трансформации механизма мониторинга ПОД/ФТ в контексте влияния на него организационно-технологических факторов трансформации механизма мониторинга ПОД/ФТ в условиях цифровизации экономики.

После этого был осуществлен обзор истории становления наднационального уровня механизма мониторинга ПОД/ФТ, а также процесса развития национального уровня механизма мониторинга ПОД/ФТ. Анализ международного опыта разработки положений, формирующих основу национального уровня механизма мониторинга ПОД/ФТ, позволил изучить процесс формирования тех международных норм, которые послужили базисом для отечественного механизма мониторинга ПОД/ФТ. Исследование отечественного механизма мониторинга

ПОД/ФТ позволило не только отследить процесс его развития, но и проанализировать текущее состояние механизма мониторинга ПОД/ФТ в Российской Федерации, а также выделить его основные составляющие. Осуществлен анализ мер по трансформации российского механизма мониторинга ПОД/ФТ в разрезе внедряемых нововведений, а также факторов, способствующих внедрению изменений в механизм мониторинга ПОД/ФТ Российской Федерации. Кроме того, сформирована классификация внедряемых цифровых новаций по группам организационно-технологических факторов трансформации механизма мониторинга ПОД/ФТ в условиях цифровизации экономики. Также был проведен анализ влияния цифровизации экономики на способы ОД/ФТ, применяемые злоумышленниками. С учетом вышеизложенного были выделены недостатки в существующем национальном механизме мониторинга ПОД/ФТ с учетом влияния цифровизации экономики, а также требования к его совершенствованию (и, соответственно, определены требования основные пути трансформации российского механизма мониторинга ПОД/ФТ).

В контексте цифровизации экономики проанализировано влияние на механизм мониторинга ПОД/ФТ нововведений цифровой экономики, в том числе технологии блокчейн (как технологии, в целом, и как способа хранения информации о криптовалютных транзакциях и операциях с цифровыми валютами, в частности), искусственного интеллекта и удаленной идентификации (в том числе, биометрической). Изучено влияние перехода к дистанционной форме надзора на эффективность национального механизма мониторинга ПОД/ФТ, по итогам чего отмечено отсутствие явной корреляционной зависимости между количеством проведенных Банком России проверок поднадзорных субъектов на предмет соблюдения требований антиотмывочного законодательства и количеством вынесенных Банком России по результатам проверок мер государственного принуждения. Это вкупе с наличием взаимосвязи между снижением объема подозрительного финансового потока и внедрением дистанционной формы надзора позволило сделать вывод о положительном влиянии цифровизации механизма мониторинга ПОД/ФТ на его эффективность. Составлена

классификация рисков эффективного функционирования механизма мониторинга ПОД/ФТ, связанных с цифровизацией экономики, и преимуществ цифровизации экономики, за счет которых возможно повышение эффективности механизма мониторинга ПОД/ФТ. Осуществлен анализ данных рисков и преимуществ в разрезе групп организационно-технологических факторов трансформации механизма мониторинга ПОД/ФТ в условиях цифровизации экономики и уровней механизма мониторинга ПОД/ФТ.

На основе анализа тенденций изменения законодательства Российской Федерации, а также научных публикаций в сфере ПОД/ФТ был выделен ряд направлений развития российского механизма мониторинга ПОД/ФТ. В качестве одного из направлений развития отечественного механизма мониторинга ПОД/ФТ было приведено внедрение систем искусственного интеллекта в деятельность субъектов Закона № 115-ФЗ. С учетом того, что данное направление трансформации механизма мониторинга ПОД/ФТ может способствовать его как интенсивному (в плане повышения скорости и качества анализа операций на предмет выявления в них признаков ОД/ФТ), так и экстенсивному (внедрение систем искусственного интеллекта в информационные системы операторов оборота цифровых финансовых активов и цифровых валют с целью отслеживания криптовалютных транзакций и иных операций с виртуальными активами) развитию, автором предложена модель модернизации механизма мониторинга ПОД/ФТ путем конвергенции микроуровня и национального уровня механизма мониторинга ПОД/ФТ за счет внедрения в информационные системы субъектов Закона № 115-ФЗ программных модулей ЕАС ПОД/ФТ, основанных на технологии искусственного интеллекта. Помимо того, в исследовании представлены предложения по разработке признаков подозрительности операций, совершаемых с криптовалютами и ЦФА, которые могут быть внедрены в механизм мониторинга ПОД/ФТ как в рамках ЕАС ПОД/ФТ, так и отдельно от нее.

Деятельность программных модулей ЕАС ПОД/ФТ может в ряде случаев заменить существующие программные комплексы, внедряемые субъектами Закона № 115-ФЗ (большинство из которых является иностранным ПО), а также

расширить их функционал. При этом, наибольший эффект от внедрения ЕАС ПОД/ФТ стоит ожидать в случае субъектов Закона № 115-ФЗ, не располагающих ресурсами, достаточными для внедрения продвинутых программных комплексов ПОД/ФТ в собственные информационные системы.

Экономический эффект от внедрения программных модулей ЕАС ПОД/ФТ в информационные системы субъектов Закона № 115-ФЗ, по нашему мнению, будет состоять как в снижении издержек данных субъектов на соблюдение требований антиотмывочного законодательства (в том числе, связанных с внедрением в собственные информационные системы специализированного программного обеспечения, обеспечением контрольно-надзорного процесса, исполнением мер государственного принуждения), так и в повышении качества процесса мониторинга ПОД/ФТ (за счет расширения возможностей по выявлению подозрительных операций субъектами Закона № 115-ФЗ, не обладающих значительными ресурсами на качественное обеспечение требований антиотмывочного законодательства, за счет повышения качества процедур НПК путем направления запросов в государственные органы и улучшения качества ответов на запросы Росфинмониторинга), что, в свою очередь, позволит повысить оперативность применения мер, направленных на привлечение к ответственности лиц, причастных к ОД/ФТ и, тем самым, снизить негативный эффект, оказываемый финансовыми потоками, связанными с ОД/ФТ, на экономическую безопасность государства. Кроме того, внедрение ЕАС ПОД/ФТ позволит сделать больший акцент в процессе реализации механизма мониторинга ПОД/ФТ на предотвращение незаконных финансовых операций, нежели на выявление факта их совершения и круга участников. Это позволит в большей степени реализовать экономическое назначение механизма мониторинга ПОД/ФТ, заключающееся в недопущении проникновения незаконных финансовых средств в легальный экономический оборот, а также пресечении финансирования терроризма, что позволит оградить экономику от негативного влияния, как «грязных» денег, так и социально-экономических процессов, связанных с ОД/ФТ.

Таким образом, трансформация механизма мониторинга ПОД/ФТ за счет внедрения ЕАС ПОД/ФТ и признаков подозрительности операций, совершаемых с цифровыми валютами и цифровыми финансовыми активами, является логическим завершением ранее описанных в работе предложений. Так, данная трансформация позволит сделать больший акцент в реализации механизма мониторинга ПОД/ФТ на принятии мер по пресечению проникновения незаконно полученных доходов и средств, предназначенных для оказания поддержки террористам и террористическим организациям, в экономику страны, что отвечает сформированному экономическому подходу к определению механизма мониторинга ПОД/ФТ. В рамках указанной трансформации находят свое применение все преимущества цифровизации экономики, за счет которых возможно повышение эффективности механизма мониторинга ПОД/ФТ, приведенные в вышеуказанной классификации. Данная трансформация механизма мониторинга ПОД/ФТ направлена на минимизацию всех актуальных рисков ОД/ФТ, содержащихся в разработанной классификации, а также такого потенциального риска, как использование технологий искусственного интеллекта в целях алгоритмизации процесса ОД/ФТ (за счет внедрения ЕАС ПОД/ФТ в информационные системы субъектов первичного финансового мониторинга, что в перспективе может позволить более эффективно противостоять попыткам использования искусственного интеллекта в противозаконных целях (составлено на основе результатов, полученных совместно с Шевляковым Е.В. [271]). Потенциальный риск применение smart-контрактов в качестве средства сокрытия улик ОД/ФТ требует выработки правового решения, тогда как решение по минимизации риска использования технологии «deepfake» и вредоносного программного обеспечения в целях обхода биометрических средств идентификации клиента лежит скорее в области информационной безопасности и не связано непосредственно с трансформационными процессами в механизме мониторинга ПОД/ФТ, в связи с чем выработка ответа на данные риски лежит вне сферы данного исследования.

Кроме того, анализ рисков эффективного функционирования механизма мониторинга ПОД/ФТ, связанных с цифровизацией экономики, и преимуществ цифровизации экономики, за счет которых возможно повышение эффективности механизма мониторинга ПОД/ФТ, в разрезе групп организационно-технологических факторов трансформации механизма мониторинга ПОД/ФТ в условиях цифровизации экономики и уровней механизма мониторинга ПОД/ФТ, позволил установить, что данные риски и преимуществ наибольшее влияние оказывают на процессы трансформации микроуровня и национального уровня механизма мониторинга ПОД/ФТ. В соответствии с этим предложенная в исследовании модернизация механизма мониторинга ПОД/ФТ предполагает модернизацию микроуровня и национального уровня механизма мониторинга ПОД/ФТ, позволяющую учесть все группы организационно-технологических факторов трансформации механизма мониторинга ПОД/ФТ в условиях цифровизации экономики.

Резюмируя, стоит отметить, что внедрение ЕАС ПОД/ФТ можно рассматривать как следующую стадию эволюционного развития механизма мониторинга ПОД/ФТ, когда за счет внедрения достижений цифровизации экономики возможно не только минимизировать порождаемые данной же цифровизацией вызовы, но и значительно расширить возможности механизма мониторинга ПОД/ФТ как средства обеспечения экономической безопасности государства.

Список литературы

Книги и монографии

1. Авдийский, В.И. Теневая экономика и экономическая безопасность государства : учебное пособие / В.И. Авдийский, В.А. Дадалко, Н.Г. Синявский. – 3-е издание. – Москва : ИНФРА-М, 2021. – 538 с. – ISBN 978-5-16-017141-8.

2. Актуальные вопросы разработки системы управления рисками в сфере противодействия отмыванию доходов и финансированию терроризма : монография / И.А. Лебедев, С.В. Ефимов, С.С. Фешина [и др.] ; под редакцией кандидата экономических наук, доцента И.А. Лебедева. – Москва : Прометей, 2021. – 270 с. – 500 экз. – ISBN 978-5-00172-130-7.

3. Бекетнова, Ю.М. Типологический анализ в финансовом мониторинге : учебное пособие / Ю.М. Бекетнова – Москва : Прометей. – 2020. – 260 с. – ISBN 978-5-00172-055-3.

4. Богомолов, С.Ю. Ответственность за финансирование терроризма: уголовно-правовое криминологическое исследование : монография / под редакцией доктора юридических наук, доцента А.В. Петрянина. – Москва : Проспект, 2021. – 256 с. – 500 экз. – ISBN 978-5-392-34237-2.

5. Гаврилин, Ю. В. Установление владельцев криптовалютных кошельков при расследовании преступлений в сфере незаконного оборота наркотических средств : учебное пособие / Ю. В. Гаврилин, И. С. Бедеров. – Москва : Академия управления МВД России, 2022. – 76 с. – ISBN 978-5-907530-11-9.

6. Зубков, В.А. Российская Федерация в международной системе противодействия легализации (отмыванию) преступных доходов и финансированию терроризма / В.А. Зубков, С.К. Осипов. – 2-е издание, переработанное и дополненное. – Москва : Издательский дом «Городец», 2007. – 752 с. – ISBN 5–9584–0137–8.

7. Кернер, Х.-Х. Отмывание денег : Путеводитель по действующему законодательству и юридической практике / Х.-Х. Кернер, Э. Дах ; [перевод с

немецкого]. – Москва : Международные отношения, 1996. - 235 с. – ISBN 5-7133-0886-3.

8. Крылов, Г.О. Проблемы безопасности оборота цифровых финансовых активов в криптоэкономике : монография / Г.О. Крылов, В.М. Селезнев. – Москва : Прометей, 2020. – 348 с. – 500 экз. – ISBN 978-5-907244-98-6.

9. Международная система противодействия легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения : учебное пособие для студентов высших учебных заведений / П. В. Ливадный, В. П. Нечаев, Г. Ю. Негляд [и др.] ; под редакцией Г.Ю. Негляда, Ю.В. Лафитской — Москва : ЮНИТИ-ДАНА, 2022. — 455 с. – ISBN 978-5-238-03594-9.

10. Ответственность за отмывание (легализацию) коррупционных доходов по законодательству зарубежных государств : научно-практическое пособие / И.С. Власов, Н.В. Власова, Н.А. Голованова [и др.] ; ответственные редакторы доктор юридических наук, профессор А.Я. Капустин, кандидат юридических наук А.М. Цирин. – Москва : ИНФРА-М, 2019. – 312 с. – ISBN 978-5-16-012885-6.

11. Финансовый мониторинг : учебное пособие для бакалавриата и магистратуры : в 2 томах / Том 1 / А.Г. Братко, И.Е. Волуевич, В.И. Глотов [и др.] ; под редакцией кандидата экономических наук Ю.А. Чиханчина, доктора юридических наук, профессора А.Г. Братко. – Москва : Юстицинформ, 2018. – 1 том – 696 с. – ISBN 978-5-7205-1426-6.

12. Шваб, Клаус. Четвертая промышленная революция / Клаус Шваб ; [перевод с английского]. – Москва : Эксмо, 2016. – 138 с. – ISBN 978-5-699-98379-7.

13. Шумилов, В.М. Международное финансовое право : учебник / В.М. Шумилов. – Москва : Междунар. отношения, 2005. – 430 с. – ISBN 5-7133-1249-6.

14. Экономическая безопасность : учебник / Н.Г. Гаджиев, М.А. Газимагомедов, А.В. Доронин [и др.] ; под общей редакцией кандидата

экономических наук, доцента С.А. Коноваленко. – Москва : ИНФРА-М, 2021. – 526 с. – ISBN 978-5-16-015729-0.

15. Экономическая безопасность России. Общий курс : учебник / под редакцией В. К. Сенчагова. – 2-е издание. – Москва : Дело, 2005. – 896 с. – ISBN 5-7749-0391-5.

Нормативные правовые акты

16. Договор государств – участников Содружества Независимых Государств о противодействии легализации (отмыванию) преступных доходов и финансированию терроризма от 5 октября 2007 года [ратифицирован Федеральным законом от 27 декабря 2009 года № 349-ФЗ, вступил в силу для Российской Федерации 23 января 2010 года]. – Официальный интернет-портал правовой информации. – Текст : электронный. – URL: http://pravo.gov.ru/proxy/ips/?docbody=&link_id=7&nd=201061420&collection=1&ysclid=lxrqumi3f0121540517 (дата обращения: 23.06.2024).

17. Договор государств-участников Содружества Независимых Государств о противодействии легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения от 15 октября 2021 года [ратифицирован Федеральным законом от 4 ноября 2022 года № 413-ФЗ с заявлением, вступил в силу для Российской Федерации 26 апреля 2023 года]. – Официальный интернет-портал правовой информации. – Текст : электронный. – URL: http://publication.pravo.gov.ru/Document/View/0001202304260002?index=1&rangeSize=1 (дата обращения: 04.06.2023).

18. Конвенция об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности [ратифицирована Федеральным законом РФ от 28 мая 2001 года № 62-ФЗ с оговорками, вступила в силу для Российской Федерации

1 декабря 2001 года]. – Бюллетень международных договоров. – 2003. – № 3. – С. 14-46. – ISSN 0869-6705.

19. Конвенция Организации Объединенных Наций о борьбе против незаконного оборота наркотических средств и психотропных веществ [ратифицирована Постановлением Верховного Совета СССР от 9 октября 1990 года № 1711-1, вступила в силу для СССР 17 апреля 1991 года]. – Справочно-правовая система «КонсультантПлюс». – Текст : электронный. – URL: https://www.consultant.ru/document/cons_doc_LAW_121092/cde09a2cd0c411568920b76ce394a82dfaae5045/?ysclid=lxuq2qqqej817809125 (дата обращения: 25.06.2024).

20. Конвенция Организации Объединенных Наций против коррупции [ратифицирована Федеральным законом от 8 марта 2006 года № 40-ФЗ с заявлением, вступила в силу для Российской Федерации 8 июня 2006 года]. – Официальный интернет-портал правовой информации. – Текст : электронный. – URL: http://pravo.gov.ru/proxy/ips/?doc_itself=&nd=201035447&ysclid=lxgpiia8hs72125293#I0 (дата обращения: 16.06.2024).

21. Конвенция Организации Объединенных Наций против транснациональной организованной преступности [ратифицирована Федеральным законом от 26 апреля 2004 года № 26-ФЗ с заявлением, вступила в силу для Российской Федерации 25 июня 2004 года]. – Официальный интернет-портал правовой информации. – Текст : электронный. – URL: http://pravo.gov.ru/proxy/ips/?docbody=&link_id=1&nd=203001028&collection=1&ysclid=lxgpkk1gqy481315692 (дата обращения: 16.06.2024).

22. Международная конвенция о борьбе с финансированием терроризма [ратифицирована Федеральным законом от 10 июля 2002 года № 88-ФЗ с заявлением, вступила в силу для Российской Федерации 27 декабря 2002 года]. – Официальный интернет-портал правовой информации. – Текст : электронный. – URL: http://pravo.gov.ru/proxy/ips/?docbody=&link_id=9&nd=201017101&collection=1&ysclid=lxuqe1lczq116191906 (дата обращения: 25.06.2024).

23. Соглашение об образовании Совета руководителей подразделений финансовой разведки государств - участников Содружества Независимых Государств от 5 декабря 2012 года [вступило в силу для Российской Федерации 23 мая 2013 года]. – Официальный интернет-портал правовой информации. – Текст : электронный. – URL: http://publication.pravo.gov.ru/document/0001201306110011?index=5 (дата обращения: 04.06.2023).

24. Российская Федерация. Законы. Кодекс Российской Федерации об административных правонарушениях : Федеральный закон № 195-ФЗ [принят Государственной Думой 20 декабря 2001 года]. – Официальный интернет-портал правовой информации. – Текст : электронный. – URL: http://pravo.gov.ru/proxy/ips/?docbody&nd=102074277&ysclid=lxqchvvbxd795315734 (дата обращения: 22.06.2024).

25. Российская Федерация. Законы. Налоговый кодекс Российской Федерации (часть первая) : Федеральный закон № 146-ФЗ [принят Государственной Думой 16 июля 1998 года]. – Официальный интернет-портал правовой информации. – Текст : электронный. – URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102054722&ysclid=lxqclwaerh322367872 (дата обращения: 22.06.2024).

26. Российская Федерация. Законы. О внесении изменений в отдельные законодательные акты Российской Федерации : Федеральный закон № 222-ФЗ [принят Государственной Думой 23 июля 2024 года]. – Официальный интернет-портал правовой информации. – Текст : электронный. – URL: http://publication.pravo.gov.ru/document/0001202408080023?ysclid=lzzzly1wyt946018374 (дата обращения: 18.08.2024).

27. Российская Федерация. Законы. О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия незаконным финансовым операциям : Федеральный закон № 134-ФЗ [принят Государственной Думой 11 июня 2013 года]. – Официальный интернет-портал правовой информации. – Текст : электронный. – URL:

http://pravo.gov.ru/proxy/ips/?docbody=&nd=102166333&rdk=&intelsearch=%EE%F2+28.06.2013+%B9+134-%D4%C7) (дата обращения: 18.08.2024).

28. Российская Федерация. Законы. О внесении изменений в Федеральный закон «О национальной платежной системе» и отдельные законодательные акты Российской Федерации : Федеральный закон № 173-ФЗ [принят Государственной Думой 25 июня 2019 года]. – Официальный интернет-портал правовой информации. – Текст : электронный. – URL: http://publication.pravo.gov.ru/Document/View/0001201907030049?ysclid=lzzybry46f891200626 (дата обращения: 18.08.2024).

29. Российская Федерация. Законы. О внесении изменений в Федеральный закон «О национальной платежной системе» и Федеральный закон «О Центральном банке Российской Федерации (Банке России)» : Федеральный закон № 264-ФЗ [принят Государственной Думой 23 июля 2019 года]. – Официальный интернет-портал правовой информации. – Текст : электронный. – URL: http://publication.pravo.gov.ru/document/0001201908020042?ysclid=lzzydpbnpu295544154 (дата обращения: 18.08.2024).

30. Российская Федерация. Законы. О внесении изменений в Федеральный закон «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» в целях совершенствования обязательного контроля : Федеральный закон № 208-ФЗ [принят Государственной Думой 7 июля 2020 года]. – Официальный интернет-портал правовой информации. – Текст : электронный. – URL: http://publication.pravo.gov.ru/Document/View/0001202007130049?ysclid=lxqbsdtaie135002894 (дата обращения: 22.06.2024).

31. Российская Федерация. Законы. О внесении изменений и дополнений в законодательные акты Российской Федерации в связи с принятием Федерального закона «О противодействии легализации (отмыванию) доходов, полученных преступным путем» : Федеральный закон № 121-ФЗ [принят Государственной Думой 14 июля 2001 года]. – Официальный интернет-портал правовой информации. – Текст : электронный. – URL:

http://pravo.gov.ru/proxy/ips/?docbody=&link_id=19&nd=102072373&bpa=cd00000&bpas=cd00000&intelsearch=%F4%E7+%EE+%E2%ED%E5%F1%E5%ED%E8%E8+%E8%E7%EC%E5%ED%E5%ED%E8%E9+%E2+%F4%E7+%EE+%E3%EE%F1%F3%E4%E0%F0%F1%F2%E2%E5%ED%ED%EE%E9+%E3%F0%E0%E6%E4%E0%ED%F1%EA%EE%E9+%F1%EB%F3%E6%E1%E5++&ysclid=lxqccov1lo365324061 (дата обращения: 22.06.2024).

32. Российская Федерация. Законы. О национальной платежной системе : Федеральный закон № 161-ФЗ [принят Государственной Думой 14 июня 2011 года]. – Официальный интернет-портал правовой информации. – Текст : электронный. – URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102148779&ysclid=lzywgv7r7f723009847 (дата обращения: 18.08.2024).

33. Российская Федерация. Законы. О персональных данных : Федеральный закон № 152-ФЗ [принят Государственной Думой 8 июля 2006 года]. – Официальный интернет-портал правовой информации. – Текст : электронный. – URL: http://pravo.gov.ru/proxy/ips/?docbody&nd=102108261&ysclid=lxqcpapnul30011028 (дата обращения: 22.06.2024).

34. Российская Федерация. Законы. О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма : Федеральный закон № 115-ФЗ : [принят Государственной Думой 13 июля 2001 года]. – Официальный интернет-портал правовой информации. – Текст : электронный. – URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102072376&ysclid=lxqd5s7s2a966835775 (дата обращения: 22.06.2024).

35. Российская Федерация. Законы. О Центральном банке Российской Федерации (Банке России) : Федеральный закон № 86-ФЗ [принят Государственной Думой 27 июня 2002 года]. – Официальный интернет-портал правовой информации. – Текст : электронный. – URL:

http://pravo.gov.ru/proxy/ips/?docbody=&nd=102077052&ysclid=lxqdlubayg305635905 (дата обращения: 22.06.2024).

36. Российская Федерация. Законы. О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации : Федеральный закон № 31-ФЗ [принят Государственной Думой 22 июля 2020 года]. – Официальный интернет-портал правовой информации. – Текст : электронный. – URL: http://pravo.gov.ru/proxy/ips/?docbody=&link_id=0&nd=102801500&intelsearch=&firstDoc=1&ysclid=lxqdwoh7g584654663 (дата обращения: 22.06.2024).

37. Российская Федерация. Законы. Уголовный кодекс Российской Федерации : Федеральный закон № 63-ФЗ [принят Государственной Думой 24 мая 1996 года]. – Официальный интернет-портал правовой информации. – Текст : электронный. – URL: http://pravo.gov.ru/proxy/ips/?docbody&nd=102041891&ysclid=lxqdz07jci2848016 (дата обращения: 22.06.2024).

38. Вопросы Федеральной службы по финансовому мониторингу [Указ Президента Российской Федерации от 13 июня 2012 года № 808]. – Официальный интернет-портал правовой информации. – Текст : электронный. – URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102157200&rdk=&backlink=1 (дата обращения: 16.06.2023).

39. Об уполномоченном органе по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма [Указ Президента Российской Федерации от 01 ноября 2001 года № 1263]. – Официальный интернет-портал правовой информации. – Текст : электронный. – URL: http://pravo.gov.ru/proxy/ips/?docbody=&firstDoc=1&lastDoc=1&nd=102073273 (дата обращения: 08.06.2023).

40. О развитии искусственного интеллекта в Российской Федерации [Указ Президента Российской Федерации от 10 октября 2019 года № 490]. – Официальный интернет-портал правовой информации. – Текст : электронный. –

URL: http://publication.pravo.gov.ru/Document/View/0001201910110003?ysclid=lt1x5hmh36672681301 (дата обращения: 25.02.2024).

41. О Стратегии национальной безопасности Российской Федерации [Указ Президента РФ от 02 июля 2021 года № 400]. – Официальный интернет-портал правовой информации. – Текст : электронный. – URL: http://publication.pravo.gov.ru/Document/View/0001202107030001 (дата обращения: 30.04.2024).

42. О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы [Указ Президента Российской Федерации от 09 мая 2017 года № 203]. – Официальный интернет-портал правовой информации. – Текст : электронный. – URL: http://publication.pravo.gov.ru/Document/View/0001201705100002?ysclid=low2151hm8790599160 (дата обращения: 13.11.2023).

43. О Стратегии экономической безопасности Российской Федерации на период до 2030 года [Указ Президента РФ от 13 мая 2017 года № 208]. – Официальный интернет-портал правовой информации. – Текст : электронный. – URL: http://publication.pravo.gov.ru/Document/View/0001201705150001 (дата обращения: 30.04.2024).

44. Об утверждении Особенностей представления в Федеральную службу по финансовому мониторингу информации, предусмотренной Федеральным законом от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» [Приказ Федеральной службы по финансовому мониторингу от 8 февраля 2022 года № 18]. – Официальный интернет-портал правовой информации. – Текст : электронный. – URL: http://publication.pravo.gov.ru/document/0001202202240014 (дата обращения: 15.06.2023).

45. О требованиях к правилам внутреннего контроля кредитной организации в целях противодействия легализации (отмыванию) доходов,

полученных преступным путем, и финансированию терроризма [Положение Банка России от 2 марта 2012 года № 375-П]. – Вестник Банка России. – 2012. – № 20. – С. 30–50. – ISSN отсутствует.

46. О требованиях к правилам внутреннего контроля некредитных финансовых организаций в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма [Положение Банка России от 15 декабря 2014 года № 445-П]. – Вестник Банка России. – 2015. – № 14. – С. 22–47. – ISSN отсутствует.

47. О внесении изменений в Положение Банка России от 2 марта 2012 года № 375-П «О требованиях к правилам внутреннего контроля кредитной организации в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» [Указание Банка России от 20 октября 2020 года № 5599-У]. – Вестник Банка России. – 2021. – № 64. – С. 15–25. – ISSN отсутствует.

48. 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 путем, и финансированию терроризма» [Указание Банка России от 15 июля 2021 года № 5861-У]. – Вестник Банка России. – 2021. – № 64. – С. 38–41. – ISSN отсутствует.

49. О порядке представления некредитными финансовыми организациями в уполномоченный орган сведений и информации в соответствии со статьями 7, 7.5 Федерального закона «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» [Указание Банка России от 17 октября 2018 года № 4937-У]. – Вестник Банка России. – 2019. – № 5. – С. 22–24. – ISSN отсутствует.

Диссертации и авторефераты диссертаций

50. Капустина, Н.В. Методология управления развитием организации на основе риск-менеджмента : специальность 08.00.05 «Экономика и управление народным хозяйством» : автореферат диссертации на соискание ученой степени доктора экономических наук / Капустина Надежда Валерьевна ; Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации. – Ростов-на-Дону, 2015. – 43 с. – Библиогр.: с. 35-43. – Место защиты: Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации.

51. Кийко, М.Ю. Противодействие наркобизнесу как стратегическое направление обеспечения экономической безопасности России : специальность 08.00.05 «Экономика и управление народным хозяйством: экономическая безопасность» : диссертация на соискание ученой степени кандидата экономических наук / Кийко Михаил Юрьевич ; Институт проблем рынка Российской академии наук. – Москва, 2017. – 286 с. – Библиогр.: с. 270-282.

52. Морозов, Е.С. Совершенствование финансового мониторинга по противодействию легализации незаконных доходов : специальность 08.00.10 «Финансы, денежное обращение, кредит» : диссертация на соискание ученой степени кандидата экономических наук / Морозов Евгений Сергеевич ; Финансовая академия при Правительстве Российской Федерации. – Москва, 2010. – 208 с. – Библиогр.: с. 175-208.

53. Фильчакова, Н.Ю. Развитие инструментов финансового мониторинга в процессах легализации доходов, полученных преступным путем : специальность 08.00.10 «Финансы, денежное обращение, кредит» : диссертация на соискание ученой степени кандидата экономических наук / Фильчакова Наталья Юрьевна ; Ростовский государственный экономический университет. – Ростов-на-Дону, 2015. – 194 с. – Библиогр.: с. 173-194.

54. Чувилкин, Н.А. Совершенствование методов обеспечения экономической безопасности в организациях с учетом требований ПОД/ФТ : специальность 5.2.3 «Региональная и отраслевая экономика: экономическая безопасность» : диссертация на соискание ученой степени кандидата

экономических наук / Чувилкин Никита Александрович ; Финансовый университет при Правительстве Российской Федерации. – Москва, 2022. – 212 с. – Библиогр.: с. 131-163.

Электронные ресурсы

55. 445 компаний стали участниками налогового мониторинга в 2023 году // Федеральная налоговая служба : официальный сайт. – 2023. – Текст : электронный. – URL: https://www.nalog.gov.ru/rn77/news/activities_fts/13059125/?ysclid=lo3g8cqujx411995870 (дата обращения: 24.10.2023).

56. Абелев, О. Переоценка ценностей: итоги криптомира 2018 года / О. Абелев // Сетевое издание Forbes : [сайт]. – 2019. – Текст : электронный. – URL: https://www.forbes.ru/tehnologii/371065-pereocenka-cennostey-itogi-kriptomira-2018-goda (дата обращения: 06.06.2023).

57. Аверкиева, О. История криптовалюты в России: от суррогата до главного слова / О. Аверкиева // Futurist : [сайт]. – 2019. – Текст : электронный. – URL: https://futurist.ru/articles/1353?ysclid=lrxy3wtzqm666282601 (дата обращения: 25.02.2024).

58. Беликов, Ю. Интернет-банкинг в России: клиент всегда прав / Ю. Беликов, В. Тетерин, А. Картуесов [и др.] // banki.ru : [сайт]. – 2014. – Текст : электронный. – URL: https://www.banki.ru/news/research/?id=6686789&ysclid=lzoqrd1ggh702490104 (дата обращения: 11.08.2024).

59. Будылин, С. Криптоактивы, часть 1. Экономическая сущность и правовая природа / С. Будылин // zakon.ru : [сайт]. – 2023. – Текст : электронный. – URL: https://zakon.ru/blog/2023/05/21/kriptoaktivy_chast_1_ekonomicheskaya_suschnost_i_pravovaya_priroda?ysclid=ltvxgqghsx277659021 (дата обращения: 18.03.2024).

60. В 2022 году к налоговому мониторингу присоединится 131 компания // Федеральная налоговая служба : официальный сайт. – 2021. – Текст : электронный. – URL: https://www.nalog.gov.ru/rn77/news/activities_fts/11664927/ (дата обращения: 24.10.2023)

61. Васильева, М. Что такое блокчейн, где применяется и что его ждет в будущем / М. Васильева // banki.ru : [сайт]. – 2022. – Текст : электронный. – URL: https://www.banki.ru/news/daytheme/?id=10975614&ysclid=low165fh5263924073 (дата обращения: 13.11.2023).

62. Ветров, И. Банкам придется подвинуться: «МегаФон» и МТС отменили комиссию за денежные переводы / И. Ветров // Информационное агентство Газета.Ru : [сайт]. – 2018. – Текст : электронный. – URL: https://www.gazeta.ru/tech/2018/09/26_a_11998123.shtml?ysclid=lzyr7dpkn7337629920&updated (дата обращения: 18.08.2024).

63. В Китае зарегистрировано первое дело об отмывании денег, связанное с CBDC // Криптомайнинг-Блог : [сайт]. – 2021. – Текст : электронный. – URL: https://cryptomining-blog.ru/v-kitae-zaregistrirovano-pervoe-delo-ob-otmyvanii-deneg-svyazannoe-s-cbdc/?ysclid=lljy9aih2k907562709 (дата обращения: 01.09.2023).

64. Возможности и проблемы новых технологий в сфере ПОД/ФТ // Группа разработки финансовых мер по борьбе с отмыванием денег ФАТФ : официальный сайт. – 2021. – Текст : электронный. – URL: https://www.fatf-gafi.org/content/dam/fatf-gafi/translations/guidance/Russian-Opportunities-and-Challenges-of-New-Technologies-for-AML-CFT.pdf (дата обращения: 17.08.2023).

65. В России прошла первая сделка с токеном на палладий. Какие перспективы у рынка ЦФА и что нужно знать инвестор // banki.ru : [сайт]. – 2022. – Текст : электронный. – URL: https://www.banki.ru/news/daytheme/?id=10969592 (дата обращения: 18.03.2024).

66. В Росфинмониторинге сообщили о сокращении финансовых операций с недружественными странами // Информационное агентство ТАСС : [сайт]. – 2022. – Текст : электронный. – URL:

https://tass.ru/ekonomika/15043967?ysclid=lswel3g4iy600763501 (дата обращения: 22.02.2024).

67. Всеобщие директивы по противодействию отмыванию доходов в частном банковском секторе (Вольфсбергские принципы) // Справочно-правовая система «Электронный фонд правовой и нормативно-технической информации». – Текст : электронный. – URL: https://docs.cntd.ru/document/901934993 (дата обращения: 02.06.2023).

68. Встреча с главой Росфинмониторинга Юрием Чиханчиным // Президент России : официальный сайт. – 2023. – Текст : электронный. – URL: http://www.kremlin.ru/events/president/transcripts/deliberations/70655 (дата обращения: 17.06.2023).

69. Встреча с директором Федеральной службы по финансовому мониторингу Юрием Чиханчиным // Президент России : официальный сайт. – 2021. – Текст : электронный. – URL: http://www.kremlin.ru/events/president/news/65036 (дата обращения: 17.06.2023).

70. Встреча с директором Федеральной службы по финансовому мониторингу Юрием Чиханчиным // Информационное агентство ТАСС : [сайт]. – 2021. – Текст : электронный. – URL: http://www.kremlin.ru/events/president/transcripts/deliberations/67034 (дата обращения: 25.02.2024).

71. ВТБ обезопасит банковские карты с помощью искусственного интеллекта // Информационное агентство РИА Новости : [сайт]. – 2021. – Текст : электронный. – URL: https://ria.ru/20210218/kiberbezopasnost-1597984923.html (дата обращения: 24.06.2023).

72. Гапонько, Е.А. Искусственный интеллект в России / Е.А. Гапонько // Образовательный портал «Справочник» : [сайт]. – 2019. – Текст : электронный. – URL: https://spravochnick.ru/informatika/ponyatie_iskusstvennogo_intellekta/iskusstvennyy_intellekt_v_rossii/ (дата обращения: 25.02.2024).

73. Глава ФСКН предложил использовать ресурсы G8 в борьбе с наркобизнесом // Информационное агентство РИА Новости : [сайт]. – 2014. – Текст : электронный. – URL: https://ria.ru/20140225/996984344.html (дата обращения: 25.02.2024).

74. Годовой отчет 2011 // Банк России : официальный сайт. – 2012. – Текст : электронный. – URL: https://cbr.ru/Collection/Collection/File/7802/ar_2011.pdf (дата обращения: 18.09.2024).

75. Годовой отчет 2012 // Банк России : официальный сайт. – 2013. – Текст : электронный. – URL: https://cbr.ru/Collection/Collection/File/7801/ar_2012.pdf (дата обращения: 18.09.2024);

76. Годовой отчет 2013 // Банк России : официальный сайт. – 2014. – Текст : электронный. – URL: https://cbr.ru/Collection/Collection/File/7800/ar_2013.pdf (дата обращения: 18.09.2024).

77. Годовой отчет 2015 // Банк России : официальный сайт. – 2016. – Текст : электронный. – URL: https://cbr.ru/Collection/Collection/File/7798/ar_2015.pdf (дата обращения: 25.10.2023).

78. Годовой отчет 2016 // Банк России : официальный сайт. – 2017. – Текст : электронный. – URL: https://cbr.ru/Collection/Collection/File/7797/ar_2016.pdf (дата обращения: 25.10.2023).

79. Годовой отчет 2017 // Банк России : официальный сайт. – 2018. – Текст : электронный. – URL: https://cbr.ru/Collection/Collection/File/7796/ar_2017.pdf (дата обращения: 25.10.2023).

80. Годовой отчет 2018 // Банк России : официальный сайт. – 2020. – Текст : электронный. – URL: https://cbr.ru/Collection/Collection/File/19699/ar_2018.pdf (дата обращения: 25.10.2023).

81. Годовой отчет 2019 // Банк России : официальный сайт. – 2020. – Текст : электронный. – URL: https://cbr.ru/Collection/Collection/File/27873/ar_2019.pdf (дата обращения: 25.10.2023).

82. Годовой отчет 2020 // Банк России : официальный сайт. – 2021. – Текст : электронный. – URL: https://cbr.ru/Collection/Collection/File/32268/ar_2020.pdf (дата обращения: 25.10.2023).

83. Годовой отчет 2021 // Банк России : официальный сайт. – 2022. – Текст : электронный. – URL: https://cbr.ru/Collection/Collection/File/40915/ar_2021.pdf (дата обращения: 25.10.2023).

84. Годовой отчет 2022 // Банк России : официальный сайт. – 2023. – Текст : электронный. – URL: https://cbr.ru/Collection/Collection/File/43872/ar_2022.pdf (дата обращения: 25.10.2023).

85. Годовой отчет Банка России за 2014 // Банк России : официальный сайт. – 2015. – Текст : электронный. – URL: https://cbr.ru/Collection/Collection/File/7799/ar_2014.pdf (дата обращения: 18.09.2024).

86. Госдума может принять документ о регулировании криптовалют в весеннюю сессию // Информационное агентство ТАСС : [сайт]. – 2022. – Текст : электронный. – URL: https://tass.ru/ekonomika/13505469?ysclid=ltxes6ni30235803773 (дата обращения: 18.03.2024).

87. Добрунов, М. Три крупнейших китайских банка перестали принимать платежи из России / М. Добрунов // Информационное агентство РБК : [сайт]. – 2024. – Текст : электронный. – URL: https://www.rbc.ru/business/21/02/2024/65d554ea9a794755d27d8fe4?ysclid=lswejz11s0790254556 (дата обращения: 22.02.2024).

88. Дульнева, М. Контроль за населением и независимость от доллара: зачем Китай создает свою цифровую валюту / М. Дульнева // Сетевое издание Forbes : [сайт]. – 2021. –Текст : электронный. – URL: https://www.forbes.ru/finansy-i-investicii/426079-kontrol-za-naseleniem-i-nezavisimost-ot-dollara-zachem-kitay-sozdaet?ysclid=llzr0aiti1781622579 (дата обращения: 01.09.2023).

89. Дяченко, О. Давать взятки будет сложнее, а отслеживать траты – проще: эксперт о цифровом рубле / О. Дяченко // Информационное агентство

РИАМО : [сайт]. – 2022. – Текст : электронный. – URL: https://riamo.ru/article/608310/davat-vzyatki-budet-slozhnee-a-otslezhivat-traty-prosche-ekspert-o-tsifrovom-ruble?ysclid=ln296rtlfr540850860 (дата обращения: 27.09.2023).

90. Еленцева, Л. Электронный документооборот в России / Л. Еленцева // КонтурДиадок : [сайт]. – Текст : электронный. – URL: https://www.diadoc.ru/articles/21931-edo_v_rossii?ysclid=lrxy2xnkoo970008168 (дата обращения: 25.02.2024).

91. Житкова, В. Слежка на миллион: как заработать на распознавании лиц клиентов / В. Житкова // Информационное агентство РБК : [сайт]. – 2015. – Текст : электронный. – URL: https://www.rbc.ru/ins/own_business/16/12/2015/567161229a79477425e22eda (дата обращения: 25.02.2024).

92. Зампред Сбербанка Анатолий Попов: безопасность средств обеспечивают и банк, и клиент // Информационное агентство ТАСС : [сайт]. – 2019. – Текст : электронный. – URL: https://tass.ru/interviews/6574591 (дата обращения: 24.06.2023).

93. Заруцкая, Н. ЦБ будет сам следить за рисками отмывания доходов в цифровых рублях / Н. Заруцкая // Деловая газета Ведомости : [сайт]. – 2023. – Текст : электронный. – URL: https://www.vedomosti.ru/finance/articles/2023/05/22/976115-tsb-budet-sledit-za-riskami-otmivaniya-dohodov-v-tsifrovih-rublyah?ysclid=ln2ca37kdi496368004 (дата обращения: 27.09.2023).

94. Измалков, С.Б. Теория экономических механизмов / С.Б. Измалков, К.И. Сонин, М.М. Юдкевич // Экономический портал : [сайт]. – Текст : электронный. – URL: https://institutiones.com/theories/259--2007-1.html (дата обращения: 10.10.2023).

95. Интернет-банкинг и оценка эффективности его применения российскими коммерческими банками // Образовательный портал «Справочник» : [сайт]. – 2024. – Текст : электронный. – URL: https://spravochnick.ru/bankovskoe_delo/internet-

banking_i_ocenka_effektivnosti_ego_primeneniya_rossiyskimi_kommercheskimi_bankami/ (дата обращения: 11.08.2024).

96. Информационное письмо Банка России от 21 февраля 2005 года № 7 «Обобщение практики применения Федерального закона «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» // Справочно-правовая система «Консультант Плюс». – Текст : электронный. – URL: https://www.consultant.ru/document/cons_doc_LAW_52053/#dst100024 (дата обращения: 11.10.2023).

97. Информация Банка России от 5 марта 2019 года «Порядок составления некредитными финансовыми организациями в электронной форме информации, предусмотренной статьями 7, 7.5 Федерального закона «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» // Справочно-правовая система «Гарант». – 2019. – Текст : электронный. – URL: https://www.garant.ru/products/ipo/prime/doc/72088966/ (дата обращения: 15.06.2023).

98. Инфраструктура точек доступа к финансовым услугам на территории России в условиях развития дистанционных каналов обслуживания // Банк России : официальный сайт. – 2022. – Текст : электронный. – URL: https://cbr.ru/Content/Document/File/135131/fin_uslugi_2021.pdf (дата обращения: 20.08.2023).

99. Искусственный интеллект помог Сбербанку РФ выявить новую схему хищения денег из банкоматов // Digital.Report : [сайт]. – 2017. – Текст : электронный. – URL: https://digital.report/iskusstvennyiy-intellekt-pomog-sberbanku-rf-vyiyavit-novuyu-shemu-hishheniya-deneg-iz-bankomatov/ (дата обращения: 24.06.2023).

100. История Росфинмониторинга // Федеральная служба по финансовому мониторингу : официальный сайт. – Текст : электронный. – URL: https://www.fedsfm.ru/about/history (дата обращения: 07.06.2023).

101. Итоги проекта на тему «Легализация (отмывание) преступных доходов от киберпреступлений, а также финансирование терроризма за счет указанной преступной деятельности, в том числе с использованием электронных денег или виртуальных активов и инфраструктуры их провайдеров» // Евразийская группа по противодействию легализации преступных доходов и финансированию терроризма ЕАГ : официальный сайт. – Текст : электронный. – URL: https://eurasiangroup.org/files/uploads/files/other_docs/WGTYP_(2022)_12_rev_1_rus.pdf (дата обращения: 19.08.2024).

102. Итоги работы Банка России 2022: коротко о главном // Банк России : официальный сайт. – 2023. – Текст : электронный. – URL: https://cbr.ru/about_br/publ/results_work/2022/razvitie-sistemy-platezhey-i-raschetov/ (дата обращения: 30.04.2024).

103. Кавеева, А. Аналитический центр НАФИ. Использование цифровых банковских сервисов в России в 2023 году / А. Кавеева // ICT.Moscow : [сайт]. – 2023. – Текст : электронный. – URL: https://ict.moscow/research/ispolzovanie-tsifrovykh-bankovskikh-servisov-v-rossii-v-2023-godu/ (дата обращения: 11.08.2024)

104. Как все начиналось. История криптовалюты // vc.ru : [сайт]. – 2023. – Текст : электронный. – URL: https://vc.ru/crypto/625801-kak-vse-nachinalos-istoriya-kriptovalyuty?ysclid=lt1q6yx8cj126855216 (дата обращения: 25.02.2024).

105. Киреева, В. Глава Росфинмониторинга рассказал о применении ИИ в работе / В. Киреева // Издание Федерального собрания Российской Федерации «Парламентская газета» : официальный сайт. – Текст : электронный. – URL: https://www.pnp.ru/social/glava-rosfinmonitoringa-rasskazal-o-primenenii-ii-v-rabote.html (дата обращения: 18.08.2024).

106. Концепция развития национальной системы противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (утв. Президентом РФ 30 мая 2018 г.) // Справочно-правовая система «Гарант». – 2018. – Текст : электронный. – URL: https://www.garant.ru/products/ipo/prime/doc/71858442/ (дата обращения 26.11.2021).

107. Козлова, К. Обзор существующих AML-систем с точки зрения новой Стратегии цифровой экономики в России / К. Козлова, П. Качурина // Экспертный союз : [сайт]. – 2021. – Текст : электронный. – URL: http://unionexpert.su/obzor-i-izuchenie-sushhestvuyushhih-aml-sistem-s-tochki-zreniya-novoj-strategii-tsifrovoj-ekonomiki-v-rossii/ (дата обращения: 17.06.2023).

108. Костерева, М. FATF приостановила участие России в организации, но ожидает продолжения членских выплат / М. Костерева // Деловая газета Коммерсант : [сайт]. – 2023. – Текст : электронный. – URL: https://www.kommersant.ru/doc/5841890 (дата обращения: 09.06.2023).

109. Крецу, К. Хронология: как развивалась биометрия / К. Крецу // vc.ru : [сайт]. – 2018. – Текст : электронный. – URL: https://vc.ru/future/32006-hronologiya-kak-razvivalas-biometriya?ysclid=lt0oba5js7773423729 (дата обращения: 25.02.2024).

110. Криптовалюты: тренды, риски, меры // Банк России : официальный сайт. – 2022. – Текст : электронный. – URL: https://cbr.ru/Content/Document/File/132241/Consultation_Paper_20012022.pdf (дата обращения: 20.06.2023).

111. Крылова, А. Мобильные платежи Все только начинается / А. Крылова // ИКС Медиа : [сайт]. – 2008. – Текст : электронный. – URL: https://www.iksmedia.ru/articles/1447887-Mobilnye-platezhi-Vse-tolko-nachina.html (дата обращения: 18.08.2024).

112. Куликова, К. Надзор криптчал / К. Куликова, Н. Королев // Деловая газета Коммерсант : [сайт]. – 2023. – Текст : электронный. – URL: https://www.kommersant.ru/doc/5774896 (дата обращения: 17.06.2023).

113. Кутырев, И. Зачем сотовые операторы выпускают банковские карты / И. Кутырев // Информационное агентство «Амурская правда» : [сайт]. – 2016. – Текст : электронный. – URL: https://ampravda.ru/2016/12/28/071930.html?ysclid=lzyrgqq8h2720111924 (дата обращения: 18.08.2024).

114. Лазарева, Ю.А. NFT: проблема определения правовой природы и перспективы законодательства / Ю.А. Лазарева // Интернет-сайт журнала Суда по

интеллектуальным правам : [сайт]. – ISSN 2313-4852. – Текст : электронный. – URL: http://ipcmagazine.ru/re-views/nft-the-problem-of-determining-the-legal-nature-and-prospects-of-legislation?ysclid=ltvujyblvc933342072 (дата обращения: 18.03.2024).

115. Легализация (отмывание) преступных доходов от киберпреступлений, а также финансирование терроризма за счет указанной преступной деятельности, в том числе с использованием электронных денег или виртуальных активов и инфраструктуры их провайдеров // Евразийская группа по противодействию легализации преступных доходов и финансированию терроризма ЕАГ : официальный сайт. – 2022. – Текст : электронный. – URL: https://eurasiangroup.org/files/uploads/files/other_docs/WGTYP_(2022)_12_rev_1_rus.pdf (дата обращения: 20.06.2023).

116. Лентяев, Д. Blockchain биометрия: здравствуй, безопасность! / Д. Лентяев // forknews : [сайт]. – 2018. – Текст : электронный. – URL: https://forknews.io/security/000205-blockchain-biometriya-pri.html?lang=ru (дата обращения: 20.08.2023).

117. Лимончикова, Е. Первая криптовалютная биржа и нынешняя крупнейшая биржа / Е. Лимончикова // freedman club : [сайт]. – 2021. – Текст : электронный. – URL: https://freedmanclub.com/pervaja-kriptovaljutnaja-birzha-i-nyneshnjaja-krupnejshaja-birzha-bitcointalk-mt-gox-bitcoinmarket/?ysclid=lt1s6ly8us75018305 (дата обращения: 25.02.2024).

118. Лузгин, А. Майнинг, кадры и законы. Каковы масштабы российского рынка криптовалют / А. Лузгин // Информационное агентство РБК : [сайт]. – Текст : электронный. – URL: https://www.rbc.ru/crypto/news/6486f59f9a7947490d1c7b54 (дата обращения: 20.10.2023).

119. Мастерчейн (Masterchain). Российская национальная блокчейн-сеть // TAdviser : [сайт]. – Текст : электронный. – URL: https://www.tadviser.ru/index.php/Продукт:Мастерчейн_(Masterchain)_Российская_национальная_блокчейн-сеть?ysclid=lt1ywnq6hi360458209 (дата обращения: 25.02.2024).

120. Международные стандарты по противодействию отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения. Рекомендации ФАТФ // Банк России : официальный сайт. – Текст : электронный. – URL: https://cbr.ru/Content/Document/File/132941/St10-21_RU.PDF (дата обращения: 05.06.2023).

121. Методология оценки технического соответствия рекомендациям ФАТФ и эффективности систем ПОД/ФТ // Группа разработки финансовых мер по борьбе с отмыванием денег ФАТФ : официальный сайт. – Текст : электронный. – URL: https://www.fatf-gafi.org/content/dam/fatf-gafi/translations/Methodology/MUMCFM-Russsian-Methodology.pdf (дата обращения: 06.06.2013).

122. Механизм. Современная энциклопедия // Академик : [сайт]. – Текст : электронный. – URL: https://dic.academic.ru/dic.nsf/enc1p/29994 (дата обращения: 11.12.2022).

123. Мигунов, Д. Чем грозит попадание России в черный список FATF - международной организации по борьбе с отмыванием капитала / Д. Мигунов // Газета Известия : [сайт]. – 2023. – Текст : электронный. – URL: https://iz.ru/1517951/dmitrii-migunov/avtomoika-chem-grozit-ekonomike-popadanie-rossii-v-chernyi-spisok-fatf (дата обращения: 29.05.2023).

124. Мингазов, С. Российский бизнес втрое снизил интерес к блокчейновым технологиям / С. Мингазов // Сетевое издание Forbes : [сайт]. – 2021. – Текст : электронный. – URL: https://www.forbes.ru/newsroom/tehnologii/424349-rossiyskiy-biznes-vtroe-snizil-interes-k-blokcheynovym-tehnologiyam?ysclid=lt1y7uu35j936361592 (дата обращения: 25.02.2024).

125. Минфин России предложил снизить пороговые требования для участников налогового мониторинга // Информационное агентство ТАСС : [сайт]. – 2023. – Текст : электронный. – URL: https://tass.ru/ekonomika/18534577?ysclid=lo3gefazk2842452118 (дата обращения: 24.10.2023).

126. Минфин США предупредил об использовании NFT для отмывания денег // Деловая газета РБК : [сайт]. – 2022. – Текст : электронный. – URL: https://www.rbc.ru/crypto/news/6200cbbd9a794767aefe9512 (дата обращения: 25.06.2023).

127. Мошенничество с deepfake: темная сторона искусственного интеллекта // Securitylab.ru : [сайт]. – 2019. – Текст : электронный. – URL: https://www.securitylab.ru/blog/company/PandaSecurityRus/347085.php?ysclid=lljvjin3d2574564267 (дата обращения: 20.08.2023).

128. На бирже Binance начались торги криптовалютой с биометрической идентификацией Worldcoin // Информационное агентство ТАСС : [сайт]. – 2023. – Текст : электронный. – URL: https://tass.ru/ekonomika/18346585?ysclid=lljpol7b83924194811 (дата обращения: 20.08.2023).

129. Навигация в мире платежей // Ассоциация банков России : официальный сайт. – 2021. – Текст : электронный. – URL: https://asros.ru/upload/iblock/26e/q3lvx8gukhlkiby9mu1p9kugvxok2rus/pwc_future_of_payments.pdf (дата обращения: 22.06.2023).

130. На заседании Совета глав государств СНГ подписано соглашение об образовании Международного центра оценки рисков // Федеральная служба по финансовому мониторингу : официальный сайт. – Текст : электронный. – URL: https://fedsfm.ru/releases/6986 (дата обращения: 10.03.2024).

131. Национальная оценка рисков легализации (отмывания) доходов, полученных преступным путем (Публичный отчет) – 2022 // Федеральная служба по финансовому мониторингу : официальный сайт. – 2022. – Текст : электронный. – URL: https://fedsfm.ru/content/files/отчеты%20нор/нор-од-2022-6.pdf (дата обращения: 20.06.2023).

132. Национальная оценка рисков финансирования терроризма (Публичный отчет) – 2022 // Федеральная служба по финансовому мониторингу : официальный сайт. – 2022. – Текст : электронный. – URL:

https://www.fedsfm.ru/content/files/отчеты%20нор/национальная%20оценка%20рисков-фт.pdf (дата обращения: 20.06.2023).

133. Новый алгоритм Яндекса «Королёв» — искусственный интеллект в поисках смысла // Технологии успеха : [сайт]. – 2017. – Текст : электронный. – URL: https://webtu.ru/blog/novyj-algoritm-yandeksa-korolyov/ (дата обращения: 25.02.2024).

134. Обзор результатов обобщения и анализа правоприменительной практики контрольной (надзорной) деятельности Федеральной службы по финансовому мониторингу за 2022 год // Федеральная служба по финансовому мониторингу : официальный сайт. – 2023. – Текст : электронный. – URL: https://www.fedsfm.ru/content/files/надзор/прил1_обзор%20ппп%20за%202022%20год%20итог_2.0%201.doc (дата обращения: 27.10.2023).

135. Обновленное руководство по применению риск-ориентированного подхода «Виртуальные активы и провайдеры услуг в сфере виртуальных активов» // Евразийская группа по противодействию легализации преступных доходов и финансированию терроризма ЕАГ : официальный сайт. – Текст : электронный. – URL: https://eurasiangroup.org/files/uploads/files/06.Updated-Guidance-VA-VASP_rus.pdf (дата обращения: 19.08.2024).

136. О ЕАГ // Евразийская группа по противодействию легализации преступных доходов и финансированию терроризма ЕАГ : официальный сайт. – Текст : электронный. – URL: https://eurasiangroup.org/ru/about-eag (дата обращения: 03.06.2023).

137. Описание структур наименования, служебной и информационной частей ФЭС, описание кодов признаков, указывающих на необычный характер операций (сделок), и требования к технологическим электронным документам, направление которых регламентировано особенностями представления в Федеральную службу по финансовому мониторингу информации, предусмотренной Федеральным законом от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», утвержденными приказом Федеральной

службы по финансовому мониторингу от 8 февраля 2022 г. № 18 // Федеральная служба по финансовому мониторингу : официальный сайт. – 2022. – Текст : электронный. – URL: https://fedsfm.ru/documents/rfm/5846 (дата обращения: 15.06.2023).

138. Отработка по процедурам дистанционного надзора ЦБ // Агентство «ФКД Консалт» : [сайт]. – Текст : электронный. – URL: https://fkdconsult.ru/otrabotka-po-proczeduram-distanczionnogo-nadzora-czb?ysclid=lo4y17xrqz461109877 (дата обращения: 25.10.2023).

139. Отчет о работе Росфинмониторинга 2020 // Федеральная служба по финансовому мониторингу : официальный сайт. – 2021. – Текст : электронный. – URL: https://fedsfm.ru/content/files/documents/2021/отчет%202020.pdf (дата обращения: 25.02.2024).

140. Отчет о работе Росфинмониторинга 2022 // Федеральная служба по финансовому мониторингу : официальный сайт. – 2023. – Текст : электронный. – URL: https://fedsfm.ru/content/files/публичный%20отчет%20рфм%202022.pdf (дата обращения: 12.10.2023).

141. Отчет ФАТФ «Виртуальные валюты. Ключевые определения и потенциальные риски в сфере ПОД/ФТ» // Евразийская группа по противодействию легализации преступных доходов и финансированию терроризма ЕАГ : официальный сайт. – Текст : электронный. – URL: https://eurasiangroup.org/files/FATF_docs/Virtualnye_valyuty_FATF_2014.pdf (дата обращения: 19.08.2024).

142. Партнер «Крок» разработает блокчейн-прототип для Внешэкономбанка // TAdviser : [сайт]. – Текст : электронный. – URL: https://www.tadviser.ru/index.php/Проект:Внешэкономбанк_%28ВЭБ%29_%28блокчейн%2C_цифровой_контракт%29?ysclid=lt1ylpqos316325759 (дата обращения: 25.02.2024).

143. Письмо Банка России от 15 февраля 2001 года № 24-Т «О Вольфсбергских принципах» (вместе со «Всеобщими директивами по противодействию отмыванию доходов в частном банковском секторе

(Вольфсбергскими принципами)» от 30 октября 2000 года) // Справочно-правовая система «Консультант Плюс». – Текст : электронный. – URL: https://www.consultant.ru/document/cons_doc_LAW_30425/ (дата обращения: 22.06.2024).

144. Письмо Банка России от 27 апреля 2007 г. № 60-Т «Об особенностях обслуживания кредитными организациями клиентов с использованием технологии дистанционного доступа к банковскому счету клиента (включая интернет-банкинг)» // Справочно-правовая система «Гарант». – Текст : электронный. – URL: https://base.garant.ru/12153297/ (дата обращения: 11.08.2024).

145. Письмо Федеральной службы по финансовому мониторингу от 6 марта 2020 года № 01-01-33/4641 «О рассмотрении предложений по совершенствованию законодательства о ПОД/ФТ» // Справочно-правовая система «Гарант». – 2020. – Текст : электронный. – URL: https://www.garant.ru/products/ipo/prime/doc/73665789/ (дата обращения: 13.06.2023).

146. Письмо ЦБР от 31 марта 2008 года № 36-Т «О Рекомендациях по организации управления рисками, возникающими при осуществлении кредитными организациями операций с применением систем интернет-банкинга» // Справочно-правовая система «Гарант». – Текст : электронный. – URL: https://www.garant.ru/products/ipo/prime/doc/488238/?ysclid=lzohxckgl6953180939 (дата обращения: 11.08.2024).

147. Платформа «Знай своего клиента» // Банк России : официальный сайт. – Текст : электронный. – URL: https://cbr.ru/counteraction_m_ter/platform_zsk/ (дата обращения: 16.06.2023).

148. Потресов, С. Билайн: Развитие мобильных платежей / С. Потресов // Mobile-review.com : [сайт]. – 2008. – Текст : электронный. – URL: https://mobile-review.com/articles/2008/bee-mobipayment.shtml (дата обращения: 17.08.2024).

149. Правила составления кредитными организациями в электронной форме сведений и информации, предусмотренных статьями 7, 7.5 Федерального закона «О противодействии легализации (отмыванию) доходов, полученных преступным

путем, и финансированию терроризма» // Справочно-правовая система «Гарант». – 2020. – Текст : электронный. – URL: https://www.garant.ru/products/ipo/prime/doc/74829852/ (дата обращения: 15.06.2023).

150. Приложение 1. Перечень компонентов, входящих в состав ЕИС Росфинмониторинга // Справочно-правовая система «Гарант». – Текст : электронный. – URL: https://base.garant.ru/71944086/d8e34e7b9274ff56b4ab44c1bd6398fb/ (дата обращения: 16.06.2023).

151. Провайдеры криптовалют должны регистрироваться в РФ и передавать данные правоохранителям // Информационное агентство ТАСС : [сайт]. – 2023. – Текст : электронный. – URL: https://tass.ru/obschestvo/17457017?ysclid=lmhs1dkieg839273807 (дата обращения: 29.09.2023).

152. Проведена оценка эффективности налогового мониторинга за 2021 год // Федеральная налоговая служба : официальный сайт. – 2022. – Текст : электронный. – URL: https://www.nalog.gov.ru/rn77/news/activities_fts/12956039/?ysclid=lo3g7j7jlt246637545 (дата обращения: 24.10.2023).

153. Противодействие отмыванию денег и валютный контроль // Банк России : официальный сайт. – Текст : электронный. – URL: https://cbr.ru/counteraction_m_ter/ (дата обращения: 21.06.2023).

154. Пятин, А. Финразведка решила следить за сделками с биткоином с помощью искусственного интеллекта / А. Пятин // Сетевое издание Forbes : [сайт]. – 2020. – Текст : электронный. – URL: https://www.forbes.ru/newsroom/tehnologii/406797-finrazvedka-reshila-sledit-za-sdelkami-s-bitkoinom-s-pomoshchyu (дата обращения: 17.06.2023).

155. Резолюция 1267 (1999), принятая Советом Безопасности на его 4051-м заседании 15 октября 1999 года // Official Documents System of the United Nations = Система официальной документации Организации Объединенных Наций :

официальный сайт. – Текст : электронный. – URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/300/46/PDF/N9930046.pdf?OpenElement (дата обращения: 01.06.2023).

156. Резолюция 1373 (2001), принятая Советом Безопасности на его 4385-м заседании 28 сентября 2001 года // Official Documents System of the United Nations = Система официальной документации Организации Объединенных Наций : официальный сайт. – Текст : электронный. – URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N01/557/45/PDF/N0155745.pdf?OpenElement (дата обращения: 01.06.2023).

157. Росбанк автоматизировал процессы противодействия отмыванию доходов // Директор информационной службы : [сайт]. – 2021. – Текст : электронный. – URL: https://cio.osp.ru/news/160221-Rosbank-avtomatizirovalprotsessy-protivodeystviya-otmyvaniyu-dohodov (дата обращения: 23.06.2023).

158. Росфинмониторинг запускает онлайн-сервис для борьбы с отмыванием денег // Информационное агентство ТАСС : [сайт]. – 2021. – Текст : электронный. – URL: https://tass.ru/ekonomika/10741467 (дата обращения: 18.08.2024).

159. Росфинмониторинг запустил «Личный кабинет» для подотчетных организаций и лиц // Федеральная служба по финансовому мониторингу : официальный сайт. – Текст : электронный. – URL: https://www.fedsfm.ru/releases/373 (дата обращения: 18.08.2024).

160. Росфинмониторинг получил от банков первые сообщения о подозрительной деятельности // Информационное агентство ТАСС : [сайт]. – 2022. – Текст : электронный. – URL: https://tass.ru/ekonomika/14287425 (дата обращения: 13.06.2023).

161. Росфинмониторинг предложил включить НСПК в антиотмывочное регулирование // Информационное агентство РИА Новости : [сайт]. – 2024. – Текст : электронный. – URL: https://ria.ru/20240514/nspk-1945812910.html?ysclid=lzovw8bqn9601807053 (дата обращения: 11.08.2024).

162. Росфинмониторинг фиксирует факты финансирования терроризма с использованием криптовалют // Информационное агентство ТАСС : [сайт]. – 2021.

– Текст : электронный. – URL: https://tass.ru/ekonomika/10978989 (дата обращения: 20.06.2023).

163. Руководство по применению риск-ориентированного подхода «Виртуальные активы и провайдеры услуг в сфере виртуальных активов» // Банк России : официальный сайт. – Текст : электронный. – URL: https://cbr.ru/content/document/file/113302/Руководство_РОП_ВА_ПУВА.pdf (дата обращения: 23.08.2024).

164. Руководство по применению риск-ориентированного подхода «Предоплаченные карты, мобильные платежи и онлайн-платежи» // Банк России : официальный сайт. – Текст : электронный. – URL: https://cbr.ru/Content/Document/File/156353/RBA-mobile-internet-payments.pdf (дата обращения: 19.08.2024).

165. Самсонова, А. Банки распробовали ИИ / А. Самсонова // Comnews : [сайт]. – 2019. – Текст : электронный. – URL: https://www.comnews.ru/content/118518/2019-03-18/banki-rasprobovali-ii (дата обращения: 25.06.2023).

166. СБП: основные показатели // Банк России : официальный сайт. – Текст : электронный. – URL: https://cbr.ru/analytics/nps/sbp/2_2024/ (дата обращения: 17.08.2024).

167. Система быстрых платежей ЦБ усилила требования к защите переводов // Информационное агентство РБК : [сайт]. – 2021. – Текст : электронный. – URL: https://www.rbc.ru/finances/03/01/2021/5fe48dd69a79477174009450 (дата обращения: 11.08.2024).

168. Системы дистанционного банковского обслуживания (рынок ДБО России) // TAdviser : [сайт]. – 2022. – Текст : электронный. – URL: https://www.tadviser.ru/index.php/Статья:ДБО_-_Системы_дистанционного_банковского_обслуживания_(рынок_России)#2009:_1.2C5_.D0.BC.D0.BB.D0.BD_.D0.BA.D0.BB.D0.B8.D0.B5.D0.BD.D1.82.D0.BE.D0.B2_.D0.94.D0.91.D0.9E_.D0.B8.D0.BB.D0.B8_1.25_.D0.BE.D1.82_.D0.BD.D0.B0.D1.81.D0.B5.D0.BB.D0.B5.D0.BD.D0.B8.D1.8F (дата обращения: 11.08.2024).

169. Смирнова, И. Единая система идентификации и аутентификации в Российской Федерации / И. Смирнова // Образовательный портал «Справочник» : [сайт]. – Текст : электронный. – URL https://spravochnick.ru/gosudarstvennoe_i_municipalnoe_upravlenie/edinaya_sistema_identifikacii_i_autentifikacii_v_rossiyskoy_federacii/ (дата обращения: 25.02.2024).

170. Смирнова, С. Закатают в «пластик»: Россия выходит вперед по темпам роста карточных платежей / С. Смирнова // Газета Известия : [сайт]. – 2021. – Текст : электронный. – URL: https://iz.ru/1234861/sofia-smirnova/zakataiut-v-plastik-rossiia-vykhodit-vpered-po-tempam-rosta-kartochnykh-platezhei (дата обращения: 22.06.2023).

171. Спиридонов, А. Различия в ИТ-оснащении министерств и ведомств приводят к невозможности организации информационного взаимодействия на современном техническом уровне / А. Спиридонов // CNews : [сайт]. – 2009. – Текст : электронный. – URL: https://ucaas.cnews.ru/reviews/free/gov2009/int/fin_m/index.shtml?ysclid=lt0nrl8yc1171000226 (дата обращения: 25.02.2024).

172. Среднее время подтверждения // Blockchain.com : [сайт]. – Текст : электронный. – URL: https://www.blockchain.com/explorer/charts/avg-confirmation-time (дата обращения: 23.06.2023).

173. СРПФР // Федеральная служба по финансовому мониторингу : официальный сайт. – Текст : электронный. – URL: https://www.fedsfm.ru/activity/crpfr (дата обращения: 03.06.2023).

174. СРПФР // Федеральная служба по финансовому мониторингу : официальный сайт. – Текст : электронный. – URL: https://www.fedsfm.ru/fm/srpfr (дата обращения: 17.06.2023).

175. Статистика проверок // Федеральная служба по финансовому мониторингу : официальный сайт. – Текст : электронный. – URL: https://www.fedsfm.ru/activity/supervisory-results?index=2 (дата обращения: 27.10.2023).

176. Стратегия партнерства государств и бизнеса в противодействии терроризму // Организация Объединенных Наций : официальный сайт. – Текст : электронный. – URL: https://www.un.org/ru/documents/decl_conv/declarations/partnerships_strategy.shtml (дата обращения: 23.04.2024).

177. Судебная статистика // Судебный департамент при Верховном Суде Российской Федерации : официальный сайт. – Текст : электронный. – URL: http://cdep.ru/?id=79 (дата обращения: 28.10.2023).

178. Технологии искусственного интеллекта и машинного обучения // Центр развития компетенций в бизнес-информатике, логистике и управлении проектами Высшей школы бизнеса НИУ ВШЭ : [сайт]. – 2021. – Текст : электронный. – URL: https://hsbi.hse.ru/articles/tekhnologii-iskusstvennogo-intellekta-i-mashinnogo-obucheniya/?ysclid=low196u08x231722270 (дата обращения: 13.11.2023).

179. ТОП-10 лучших биткоин-миксеров // Информационное агентство РБК : [сайт]. – 2022. – Текст : электронный. – URL: https://ekb.plus.rbc.ru/partners/61f419a67a8aa91ef75094df (дата обращения: 20.06.2023).

180. Узбекова, А. Цифровой рубль повысит прозрачность расходования бюджетных средств / А. Узбекова // Российская газета : [сайт]. – 2022. – Текст : электронный. – URL: https://rg.ru/2022/10/09/cifrovoj-rubl-povysit-prozrachnost-rashodovaniia-biudzhetnyh-sredstv.html?ysclid=ln294pjwte432367866 (дата обращения: 27.09.2023).

181. Цифровизация экономики в России // Центр развития компетенций в бизнес-информатике, логистике и управлении проектами Высшей школы бизнеса НИУ ВШЭ : [сайт]. – 2021. – Текст : электронный. – URL: https://hsbi.hse.ru/articles/tsifrovizatsiya-ekonomiki-v-rossii/?ysclid=lovpek07h7760605938 (дата обращения: 13.11.2023).

182. Цифровой рубль // Банк России : официальный сайт. – 2023. – Текст : электронный. – URL: https://cbr.ru/fintech/dr/ (дата обращения: 25.09.2023).

183. Цифровой рубль: старт тестирования // Банк России : официальный сайт. – 2022. – Текст : электронный. – URL: https://cbr.ru/press/event/?id=12685 (дата обращения: 25.09.2023).

184. Чемоданова, К. Перегнали Европу: россияне променяли наличные на «пластик» / К. Чемоданова // Газета.ru : [сайт]. – 2019. – Текст : электронный. – URL: https://www.gazeta.ru/business/2019/10/03/12726973.shtml?updated (дата обращения: 22.06.2023).

185. Ченг, К. Бот с Уолл-стрит. Что такое алгоритмическая торговля криптовалютами / К. Ченг // Информационное агентство РБК : [сайт]. – 2018. – Текст : электронный. – URL: https://www.rbc.ru/crypto/news/5bbc7b679a79474e8a81e267 (дата обращения: 25.06.2023).

186. Через год в России заработает ИТ-система финансовой разведки // CNews : [сайт]. – 2021. – Текст : электронный. – URL: https://www.cnews.ru/news/top/2021-07-29_mezhdunarodnaya_sistema_finansovyh (дата обращения: 17.06.2023).

187. Чернышова, Е. Аналитики допустили рост рынка цифровых активов в России до ₽500 млрд Как может развиваться новый инструмент / Е. Чернышова // Информационное агентство РБК : [сайт]. – 2024. – Текст : электронный. – URL: https://www.rbc.ru/finances/20/02/2024/65d33f059a79473986e2ff19 (дата обращения: 31.03.2024).

188. Чернышова, Е. В России запретят анонимное пополнение кошельков «Яндекс.Деньги» и QIWI / Е. Чернышова // Информационное агентство РБК : [сайт]. – 2019. – Текст : электронный. – URL: https://www.rbc.ru/finances/29/07/2019/5d3b00db9a7947f7ddbd3787?ysclid=lzzuj3w9za146401150 (дата обращения: 18.08.2024).

189. Чернышова, Е. Финразведка предложила урегулировать блокировки онлайн-банков у клиентов / Е. Чернышова, Ю. Кошкина, А. Пустякова // Информационное агентство РБК : [сайт]. – 2023. – Текст : электронный. – URL:

https://www.rbc.ru/finances/26/12/2023/6589a0f89a79473596603226 (дата обращения: 11.08.2024).

190. Чернышова, Е. ЦБ предложит комиссии за оплату цифровым рублем в разы ниже карточных / Е. Чернышова // Информационное агентство РБК : [сайт]. – 2023. – Текст : электронный. – URL: https://www.rbc.ru/finances/17/06/2023/648d84439a794760844ce3b9 (дата обращения: 25.09.2023).

191. Чернышова, Е. Цифровой рубль: что это, зачем его запускают и как он будет работать / Е. Чернышова // РБК. Тренды : [сайт]. – 2023. – Текст : электронный. – URL: https://trends.rbc.ru/trends/industry/60e4014c9a7947816217cac1 (дата обращения: 26.02.2024).

192. Что такое майнинг пул? Преимущества и как выбрать // banki.ru : [сайт]. – 2023. – Текст : электронный. – URL: https://www.banki.ru/dialog/articles/54/ (дата обращения: 18.08.2024).

193. Что такое налоговый мониторинг и как он проводится // Клерк : [сайт]. – 2021. – Текст : электронный. – URL: https://www.klerk.ru/blogs/moedelo/513331/ (дата обращения: 25.02.2024).

194. Эволюция платежей: как СБП, QR-коды, NFC и Pay-приложения изменили опыт россиян // Сетевое издание Forbes : [сайт]. – 2024. – Текст : электронный. – URL: https://www.forbes.ru/spetsproekt/505979-evolucia-platezej-kak-sbp-qr-kody-nfc-i-pay-prilozenia-izmenili-opyt-rossian?erid=4CQwVszH9pWvoxv9cBQ&ysclid=lzov61fb81591680223 (дата обращения: 11.08.2024).

195. Электронные платежные системы в России // TAdviser : [сайт]. – 2023. – Текст : электронный. – URL: https://www.tadviser.ru/index.php/Статья:Электронные_платежные_системы_в_России#1993:_.D0.98.D0.B7.D0.BE.D0.B1.D1.80.D0.B5.D1.82.D0.B5.D0.BD.D0.B8.D0.B5_.D1.8D.D0.BB.D0.B5.D0.BA.D1.82.D1.80.D0.BE.D0.BD.D0.BD.D1.8B.D1.85_.D0.B4.D0.B5.D0.BD.D0.B5.D0.B3 (дата обращения: 18.08.2024).

196. Янушкевич, К. ЕЦБ запускает пилотный проект цифрового евро / К. Янушкевич // Информационное агентство РБК : [сайт]. – 2021. – Текст : электронный. – URL: https://trends.rbc.ru/trends/industry/60f0349b9a7947ad48998e53 (дата обращения: 01.09.2023).

197. CipherTrace подала патенты на технологию отслеживания транзакций в сети Monero // forklog : [сайт]. – 2020. – Текст : электронный. – URL: https://forklog.com/news/ciphertrace-podala-patenty-na-tehnologiyu-otslezhivaniya-tranzaktsij-v-seti-monero (дата обращения: 25.06.2023).

198. VisionLabs // TAdviser : [сайт]. – Текст : электронный. – URL: https://www.tadviser.ru/index.php/Компания:VisionLabs_(ВижнЛабс)?ysclid=lt1tlp5bup957002735 (дата обращения: 25.02.2024).

Статьи

199. Абалкин, Л.И. Экономическая безопасность России: угрозы и их отражение / Л.И. Абалкин // Вопросы экономики. – 1994. – № 12. – С. 4–16. – ISSN 0042-8736.

200. Абрамова, А.А. Комплаенс-система финансовых организаций как способ противодействия финансированию терроризма и легализации (отмыванию) доходов, полученных преступным путем / А.А. Абрамова, М.Ю. Дендиберя // Теория и практика общественного развития. – 2020. – № 9 (151). – С. 33-37. – ISSN 1815-4964.

201. Ашин, Д.А. Виды предикатных преступлений в уголовном праве России / Д.А. Ашин // Актуальные проблемы российского права. – 2010. – № 3. – С. 251–261. – ISSN 1994-1471.

202. Бадеева, Е.А. Современные тенденции и перспективы развития налогового мониторинга в России / Е.А. Бадеева, А.А. Машкина, А.Н. Нагаева // Модели, системы, сети в экономике, технике, природе и обществе. – 2020. – № 1. – С. 24–36. – ISSN 2227-8486.

203. Балашев, Н.Б. Динамика развития электронных платежных технологий в РФ / Н. Б. Балашев, Д. В. Пономарев // Международный журнал гуманитарных и естественных наук. – 2019. – № 11-3. – С. 119-123. – ISSN 2500-1000.

204. Баранов, Р.А. Международный опыт государственных механизмов предотвращения и противодействия легализации (отмыванию) доходов, полученных преступным путем / Р.А. Баранов // Актуальные проблемы современности: наука и общество. – 2015. – № 3 (8). – С. 16–20. – ISSN 2308-8923.

205. Баринов, В.Р. Использование инструментов искусственного интеллекта при разработке программного обеспечения в контексте ПОД/ФТ / В.Р. Баринов, Н.В. Баринова // Угрозы и риски финансовой безопасности в контексте цифровой трансформации : материалы VII Международной научно-практической конференции Международного сетевого института в сфере ПОД/ФТ, Москва, 24 ноября 2021 года. – Москва : Национальный исследовательский ядерный университет «МИФИ», 2021. – С. 241–246. – ISBN 978-5-7262-2839-6. – Текст : электронный. – DOI отсутствует. – URL: https://aml.university/mediateka/659?ysclid=lxryyoblon141657413 (дата обращения: 23.06.2024).

206. Бегишева, И.В. Легализация доходов от наркотрафика как один из видов преступной деятельности / И.В. Бегишева // Финансовая безопасность. – 2020. – № 28. – С. 41-48. – ISSN отсутствует. – Текст : электронный. – DOI отсутствует. – URL: https://fedsfm.ru/content/files/documents/2020/28.pdf (дата обращения: 23.06.2024).

207. Безденежных, В.М. Методология проведения мониторинга мер противодействия проявлениям коррупционного риска в органах государственной исполнительной власти / В.М. Безденежных, В.В. Блекус // Вестник ГГУ. – 2023. – № 6. – С. 317-327. – ISSN 2713-2587. – Текст : электронный. – DOI отсутствует. – URL: http://vestnik-ggu.ru/arhiv_nomera/6_2023/Э%20Безденежных,%20Блекус%20317-327.pdf (дата обращения: 23.06.2024).

208. Безденежных, В.М. Мониторинг теневой экономики региона (на материалах Республики Калмыкия) / В.М. Безденежных, Б.Ц. Сарунова, Н.Э. Манджиев // Тренды социально-экономического развития в условиях реального и виртуального мира : материалы Национальной студенческой научно-практической конференции с международным участием, Элиста, 22 апреля 2021 года / Редколлегия: К.Е. Бадмаева [и др.]. – Элиста : Калмыцкий государственный университет имени Б.Б. Городовикова, 2021. – С. 96-100. – ISBN отсутствует.

209. Беленко, В.В. Проблемы реализации финансового контроля по противодействию легализации доходов, полученных преступным путем, в современной России / В.В. Беленко // Российская юстиция. – 2013. – № 10. – С. 44-47. – ISSN 0131-6761.

210. Бельдина, О.Г. NFT-токен: проблемы правового регулирования / О.Г. Бельдина, С.Н. Бурлака // Право и государство: теория и практика. – 2023. – № 11 – С. 288–290. – ISSN 1815-1337.

211. Борисова, Е.В. К вопросам цифровизации экономики / Е.В. Борисова // Вестник Академии права и управления. – 2020. – № 2. – С. 54–57. – ISSN 2074-9201.

212. Васильева, Т.В. Мобильная коммерция: прошлое, настоящее, будущее / Т.В. Васильева // Вопросы современной науки и практики. Университет им. В.И. Вернадского. – 2014. – № 3. – С. 105-111. – ISSN 1990-9047.

213. Ващекина, И.В. Международное сотрудничество в области противодействия легализации преступных доходов и финансированию терроризма на фоне внешних негативных воздействий / И.В. Ващекина // Международная торговля и торговая политика. – 2018. – № 2. – С. 113-126. – ISSN 2410-7395.

214. Винникова, Р.В. Механизмы мониторинга реализации антикоррупционных конвенций ООН, ГРЕКО и ОЭСР / Р.В. Винникова // Правопорядок: история, теория, практика. – 2017. – № 3. – С. 16-20. – ISSN 2311-696X.

215. Воронин, И.А. Теоретические аспекты отмывания денег и его влияние на экономику / И.А. Воронин // Вестник Северо-Кавказского федерального университета. – 2021. – № 5. – С. 42–48. – ISSN 2307-907X.

216. Галкина, Г.С. Механизм мониторинга устойчивого развития федеральных округов / Г.С. Галкина // Практический маркетинг. – 2015. – № 3. – С. 12-18. – ISSN 2071-3762.

217. Глазкова, М.Е. Органы судебной власти в механизме мониторинга правоприменения и мониторинга процессуальных норм / М.Е. Глазкова // Журнал российского права. – 2012. – № 9. – С. 97-104. – ISSN 1605-6590.

218. Говоров, С.Н. Правовой статус субъектов рынка лизинговых услуг в механизме противодействия легализации (отмыванию) доходов, полученных преступным путем / С.Н. Говоров // Проблемы экономики и юридической практики. – 2007. – № 3. – С. 162–164. – ISSN 2541-8025.

219. Горбунов, Ю.В. О понятии «механизм» в экономических науках / Ю.В. Горбунов // Экономика. Профессия. Бизнес. – 2018. – № 2. – С. 17–21. – ISSN 2413-8584.

220. Грачева, А.Д. Риски трансформации наркоторговли с использованием криптовалют / А.Д. Грачева, И.А. Лебедев, Н.В. Капустина // Государственное и муниципальное управление. Ученые записки. – 2024. – № 1. – С. 104-109. – ISSN 2079-1690.

221. Долгиева, М.М. Противодействие легализации преступных доходов при использовании криптовалюты / М.М. Долгиева // Вестник Томского государственного университета. – 2019. – № 449. – С. 213–218. – ISSN 1561-7793.

222. Едронова, В.Н. Финансовый мониторинг как категория научного исследования / В.Н. Едронова // Финансы и кредит. – 2016. – № 14. – С. 43-57. – ISSN 2071-4688.

223. Ефимов, Д.А. Некредитные финансовые организации: понятие и роль на финансовом рынке Российской Федерации / Д.А. Ефимов // Актуальные проблемы российского права. – 2018. – № 6. – С. 49–56. – ISSN 1994-1471.

224. Заернюк, В.М. Оценка существующего механизма противодействия отмыванию преступных доходов в банковской сфере России / В.М. Заернюк // Дайджест-финансы. – 2012. – № 12. – С. 6–12. – ISSN 2073-8005.

225. Заколдаев, Д.А. Технология блокчейн в России: достижения и проблемы / Д.А. Заколдаев, Р.В. Ямщиков, Н.В. Ямщикова // Российский социально-гуманитарный журнал. – 2018. – № 2. – С. 93–107. – ISSN 2949-5032. – Текст : электронный. – DOI 10.18384/2224-0209-2018-2-889. – URL: https://www.evestnik-mgou.ru/jour/article/view/345/343 (дата обращения: 23.06.2024).

226. Зимин, О.В. Понятие и структура государственной системы противодействия легализации (отмыванию) преступных доходов в Российской Федерации / О.В. Зимин // Вестник экономической безопасности. – 2009. – № 10. – С. 45–53. – ISSN 2414-3995.

227. Зимин, О.В. Современные способы, экономические схемы и классификация моделей легализации (отмывания) преступных доходов / О.В. Зимин // Законодательство и экономика. – 2007. – № 8. – С. 63–72. – ISSN 0869-1983.

228. Исаков, Р.В. О противодействии легализации (отмыванию) наркодоходов с использованием финансовых активов (криптовалют) / Р.В. Исаков, Д.В. Теткин, А.М. Попов // Вестник Воронежского института МВД России. – 2021. – № 2. – С. 267–271. – ISSN 2071-3584.

229. Казанцев, Д.А. Влияние отмывания преступных доходов на экономическую безопасность государства / Д.А. Казанцев // Научный форум: Инновационная наука : сборник статей по материалам LX Международной научно-практической конференции. – Москва : Издательство «МЦНО», 2023. – № 5 (60). – С. 38-43. – 44 с. – ISSN 2542-1255.

230. Казанцев, Д.А. К вопросу о генезисе легализации (отмывания) доходов, полученных преступным путем / Д.А. Казанцев // Самоуправление. – 2022. – № 3 (131). – С. 56–59. – ISSN 2221-8173.

231. Казанцев, Д.А. К вопросу о повышении эффективности механизма противодействия отмыванию доходов, полученных преступным путем, и финансированию терроризма / Д.А. Казанцев, Н.В. Капустина // Вестник Евразийской науки. – 2023. – № S6. Том 15. – ISSN 2588-0101. – Текст : электронный. – DOI отсутствует. — URL: https://esj.today/PDF/07FAVN623.pdf (дата обращения: 16.07.2024).

232. Казанцев, Д.А. К вопросу о понятии механизма противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма / Д.А. Казанцев // Вопросы экономики и права. – 2023. – № 8 (182). – С. 43-47. – ISSN 2072-5574.

233. Казанцев, Д.А. Роль системы противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма в обеспечении экономической безопасности государства / Д.А. Казанцев, С.И. Кравченко // Экономика. Наука. Инноватика : материалы III Международной научно-практической конференции ; под редакцией А.В. Ярошенко. – Донецк : ДонНТУ, 2023. – С. 159-162. – 636 с. – ISBN отсутствует. – Текст : электронный. – DOI отсутствует. – URL: https://www.elibrary.ru/download/elibrary_60005805_10465218.pdf (дата обращения: 16.07.2024).

234. Казанцев, Д.А. Теоретический базис механизма мониторинга противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма в условиях цифровизации экономики / Д.А. Казанцев // Вестник Евразийской науки. – 2024. – № S4. Том 16. – ISSN 2588-0101. – Текст : электронный. – DOI отсутствует. — URL: https://esj.today/23FAVN424.html (дата обращения: 06.08.2024).

235. Казанцев, Д.А. Трансформация механизма противодействия отмыванию доходов, полученных преступным путем, и финансированию терроризма в условиях цифровизации экономики (на примере минимизации рисков, связанных с использованием криптовалют) / Д.А. Казанцев // Вестник Евразийской науки. – 2024. – № S2. Том 16. – ISSN 2588-0101. – Текст :

электронный. – DOI отсутствует. — URL: https://esj.today/PDF/43FAVN224.pdf (дата обращения: 23.06.2024).

236. Казанцев, Д.А. Финансирование терроризма: понятие и источники / Д.А. Казанцев // Право, экономика и управление: теория и практика : материалы III Всероссийской научно-практической конференции с международным участием ; под редакцией Э.В. Фомина. – Чебоксары : Среда, 2022. – С. 309-312. – 340 с. – ISBN 978-5-907561-45-8.

237. Капустина, Н.В. Проблемы и перспективы взаимодействия федеральных органов исполнительной власти в сфере ПОД/ФТ / Н.В. Капустина // Вестник евразийской науки. – 2024. – Т. 16. – № 1. – ISSN 2588-0101. – Текст : электронный. – DOI отсутствует. — URL: https://esj.today/PDF/84ECVN124.pdf (дата обращения: 24.03.2024).

238. Карпова, Е.Н. Современные тенденции в области цифровизации внутреннего контроля в целях противодействия отмыванию преступных доходов и финансированию терроризма в кредитных организациях / Е.Н. Карпова, И.А. Колесник, А.А. Коновалов // Фундаментальные исследования. – 2020. – № 4. – С. 52-56. – ISSN 1812-7339.

239. Коваль, А.А. Риски включения России в «черный» или «серый» списки ФАТФ / А.А. Коваль, А.Д. Левашенко // Экономическое развитие России. – 2023. – № 8. – С. 8–11. – ISSN 2306-5001.

240. Кондрат, Е.Н. Влияние легализации преступных доходов на экономическую безопасность государства / Е.Н. Кондрат // Вестник экономической безопасности. – 2010. – № 9. – С. 78–84. – ISSN 2414-3995.

241. Курьянова, С.Л. Биометрическая идентификация клиентов в банковской сфере: отечественный и зарубежный опыт / С.Л. Курьянова, О.С. Цвигунова // Азимут научных исследований: экономика и управление. – 2019. – № 4. – С. 238–241. – ISSN 2309-1762.

242. Лапина, С.Б. Научные подходы к совершенствованию механизма противодействия легализации преступных доходов в России / С.Б. Лапина //

Вестник Московского университета МВД России. – 2020. – № 4. – С. 253–258. – ISSN 2073-0454.

243. Ларин, Д.С. Особенности организации системы ПОД/ФТ США (American AML/CFT system key features) / Д.С. Ларин // Восточно-европейский научный журнал. – 2015. – № 1. – С. 59–61. – ISSN 2782-1994. – Текст : электронный. – DOI отсутствует. — URL: https://www.elibrary.ru/download/elibrary_25469417_37634408.pdf (дата обращения: 23.06.2024).

244. Лебедев, И.А. Проблемы эффективности российской системы финансового мониторинга / И.А. Лебедев, С.В. Ефимов, В.В. Потехина // Известия высших учебных заведений. Серия: Экономика, финансы и управление производством. – 2019. – № 4. – С. 26-31. – ISSN 2218-1784.

245. Лоскутов, И.Н. Цифровая идентификация как инструмент противодействия отмыванию доходов и финансированию терроризма / И.Н. Лоскутов, Ф.К. Иванов // Финансовые исследования. – 2020. – № 1 (66). – С. 14–19. – ISSN 1991-0525.

246. Марамыгин, М.С. Цифровая трансформация российского рынка финансовых услуг: тенденции и особенности / М.С. Марамыгин, Г.В. Чернова, Л.Г. Решетникова // Управленец. – 2019. – № 3. – С. 70-82. – ISSN 2218-5003.

247. Милюков, А.Ф. К вопросу о сущности отмывания и легализации преступных доходов и мерах по их нейтрализации / А.Ф. Милюков // Вестник Воронежского института МВД России. – 2007. – № 1. – С. 86–88. – ISSN 2071-3584.

248. Михайлов, С.Н. Методологические механизмы мониторинга функционирования и устойчивого развития хозяйственных образований в промышленности / С.Н. Михайлов // Евразийская интеграция: экономика, право, политика. – 2011. – № 9. – С. 56-64. – ISSN 2073-2929.

249. Мурадян, С.В. Перспективы использования криптовалют для целей финансирования терроризма и меры по предупреждению указанной тенденции / С.В. Мурадян // Закон и право. – 2022. – № 5. – С. 196–201. – ISSN 2073-3313.

250. Мчедлишвили, Р.С. Роль криптовалюты в легализации доходов, полученных преступным путем / Р.С. Мчедлишвили, А.И. Аманлиев // Вестник евразийской науки. – 2021. – № 6. – ISSN 2588-0101. – Текст : электронный. – DOI отсутствует. – URL: https://esj.today/PDF/69ECVN621.pdf (дата обращения: 22.06.2023).

251. Новиков, И.А. Российская система противодействия легализации преступных доходов и финансированию терроризма / И.А. Новиков // Власть. – 2012. – № 3. – С. 63–66. – ISSN 2071-5358.

252. Овчинникова, О.П. Эволюция национальной системы финансового мониторинга / О.П. Овчинникова, И.М. Аничкин // Вестник Воронежского государственного университета. Серия: Экономика и управление. – 2016. – № 3. – С. 117–124. – ISSN 1814-2966.

253. Павлов, К.В. Формы и направления цифровизации экономики / К.В. Павлов, Н.Р. Асадуллина // Большая Евразия: развитие, безопасность, сотрудничество : ежегодник : материалы XIX Национальной научной конференции с международным участием, Москва, 18–19 декабря 2019 года. Выпуск 3. Часть 1. – Москва : Институт научной информации по общественным наукам РАН, 2020. – С. 355–358. – ISBN 978-5-248-00956-5.

254. Петухова, Н.В. Противодействие легализации (отмыванию) денежных средств как фактор экономического роста России / Н.В. Петухова // Научные труды Вольного экономического общества России. – 2013. – С. 159-177. – ISSN 2072-2060.

255. Прасолов, В.И. Влияние цифровой трансформации на процессы выявления легализации доходов, полученных преступным путем / В.И. Прасолов, С.С. Фешина // Экономика: вчера, сегодня, завтра. – 2020. – № 8А. – С. 130-145. – ISSN 2222-9167.

256. Прошунин, М.М. К вопросу о понятии отмывания преступных доходов / М.М. Прошунин // Вестник Российского университета дружбы народов. Серия: Юридические науки. – 2008. – № 3. – С. 47–52. – ISSN 2313-2337.

257. Прошунин, М.М. Финансовый мониторинг и цифровая экономика: вызовы и пути их решения / М.М. Прошунин // Финансовое право. – 2018. – № 8. – С. 3–7. – ISSN 1813-1220.

258. Прошунин, М.М. Финансовый мониторинг: субъекты, объекты и значение / М.М. Прошунин // Вестник Российского университета дружбы народов. Серия: Юридические науки. – 2008. – № 2. – С. 43-50. – ISSN 2313-2337.

259. Ревенков, П.В. Риски отмывания денег в условиях применения электронных денег / П.В. Ревенков, А.Б. Дудка // Вестник Омского университета. Серия: Экономика. – 2015. – № 4. – С. 78-88. – ISSN 1812-3988.

260. Симакова, Д.Е. Цифровой рубль как инструмент противодействия финансовым преступлениям / Д.Е. Симакова, Д.А. Гурнина // Российский экономический Интернет-журнал. – 2021. – № 2. – ISSN 2218-5402. – Текст : электронный. – DOI отсутствует. – URL: https://www.e-rej.ru/upload/iblock/939/9395751bf12b4f3fd4db0e692d99bad6.pdf (дата обращения: 25.09.2023).

261. Соколов, Ю.А. Методика определения численности службы внутреннего контроля кредитной организации / Ю.А. Соколов, А.А. Оськина // Известия высших учебных заведений. Серия: Экономика, финансы и управление производством. – 2013. – № 1. – С. 82–85. – ISSN 2218-1784.

262. Тарасов, И.В. Индустрия 4.0: понятие, концепции, тенденции развития / И.В. Тарасов // Стратегии бизнеса. – 2018. – № 6. – ISSN 2311-7184. – Текст : электронный. – DOI 10.17747/2311-7184-2018-5-43-49. – URL: https://www.strategybusiness.ru/jour/article/view/433/377 (дата обращения: 23.06.2024).

263. Тихонин, И.А. Создание Федеральной службы по финансовому мониторингу: исторический аспект / И.А. Тихонин, Н.А. Максякова // Вопросы российской юстиции. – 2023. – № 24. – С. 433–443. – ISSN 2687-007X. – Текст : электронный. – DOI отсутствует. – URL: https://www.elibrary.ru/download/elibrary_52694629_47187020.pdf (дата обращения: 23.06.2024).

264. Третьяков, В.И. О правовых механизмах борьбы с легализацией криминальных доходов / В.И. Третьяков // Юристъ-Правоведъ. – 2007. – № 4 (23). – С. 76-79. – ISSN 1817-7093.

265. Хисамова, З.И. Концепция цифровых валют центральных банков: основные риски в части соблюдения требований AML («Противодействия отмыванию денег») и KYC («Знай своего клиента») / З.И. Хисамова // Russian Journal of Economics and Law. – 2020. – № 3. – С. 508-515. – ISSN 2782-2923.

266. Хисамова, З.И. Способы легализации (отмывания) доходов, полученных преступным путем, с использованием информационно-телекоммуникационных технологий / З.И. Хисамова // Вестник Краснодарского университета МВД России. – 2017. – № 2 (36). – С. 84-87. – ISSN 2073-1078.

267. Хомич, О.В. Понятие легализации доходов, полученных преступным путем // Образование и право. – 2018. – № 2. – С. 153–159. – ISSN 2076-1503.

268. Чистюхин, В.В. Виды некредитных финансовых организаций / В.В. Чистюхин // Актуальные проблемы российского права. – 2021. – № 11. – С. 32–41. – ISSN 1994-1471.

269. Чувилкин, Н.А. Противодействие отмыванию доходов и финансированию терроризма как фактор обеспечения экономической безопасности экономики и общества / Н.А. Чувилкин // Экономическая безопасность. – 2021. – № 4. – С. 1237-1258. – ISSN 2658-7548.

270. Шаманина, Е.И. Биометрические технологии как перспективное направление совершенствования дистанционного банковского обслуживания / Е.И. Шаманина, Ю.С. Захаренко // Вестник университета. – 2020. – №5. – С. 193–199. – ISSN 1816-4277.

271. Шевляков, Е.В. Возможности и вызовы, связанные с искусственным интеллектом, в сфере противодействия отмыванию преступных доходов и финансированию терроризма / Е.В. Шевляков, Д.А. Казанцев // Вопросы экономики и права. – 2023. – № 11 (185). – С. 68-75. – ISSN 2072-5574.

272. Юсупов, Н.В. Некоторые аспекты теоретического анализа правового механизма противодействия отмыванию доходов полученных преступным путем /

Н.В. Юсупов // Вестник экономической безопасности. – 2009. – № 2. – С. 148–149. – ISSN 2414-3995.

273. Юсупов, Н.В. Политико-правовой механизм противодействия отмыванию денег, полученных незаконным путем в Российской Федерации: проблемы теоретического анализа / Н.В. Юсупов // Проблемы экономики и юридической практики. – 2008. – № 2. – С. 215–217. – ISSN 2541-8025.

Источники на иностранном языке

274. 2024 Crypto Crime Trends: Illicit Activity Down as Scamming and Stolen Funds Fall, But Ransomware and Darknet Markets See Growth = Тенденции криптопреступности в 2024 году: Незаконная деятельность снижается по мере снижения уровня мошенничества и кражи средств, но рынки программ-вымогателей и Даркнета растут // Chainalysis : [website]. – 2024. – Текст : электронный. – URL: https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/ (дата обращения: 06.04.2024).

275. About GIABA = О Межправительственной группе по борьбе с отмыванием денег в Западной Африке // Inter Governmental Action Group against Money Laundering in West Africa GIABA = Межправительственная группа по борьбе с отмыванием денег в Западной Африке : официальный сайт. – Текст : электронный. – URL: https://www.giaba.org/about-giaba/index_656.html (дата обращения: 03.06.2023).

276. About - Wolfsberg Group = О Вольфсбергской группе // The Wolfsberg Group = Вольфсбергская группа : официальный сайт. – Текст : электронный. – URL: https://wolfsberg-group.org/about (дата обращения: 02.06.2023).

277. APG History And Background = История и происхождение Азиатско-Тихоокеанской группы по борьбе с отмыванием денег // Asia / Pacific Group On Money Laundering APG = Азиатско-Тихоокеанская группа по борьбе с отмыванием денег : официальный сайт. – Текст : электронный. – URL: https://apgml.org/about-

us/page.aspx?p=91ce25ec-db8a-424c-9018-8bd1f6869162 (дата обращения: 01.06.2023).

278. «Black and grey» lists = «Черный и серый» списки // The Financial Action Task Force FATF = Группа разработки финансовых мер по борьбе с отмыванием денег ФАТФ : официальный сайт. – Текст : электронный. – URL: https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html (дата обращения: 05.06.2023).

279. Central Bank Digital Currency = Цифровая валюта Центрального банка // Cato Institute : [website]. – 2023. – Текст : электронный. – URL: https://www.cato.org/policy-analysis/central-bank-digital-currency (дата обращения: 01.09.2023).

280. Central KYC Registry in India = Центральный реестр KYC в Индии // MN & Associates : [website]. – Текст : электронный. – URL: https://cs-india.com/central-kyc-registry-in-india/ (дата обращения: 19.08.2023).

281. CFATF Overview = Обзор Карибской группы разработки финансовых мер борьбы с отмыванием денег // Caribbean Financial Action Task Force (CFATF) = Карибская группа разработки финансовых мер борьбы с отмыванием денег (КФАТФ) : официальный сайт. – Текст : электронный. – URL: https://www.cfatf-gafic.org/index.php/home/cfatf-overview (дата обращения: 31.05.2023).

282. Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering = Директива Совета ЕС 91/308/EEC от 10 июня 1991 года о предотвращении использования финансовой системы в целях отмывания денег // EUR-lex : [website]. – Текст : электронный. – URL: https://eur-lex.europa.eu/eli/dir/1991/308/oj (дата обращения: 30.05.2023).

283. Dorman, M. Criminals channel £4bn of illegal money through cryptocurrencies, says Europol = Преступники направляют 4 миллиарда фунтов стерлингов преступных доходов через криптовалюты, сообщает Европол / M. Dorman // Yahoo : [website]. – 2018. – Текст : электронный. – URL: https://www.yahoo.com/lifestyle/criminals-channel-4bn-illegal-money-cryptocurrencies-says-europol-151513486.html (дата обращения: 23.06.2023).

284. ESAAMLG – About = О Группе по борьбе с отмыванием денег в Восточной и Южной Африке // Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) = Группа по борьбе с отмыванием денег в Восточной и Южной Африке : официальный сайт. – Текст : электронный. – URL: https://www.esaamlg.org/index.php/about_esaamlg_history (дата обращения: 03.06.2023).

285. Financial Action Task Force of Latin America (GAFILAT) = Группа разработки финансовых мер борьбы с отмыванием денег государств Латинской Америки (ГАФИЛАТ) // Financial Action Task Force FATF = Группа разработки финансовых мер по борьбе с отмыванием денег ФАТФ : официальный сайт. – Текст : электронный. – URL: https://www.fatfgaf.org/pages/gafilat.html (дата обращения: 03.06.2023).

286. GABAC = Группа разработки финансовых мер борьбы с отмыванием денег в Центральной Африке (ГАБАК) // Financial Action Task Force FATF = Группа разработки финансовых мер по борьбе с отмыванием денег ФАТФ : официальный сайт. – Текст : электронный. – URL: https://www.fatfgaf.org/pages/gabac.html (дата обращения: 03.06.2023).

287. Global Cryptocurrency Market Cap Charts = Графики глобальной рыночной капитализации криптовалют // CoinGecko : [website]. – Текст : электронный. – URL: https://www.coingecko.com/en/global-charts (дата обращения: 23.06.2023).

288. Golsten, S. Department of Homeland Security Turns Attention to Monero, Zcash = Министерство внутренней безопасности обратило внимание на Monero, Zcash / S. Golsten // Finance Magnates : [website]. – 2018. – Текст : электронный. – URL: https://www.financemagnates.com/cryptocurrency/news/department-of-homeland-security-turns-attention-to-monero-zcash/ (дата обращения: 25.06.2023).

289. Guidance on Digital ID = Руководство по цифровому ID // Financial Action Task Force FATF = Группа разработки финансовых мер по борьбе с отмыванием денег ФАТФ : официальный сайт. – 2020. – Текст : электронный. –

URL: https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Digital-identity-guidance.html (дата обращения: 20.08.2023).

290. Machines responsible for 80% of trades in the US, fund manager says = По словам управляющего фондом, на машины приходится 80% сделок в США // CNBC : [website]. – 2018. – Текст : электронный. – URL: https://www.cnbc.com/video/2018/12/05/machines-responsible-for-80-percent-of-trades-in-the-us-fund-manager-says.html (дата обращения: 25.06.2023).

291. McSweeney, M. Coinbase wants to sell blockchain analysis software to the IRS and DEA a year after its Neutrino acquisition = Coinbase хочет продать программное обеспечение для анализа блокчейна Налоговому управлению США и DEA через год после приобретения Neutrino / M. McSweeney // THE Block : [website]. – 2020. – Текст : электронный. – URL: https://www.theblock.co/post/67551/coinbase-irs-dea-analytics-neutrino (дата обращения: 25.06.2023).

292. McSweeney, M. IRS seeks info on tracing privacy coins, Lightning network transactions for pilot program = Налоговое управление США запрашивает информацию об отслеживании анонимных криптовалют и транзакций посредством Lightning network для пилотной программы / M. McSweeney // THE Block : [website]. – 2020. – Текст : электронный. – URL: https://www.theblock.co/post/70320/irs-crypto-pilot-privacy-coins-lightning (дата обращения: 25.06.2023).

293. Mutual Evaluation Russian Federation 2019 = Отчет о взаимной оценке Российской Федерации 2019 // Financial Action Task Force FATF = Группа разработки финансовых мер по борьбе с отмыванием денег ФАТФ : официальный сайт. – 2019. – Текст : электронный. – URL: https://www.fatf-gafi.org/content/dam/fatf-gafi/mer/Mutual-Evaluation-Russian-Federation-2019.pdf (дата обращения: 16.06.2023).

294. Overview = Обзор // Middle East and North Africa Financial Action Task Force MENAFATF = Группа разработки финансовых мер борьбы с отмыванием денег на Ближнем Востоке и в Северной Африке : официальный сайт. – Текст : электронный. – URL: https://menafatf.org/about (дата обращения: 03.06.2023).

295. The Chainalysis 2023 Crypto Crime Report = Отчет о криптопреступлениях Chainalysis за 2023 год // Chainalysis : [website]. – 2023. – Текст : электронный. – URL: https://go.chainalysis.com/2023-crypto-crime-report.html (дата обращения: 21.06.2023).

296. The forty recommendations of the Financial Action Task Force on money laundering 1990 = Сорок рекомендаций Группы разработки финансовых мер по борьбе с отмыванием денег 1990 года // Financial Action Task Force FATF = Группа разработки финансовых мер по борьбе с отмыванием денег ФАТФ : официальный сайт. – Текст : электронный. – URL: https://www.fatf-gafi.org/content/dam/fatf/documents/recommendations/pdfs/FATF%20Recommendations%201990.pdf (дата обращения: 29.05.2023).

297. Mansa, J. What Are Crypto Tokens, and How Do They Work? = Что такое криптотокены и как они работают / J. Mansa // Investopedia : [website]. – 2023. – Текст : электронный. – URL: https://www.investopedia.com/terms/c/crypto-token.asp (дата обращения: 18.03.2024).

298. Arnold, M. HSBC brings in AI to help spot money laundering = HSBC использует искусственный интеллект для выявления случаев отмывания денег / M. Arnold // Financial Times : [website]. – 2018. – Текст : электронный. – URL: https://www.ft.com/content/b9d7daa6-3983-11e8-8b98-2f31af407cc8 (дата обращения: 24.06.2023).

299. Prevention of criminal use of the banking system for the purpose of money-laundering = Предотвращение преступного использования банковской системы в целях отмывания денег // Bank for International Settlements = Банк международных расчетов : официальный сайт. – Текст : электронный. – URL: https://www.bis.org/publ/bcbsc137.pdf (дата обращения: 26.05.2023).

300. Private Sector Economic Impacts from Identification Systems = Экономическое воздействие систем идентификации на частный сектор // The World Bank = Всемирный банк : официальный сайт. – 2018. – Текст : электронный. – URL: https://documents1.worldbank.org/curated/en/219201522848336907/pdf/Private-Sector-Economic-Impacts-from-Identification-Systems.pdf (дата обращения: 19.08.2023).

301. Tokar, D. Google Cloud Launches Anti-Money-Laundering Tool for Banks, Betting on the Power of AI = Google Cloud запускает инструмент для борьбы с отмыванием денег для банков, делая ставку на возможности искусственного интеллект / D. Tokar // The Wall Street Journal : [website]. – 2023. – Текст : электронный. – URL: https://www.wsj.com/articles/google-cloud-launches-anti-money-laundering-tool-for-banks-betting-on-the-power-of-ai-2512ccce (дата обращения: 24.06.2023).

302. Using eKYC to seamlessly onboard Indian consumers = Использование eKYC для бесперебойной работы с индийскими потребителями // Trulioo : [website]. – 2019. – Текст : электронный. – URL: https://www.trulioo.com/blog/identity-verification/ekyc-india (дата обращения: 19.08.2023).

303. What You Should Know About Singapore’s Myinfo Service (Business & Individual) = Что Вам следует знать о Сингапурском Сервисе Myinfo (для бизнеса и физических лиц) // MPM Capital : [website]. – 2021. – Текст : электронный. – URL: https://www.mpmcapital.com.sg/singapore-myinfo-service/ (дата обращения: 19.08.2023).

304. Wolfsberg Anti-Money Laundering Principles for Private Banking (2012) = Вольфсбергские принципы борьбы с отмыванием денег для частных банковских учреждений (2012) // Wolfsberg Group DB = Вольфсбергская группа : официальный сайт. – Текст : электронный. – URL: https://wb-db.basel.institute/assets/7d384fb4-8c82-4669-acb8-621aed03e928/10.%20Wolfsberg-Private-Banking-Prinicples-May-2012.pdf (дата обращения: 02.06.2023).

305. Wolfsberg Statement on the Suppression of the Financing of Terrorism = Вольфсбергское заявление о борьбе с финансированием терроризма // Wolfsberg Group DB = Вольфсбергская группа : официальный сайт. – Текст : электронный. – URL: https://wb-db.basel.institute/assets/223bfb8c-6536-41e1-8f3c-6c9f7bebae8a/16.%20Wolfsberg_Statement_on_the_Suppression_of_the_Financing_of_Terrorism_(2002).pdf (дата обращения: 02.06.2023).

306. Chan, Y.-L. Trade-based Money Laundering: general methodologies. Is smart contract blockchain technology a possible solution? = Отмывание денег на основе

торговли: общие методологии. Является ли технология блокчейна для смарт-контрактов возможным решением? / Y.-L. Chan // International Journal of Academic Research in Business, Arts and Science. – 2022. – № 4. – ISSN 2664-7354. – Текст : электронный. – DOI 10.5281/zenodo.7126375. – URL: https://www.ijarbas.com/wp-content/uploads/2022/09/4.9-2022-1-Trade-based-Money-Laundering-general-methodologies-Is-smart-contract-blockchain-technology-a-possible-solution.pdf (дата обращения: 23.06.2024).

Приложение А

(информационное)

Расчеты корреляционной зависимости величин, фигурирующих в исследовании

Для расчета коэффициента корреляции используется формула (1)

$$Correl\ (X;Y) = \frac{\sum(x-\bar{x})(y-\bar{y})}{\sqrt{\sum(x-\bar{x})^2\sum(y-y)^2}}, \quad (1)$$

где x,y – переменные, которые анализируются на наличие корреляции;

$\bar{x}$, $\bar{y}$ – средние значения переменных, которые анализируются на наличие корреляции.

Для вычислений коэффициентов корреляции использовалась функция КОРРЕЛ (X;Y) в программном продукте Microsoft Excel.

	Выявление корреляционной зависимости между числом проверок кредитных организаций и объемом вывода денежных средств за рубеж по подозрительным основаниям в банковском секторе			
	Количество проверок кредитных организаций (шт.)	Объем вывода денежных средств за рубеж по подозрительным основаниям в банковском секторе (млрд рублей)		
2015	626	501		
2016	557	199		
2017	200	96		
2018	146	73		
2019	59	66		
2020	48	52		
2021	46	43		
2022	16	37		
	Коэффициент корреляции	0,887606202		

Источник: составлено автором.

Рисунок А.1 – Выявление корреляционной зависимости между числом проверок кредитных организаций и объемом вывода денежных средств за рубеж по подозрительным основаниям в банковском секторе

Источник: составлено автором.

Рисунок А.2 – Поле корреляции между числом проверок кредитных организаций и объемом вывода денежных средств за рубеж по подозрительным основаниям в банковском секторе

Выявление корреляционной зависимости между числом проверок кредитных организаций и объемом обналичивания денежных средств по подозрительным основаниям в банковском секторе				
	Количество проверок кредитных организаций (шт.)	Объем обналичивания денежных средств по подозрительным основаниям в банковском секторе (млрд рублей)		
2015	626	600		
2016	557	522		
2017	200	326		
2018	146	176		
2019	59	111		
2020	48	78		
2021	46	62		
2022	16	64		
	Коэффициент корреляции	0,982720273		

Источник: составлено автором.

Рисунок А.3 – Выявление корреляционной зависимости между числом проверок кредитных организаций и объемом обналичивания денежных средств по подозрительным основаниям в банковском секторе

Источник: составлено автором.

Рисунок А.4 – Поле корреляции между числом проверок кредитных организаций и объемом обналичивания денежных средств по подозрительным основаниям в банковском секторе

Выявление корреляционной зависимости между числом проверок кредитных организаций и количеством возбужденных Банком России дел об административных правонарушениях

	Количество проверок кредитных организаций (шт.)	Количество дел об административных правонарушениях в отношении кредитных организаций и их должностных лиц (шт.)		
2015	626	370		
2016	557	545		
2017	200	479		
2018	146	466		
2019	59	559		
2020	48	79		
2021	46	64		
2022	16	59		
Коэффициент корреляции		0,484676974		

Источник: составлено автором.

Рисунок А.5 – Выявление корреляционной зависимости между числом проверок кредитных организаций и количеством возбужденных Банком России дел об административных правонарушениях

Источник: составлено автором.

Рисунок А.6 – Поле корреляции между числом проверок кредитных организаций и количеством возбужденных Банком России дел об административных правонарушениях

Выявление корреляционной зависимости между числом проверок некредитных финансовых организаций и количеством возбужденных Банком России дел об административных правонарушениях

	Количество проверок некредитных финансовых организаций (шт.)	Количество дел об административных правонарушениях в отношении некредитных финансовых организаций и их должностных лиц (шт.)		
2017	73	3001		
2018	32	2859		
2019	21	7034		
2020	17	2477		
2021	36	3796		
2022	10	2044		
	Коэффициент корреляции	-0,052418343		

Источник: составлено автором.

Рисунок А.7 – Выявление корреляционной зависимости между числом проверок некредитных финансовых организаций и количеством возбужденных Банком России дел об административных правонарушениях

Источник: составлено автором.

Рисунок А.8 – Поле корреляции между числом проверок некредитных финансовых организаций и количеством возбужденных Банком России дел об административных правонарушениях

Выявление корреляционной зависимости между числом проверок кредитных организаций и количеством кредитных организаций, к которым были применены меры государственного принуждения

	Количество проверок кредитных организаций (шт.)	Количество кредитных организаций, к которым были применены меры государственного принуждения (шт.)		
2017	200	248		
2018	146	316		
2019	59	182		
2020	48	92		
2021	46	84		
2022	16	128		
	Коэффициент корреляции	0,812729419		

Источник: составлено автором.

Рисунок А.9 – Выявление корреляционной зависимости между числом проверок кредитных организаций и количеством кредитных организаций, к которым были применены меры государственного принуждения

Источник: составлено автором.

Рисунок А.10 – Поле корреляции между числом проверок кредитных организаций и количеством кредитных организаций, к которым были применены меры государственного принуждения

Выявление корреляционной зависимости между числом проверок некредитных финансовых организаций и количеством НФО, к которым были применены меры государственного принуждения

	Количество проверок некредитных финансовых организаций (шт.)	Количество некредитных финансовых организаций, к которым были применены меры государственного принуждения (шт.)		
2017	73	2028		
2018	32	1419		
2019	21	3118		
2020	17	1568		
2021	36	2156		
2022	10	1657		
	Коэффициент корреляции	0,049921649		

Источник: составлено автором.

Рисунок А.11 – Выявление корреляционной зависимости между числом проверок некредитных финансовых организаций и количеством НФО, к которым были применены меры государственного принуждения

Источник: составлено автором.

Рисунок А.12 – Поле корреляции между числом проверок некредитных финансовых организаций и количеством некредитных финансовых организаций, к которым были применены меры государственного принуждения

Выявление корреляционной зависимости между числом проверок кредитных организаций и количеством кредитных организаций, у которых были отозваны лицензии

	Количество проверок кредитных организаций (шт.)	Количество кредитных организаций, у которых была отозвана лицензия (шт.)		
2015	626	34		
2016	557	35		
2017	200	24		
2018	146	35		
2019	59	14		
2020	48	9		
2021	46	14		
2022	16	2		
	Коэффициент корреляции	0,782172493		

Источник: составлено автором.

Рисунок А.13 – Выявление корреляционной зависимости между числом проверок кредитных организаций и количеством кредитных организаций, у которых были отозваны лицензии

Источник: составлено автором.

Рисунок А.14 – Поле корреляции между числом проверок кредитных организаций и количеством кредитных организаций, у которых были отозваны лицензии

Выявление корреляционной зависимости между числом проверок некредитных финансовых организаций и количеством некредитных финансовых организаций, у которых были отозваны лицензии

	Количество проверок некредитных финансовых организаций (шт.)	Количество некредитных финансовых организаций, у которых была отозвана лицензия (шт.)		
2017	73	1		
2018	32	0		
2019	21	4		
2020	17	0		
2021	36	7		
2022	10	1		
	Коэффициент корреляции	0,03033525		

Источник: составлено автором.

Рисунок А.15 – Выявление корреляционной зависимости между числом проверок некредитных финансовых организаций и количеством некредитных финансовых организаций, у которых были отозваны лицензии

Источник: составлено автором.

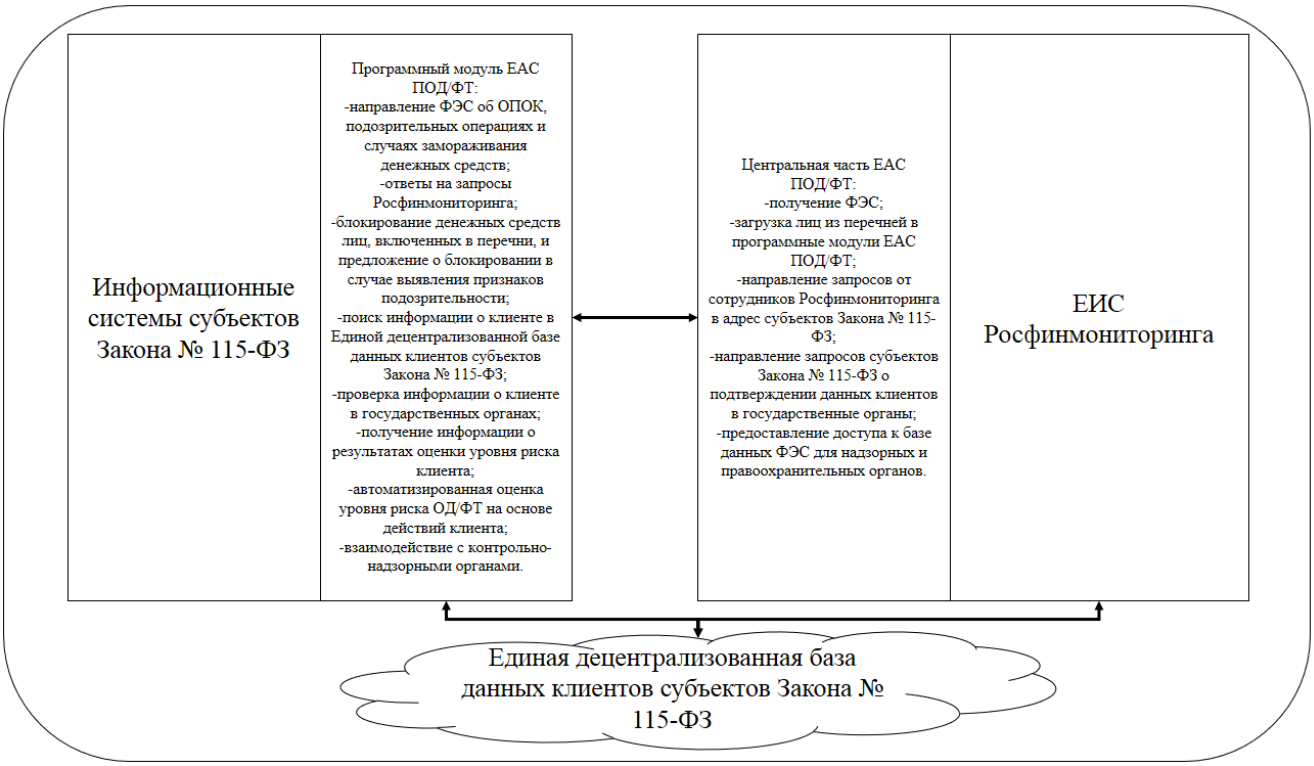
Рисунок А.16 – Поле корреляции между числом проверок некредитных финансовых организаций и количеством некредитных финансовых организаций, у которых были отозваны лицензии

Приложение Б

(информационное)

Структура Единой автоматизированной системы противодействия отмыванию доходов, полученных преступным путем, и финансированию терроризма

Структура ЕАС ПОД/ФТ представлена на Рисунке Б.1.



Источник: составлено автором.

Рисунок Б.1 – Структура Единой автоматизированной системы противодействия отмыванию доходов, полученных преступным путем, и финансированию терроризма

Структурно ЕАС ПОД/ФТ состоит из двух частей:

а) Центральная часть ЕАС ПОД/ФТ, расположенная на серверах Росфинмониторинга.

б) Программный модуль ЕАС ПОД/ФТ, интегрированный в информационные системы субъектов Закона № 115-ФЗ.

Структура подмодулей ЕАС ПОД/ФТ представлена в таблице Б.1.

Таблица Б.1 – Структура подмодулей ЕАС ПОД/ФТ

Название подмодуля	Описание
1	2
Центральная часть ЕАС ПОД/ФТ	
Подмодуль получения ФЭС	Получение ФЭС от субъектов Закона № 115-ФЗ с последующие передачей информации в ЕИС Росфинмониторинга

Продолжение таблицы Б.1

1	2
Подмодуль получения ответов на запросы	Получение ответов на запросы от субъектов Закона № 115-ФЗ с последующие передачей информации в ЕИС Росфинмониторинга
Подмодуль загрузки информации из перечней	Загрузка информации из перечней лиц, чьи средства подлежат замораживанию, в программные модули ЕАС ПОД/ФТ для последующей блокировки денежных средств
Подмодуль передачи запросов от субъектов Закона № 115-ФЗ в государственные органы	Получение от субъектов Закона № 115-ФЗ запросов на проверку информации о клиенте, проверка их обоснованности и передача запросов в адрес государственных органов
Подмодуль доступа к ФЭС для правоохранительных и надзорных органов	Предоставление доступа к базе данных ФЭС учетным записям, выделенным для сотрудников правоохранительных и контрольно-надзорных органов
Подмодуль доступа к Единой децентрализованной базе данных клиентов субъектов Закона № 115-ФЗ	Получение информации из Единой децентрализованной базы данных клиентов субъектов Закона № 115-ФЗ о результатах прохождения процедуры идентификации клиентов, их представителей, выгодоприобретателей и бенефициарных владельцев
Встраиваемый модуль ЕАС ПОД/ФТ	
Подмодуль автоматизированного направления ФЭС об ОПОК, заблокированных операциях и выявленных ЕАС ПОД/ФТ подозрительных операциях, а также предоставления рекомендаций по блокированию финансовых операций	Выявление ОПОК, подозрительных операций и направление в их отношении, а также в связи с замораживанием денежных средств ФЭС в центральную часть ЕАС ПОД/ФТ. Предоставление должностным лицам субъектов Закона № 115-ФЗ рекомендаций по блокированию денежных средств лиц, в финансовых операциях которых наблюдаются очевидные признаки ОД/ФТ
Подмодуль ручного ввода для ФЭС о подозрительных операциях, а также в иных случаях, предусмотренных Законом № 115-ФЗ и принятыми в соответствии с ним подзаконными актами	Ручной ввод данных для направления ФЭС, а также направление данных ФЭС в центральную часть ЕАС ПОД/ФТ
Подмодуль ответов на запросы Росфинмониторинга	Получение, поиск необходимой информации и направление ответа в центральную часть ЕАС ПОД/ФТ
Подмодуль проверки прохождения клиентом идентификации	Направление запросов в Единую децентрализованную базу данных клиентов субъектов Закона № 115-ФЗ
Подмодуль направления запросов в государственные органы	Направление запросов в государственные органы в целях проверки сведений, представленных клиентом

Продолжение таблицы Б.1

1	2
Подмодуль направления запросов в государственные органы	Направление запросов в государственные органы в целях проверки сведений, представленных клиентом
Подмодуль автоматизированного определения уровня риска ОД/ФТ в действиях клиента	Автоматизированный мониторинг операций клиента, которые в сочетании с определенными регистрационными данными могут указывать на незаконный характер его деятельности
Подмодуль направления результатов идентификации	Ручной ввод результатов идентификации клиента, его представителей, выгодоприобретателей и бенефициарных владельцев и загрузка результатов в Единую децентрализованную базу данных клиентов Закона № 115-ФЗ
Подмодуль блокирования денежных средств	Автоматизированное приостановление финансовых операций по счетам физических и юридических лиц, внесенных в перечни лиц, средства которых подлежат замораживанию
Подмодуль взаимодействия с контрольно-надзорными и правоохранительными органами	Взаимодействие с контрольно-надзорными органами в части предоставления информации о направленных ФЭС и документации об организации системы внутреннего контроля в отношении ПОД/ФТ, а также с правоохранительными органами в части доступа к базе данных ФЭС

Источник: составлено автором.

Приложение В

(информационное)

Формула для расчета среднегодовой суммы штрафа по статье 15.27 КоАП РФ после внедрения ЕАС ПОД/ФТ

Формула для расчета среднегодовой суммы штрафа по статье 15.27 КоАП РФ после внедрения ЕАС ПОД/ФТ представлена на Рисунке В.1.

Формула для расчета среднегодовой суммы штрафа по статье 15.27 КоАП РФ после внедрения ЕАС ПОД/ФТ

$$F_1 = F_0 - F_0 \cdot \frac{N_1}{P} - F_0 \cdot \frac{N_2}{k \cdot P} = 104 - 104 \cdot \frac{2}{8} - 104 \cdot \frac{3}{2 \cdot 8} = 104 - 26 - 19{,}5 = 58{,}5 \text{ (тыс. рублей)}$$

F_1 – значение среднегодовой суммы штрафа по статье 15.27 КоАП РФ после внедрения ЕАС ПОД/ФТ

F_0 – значение среднегодовой суммы штрафа по статье 15.27 КоАП РФ за период 2015-2022 гг.

N_1 – количество составов правонарушений, по которым субъекты Закона № 115-ФЗ не будут привлекаться к ответственности после внедрения ЕАС ПОД/ФТ

N_2 – количество составов правонарушений, по которым субъекты Закона № 115-ФЗ частично не будут привлекаться к ответственности после внедрения ЕАС ПОД/ФТ

N_2 – количество составов правонарушений, по которым субъекты Закона № 115-ФЗ частично не будут привлекаться к ответственности после внедрения ЕАС ПОД/ФТ

P – количество составов правонарушений, предусмотренных статьей 15.27 КоАП РФ

k – коэффициент, учитывающий частичность снятия ответственности

Источник: составлено автором.

Рисунок В.1 – Формула для расчета среднегодовой суммы штрафа по статье 15.27 КоАП РФ после внедрения ЕАС ПОД/ФТ

Приложение Г

(информационное)

Формула для расчета текущих расходов субъектов Закона № 115-ФЗ, связанных с функционированием механизма мониторинга ПОД/ФТ

Формула для расчета текущих расходов субъектов Закона № 115-ФЗ, связанных с функционированием механизма мониторинга ПОД/ФТ представлена на Рисунках Г.1-Г.3.

Формула для расчета текущих расходов субъектов Закона № 115-ФЗ, связанных с функционированием механизма мониторинга ПОД/ФТ

$$E = E_{M\_SUS} + E_{M\_OBL} + E_{M\_REF} + E_{M\_B} + E_{M\_etc} + E_S + E_F + E_I + E_B + E_{REF} + E_{REQ}$$

E_{M_SUS} – расходы на направление ФЭС о подозрительных операциях и подозрительной деятельности

E_{M_OBL} – расходы на направление ФЭС об операциях, подлежащих обязательному контролю

E_{M_REF} – расходы на направление ФЭС о случаях отказа от заключения договора и осуществления операций в случае наличия подозрений о причастности деятельности клиента к ОД/ФТ

E_{M_B} – расходы на направление ФЭС о случаях блокирования денежных средств

Источник: составлено автором.

Рисунок Г.1 – Формула для расчета текущих расходов субъектов Закона № 115-ФЗ, связанных с функционированием механизма мониторинга ПОД/ФТ (начало)

Формула для расчета текущих расходов субъектов Закона № 115-ФЗ, связанных с функционированием механизма мониторинга ПОД/ФТ

$$E = E_{M\_SUS} + E_{M\_OBL} + E_{M\_REF} + E_{M\_B} + E_{M\_etc} + E_S + E_F + E_I + E_B + E_{REF} + E_{REQ}$$

E_{M_etc} – расходы, связанные с предоставлением ФЭС в иных случаях, предусмотренных Законом № 115-ФЗ и нормативно-правовыми актами контрольно-надзорных органов

E_S – расходы, связанные с осуществлением контроля (надзора) в отношении субъектов Закона № 115-ФЗ, в том числе на направление информации в отношении контрольно-надзорных органов, а также на сопровождение выездных проверок

E_F – расходы, связанные с уплатой штрафов, а также иными мерами ответственности за несоблюдение мер Закона № 115-ФЗ (данный параметр опционален и зависит от уровня правовой культуры и ресурсов организации, направленных на выполнение требований Закона № 115-ФЗ)

E_I – расходы, связанные с осуществлением идентификации клиентов и определения их бенефициарных владельцев

Источник: составлено автором.

Рисунок Г.2 – Формула для расчета текущих расходов субъектов Закона № 115-ФЗ, связанных с функционированием механизма мониторинга ПОД/ФТ (продолжение)

Формула для расчета текущих расходов субъектов Закона № 115-ФЗ, связанных с функционированием механизма мониторинга ПОД/ФТ

$$E = E_{M\_SUS} + E_{M\_OBL} + E_{M\_REF} + E_{M\_B} + E_{M\_etc} + E_S + E_F + E_I + E_B + E_{REF} + E_{REQ}$$

E_B – расходы, связанные с замораживанием денежных средств клиентов

E_{REF} – расходы, связанные с отказом от заключения договора с клиентом или проведения операций в случае наличия подозрений о связи с ОД/ФТ

E_{REQ} – расходы, связанные с составлением ответов на запросы Росфинмониторинга

Рисунок Г.3 – Формула для расчета текущих расходов субъектов Закона № 115-ФЗ, связанных с функционированием механизма мониторинга ПОД/ФТ (окончание)

Приложение Д

(информационное)

Формула для расчета расходов субъектов Закона № 115-ФЗ, связанных с функционированием механизма мониторинга ПОД/ФТ, после внедрения ЕАС ПОД/ФТ

Формула для расчета расходов субъектов Закона № 115-ФЗ, связанных с функционированием механизма мониторинга ПОД/ФТ, после внедрения ЕАС ПОД/ФТ представлена на Рисунках Д.1-Д.3.

Формула для расчета расходов субъектов Закона № 115-ФЗ, связанных с функционированием механизма мониторинга ПОД/ФТ, после внедрения ЕАС ПОД/ФТ

$$E^* = E^*_{M\_SUS} + E^*_{M\_REF} + E_{M\_etc} + E^*_S + E^*_F + E^*_l + E^*_{REF} + E_{IAS}$$

$E^*_{M\_SUS}$ – расходы на направление ФЭС о подозрительных операциях и подозрительной деятельности (должны снизиться в связи с частичной автоматизацией обязанностей системой ЕАС ПОД/ФТ и производным от этого снижением издержек)

$E^*_{M\_REF}$ – расходы на направление ФЭС о случаях отказа от заключения договора и осуществления операций в случае наличия подозрений о причастности деятельности клиента к ОД/ФТ (должны снизиться в связи с частичной автоматизацией обязанностей системой ЕАС ПОД/ФТ и производным от этого снижением издержек)

E_{M_etc} – расходы, связанные с предоставлением ФЭС в иных случаях, предусмотренных Законом № 115-ФЗ и нормативно-правовыми актами контрольно-надзорных органов

Источник: составлено автором.

Рисунок Д.1 – Формула для расчета расходов субъектов Закона № 115-ФЗ, связанных с функционированием механизма мониторинга ПОД/ФТ, после внедрения ЕАС ПОД/ФТ (начало)

Формула для расчета расходов субъектов Закона № 115-ФЗ, связанных с функционированием механизма мониторинга ПОД/ФТ, после внедрения ЕАС ПОД/ФТ

$$E^* = E^*_{M\_SUS} + E^*_{M\_REF} + E_{M\_etc} + E^*_S + E^*_F + E^*_l + E^*_{REF} + E_{IAS}$$

E^*_S – расходы, связанные с осуществлением контроля (надзора) в отношении субъектов Закона № 115-ФЗ, в том числе на направление информации в отношении контрольно-надзорных органов, а также на сопровождение выездных проверок (должны снизиться в связи с частичной автоматизацией обязанностей системой ЕАС ПОД/ФТ и производным от этого снижением издержек)

E^*_F – расходы, связанные с уплатой штрафов, а также иными мерами ответственности за несоблюдение мер Закона № 115-ФЗ (должны снизиться в связи с частичной автоматизацией обязанностей системой ЕАС ПОД/ФТ и производным от этого снижением издержек)

E^*_l – расходы, связанные с осуществлением идентификации клиентов и определения их бенефициарных владельцев (должны снизиться в связи с частичной автоматизацией обязанностей системой ЕАС ПОД/ФТ и производным от этого снижением издержек)

Источник: составлено автором.

Рисунок Д.2 – Формула для расчета расходов субъектов Закона № 115-ФЗ, связанных с функционированием механизма мониторинга ПОД/ФТ, после внедрения ЕАС ПОД/ФТ (продолжение)

Формула для расчета расходов субъектов Закона № 115-ФЗ, связанных с функционированием механизма мониторинга ПОД/ФТ, после внедрения ЕАС ПОД/ФТ

$$E^* = E^*_{M\_SUS} + E^*_{M\_REF} + E_{M\_etc} + E^*_S + E^*_F + E^*_l + E^*_{REF} + E_{IAS}$$

E^*_{REF} – расходы, связанные с отказом от заключения договора с клиентом или проведения операций в случае наличия подозрений о связи с ОД/ФТ (должны снизиться в связи с частичной автоматизацией обязанностей системой ЕАС ПОД/ФТ и производным от этого снижением издержек)

E_{IAS} – расходы на внедрение и обслуживание системы ЕАС ПОД/ФТ

Рисунок Д.3 – Формула для расчета расходов субъектов Закона № 115-ФЗ, связанных с функционированием механизма мониторинга ПОД/ФТ, после внедрения ЕАС ПОД/ФТ (окончание)

Приложение Е

(информационное)

Признаки подозрительности операций с цифровыми валютами и цифровыми финансовыми активами

Признаки подозрительности операций с цифровыми валютами представлены в таблице Е.1.

Таблица Е.1 – Признаки подозрительности для операций с цифровыми валютами

Код признака	Описание признака
1	2
«51	Признаки необычных сделок при совершении операций с цифровыми валютами
5101	Множественные зачисления на цифровой кошелек с разных адресов на незначительные суммы (возможная связь с использованием «криптовалютных миксеров»)
5102	Множественные переводы с одного цифрового кошелька на различные цифровые кошельки на незначительные суммы (возможная связь с использованием «криптовалютных миксеров»)
5103	Наличие операции (получение цифровой валюты или перевод цифровой валюты) с цифровым кошельком, идентифицированного, как связанного с незаконной деятельностью
5104	Осуществление конвертации в цифровую валюту, функционал которой связан с затруднением процесса идентификации владельца цифровой валюты и отслеживания цепочки переводов цифровой валюты
5105	Осуществление конвертации из цифровой валюты, функционал которой связан с затруднением процесса идентификации владельца цифровой валюты и отслеживания цепочки переводов цифровой валюты
5106	Осуществление множественных операций по конвертации между различными цифровыми валютами за незначительный период времени в отсутствие экономической выгоды
5107	Осуществление конвертации из фиатных валют в цифровые и обратно за незначительный период времени
5108	Получение перевода цифровых валют от адресата, осуществляющего многочисленные операции по конвертации цифровых валют в отсутствие экономической выгоды
5109	Осуществление перевода цифровых валют получателю, осуществляющему многочисленные операции по конвертации цифровых валют в отсутствие экономической выгоды» [236, с. 10-11]

Продолжение таблицы Е.1

1	2
«5110	Получение юридическими лицами, личным законом которых является российское право, филиалами, представительствами и иными обособленными подразделениями международных организаций и иностранных юридических лиц, компаний и других корпоративных образований, обладающих гражданской правоспособностью, созданными на территории Российской Федерации, физическими лицами-гражданами Российской Федерации и физическим лицами, проживающими на постоянной основе в Российской Федерации, переводов в цифровой валюты, если в таких переводах присутствуют признаки оплаты за товары, работы, услуги
5111	Осуществление множественных операций, связанных с переводом цифровых валют между собственными цифровыми кошельками, за незначительный период времени
5199	Иные признаки, свидетельствующие о возможном осуществлении легализации (отмывания) доходов, полученных преступным путем, или финансировании терроризма» [236, с. 11]

Источник: составлено автором и опубликовано [236, с. 10-11].

Признаки подозрительности операций с цифровыми финансовыми активами представлены в таблице Е.2.

Таблица Е.2 – Признаки подозрительности для операций с цифровыми финансовыми активами

Код признака	Описание признака
1	2
«52	Признаки необычных сделок при совершении операций с цифровыми финансовыми активами
5201	Осуществление купли/продажи цифровых финансовых активов по стоимости, значительно отличающейся от стоимости ценных бумаг, возможность осуществления прав по которым удостоверяют цифровые финансовые активы
5202	Совершение взаимных сделок с цифровыми финансовыми активами, когда стороны таких сделок регулярно меняются, выступая в качестве то продавцов, то покупателей, приобретая/продавая при этом единовременно или по частям одни и те же цифровые финансовые активы примерно одного и того же объема
5203	Покупка/продажа цифровых финансовых активов с использованием цифровых валют, функционал которых связан с затруднением процесса идентификации владельца цифровой валюты и отслеживания цепочки переводов цифровой валюты
5204	Осуществление расчетов между сторонами сделки с цифровым финансовым активом с использованием расчетных счетов, открытых в кредитных организациях, зарегистрированных за пределами Российской Федерации
5299	Иные признаки, свидетельствующие о возможном осуществлении легализации (отмывания) доходов, полученных преступным путем, или финансировании терроризма» [236, с. 11]

Источник: составлено автором и опубликовано [236, с. 11].