Владимир Васильевич Земсков

доктор экономических наук, профессор департамента экономической безопасности и управления рисками Финансового университета при Правительстве РФ, г. Москва, VVZemskov@fa.ru

ВЫЯВЛЕНИЕ НЕОБЫЧНЫХ ОПЕРАЦИЙ КАК ЧАСТЬ ДЕЯТЕЛЬНОСТИ АГЕНТОВ СИСТЕМЫ ПОД/ФТ

Аннотация. В настоящем исследовании анализируются проблемы выявления необычных и подозрительных операций субъектами финансового мониторинга в ходе противодействия легализации доходов и финансированию терроризма. Сложность выявления необычных и подозрительных операций заключается в том, что преступники постоянно разрабатывают новые методы и стратегии для скрытия своих финансовых транзакций, что требует от субъектов финансового мониторинга постоянного обновления и совершенствования своих методов анализа и мониторинга. Актуальность этой проблемы продолжает возрастать, поскольку в условиях мировой глобализации и развития технологий, преступники все время совершенствуют способы перевода финансовых средств и укрывания активов в офшорных юрисдикциях.

Ключевые слова: необычные операции, подозрительные операции, признаки необычных операций, жизненный цикл необычной операции, поведенческий профиль, анкета (досье) клиента, субъекты финансового мониторинга.

Vladimir Vasilevich Zemskov

Doctor of Economic Sciences, Professor, Department "Economic security and risk management", Financial University under the Government of the Russian Federation, Moscow, VVZemskov@fa.ru

IDENTIFICATION OF UNUSUAL OPERATIONS AS PART OF THE ACTIVITIES OF AML/CFT SYSTEM AGENTS

Abstract. This study analyzes the problems of identifying unusual and suspicious transactions by financial monitoring entities in the course of countering money laundering and terrorist financing. The difficulty in detecting unusual and suspicious transactions lies in the fact that criminals are constantly developing new methods and strategies to hide their financial transactions. This requires financial monitoring entities to constantly update and improve their methods of analysis and monitoring. The urgency of this problem continues to increase, because in the context of global globalization and the development of technology, criminals are constantly improving ways to transfer funds and hide assets in offshore jurisdictions.

Keywords: unusual transactions, suspicious transactions, signs of unusual transactions, the life cycle of an unusual transaction, behavioral profile, client profile (dossier), subjects of financial monitoring.

Финансовые преступления являются одним из самых распространенных видов преступной деятельности в современном обществе. Они охватывают широкий спектр действий, направленных на незаконное получение финансовой выгоды и нарушение финансовой стабильности. Они представляют собой серьезную угрозу для экономической безопасности как отдельных лиц, так и для всего общества. Эти преступления включают в себя различные виды мошенничества, коррупции, легализации денег, уклонения от уплаты налогов и другие деяния, направленные на незаконное обогащение за счет неправомерного распоряжения финансовыми активами. Одним из признаков финансовых преступлений является необычный характер операций [1].

В научной литературе приводится обобщенная классификация обычных операций для целей финансового учета и признаки необычных операций

в сфере ПОД/ФТ. Автор ранее уже рассматривал сущность обычных и необычных операций, совершаемых в процессе осуществления обычного вида деятельности [2], первый из которых определяется на основании требований положения по бухгалтерскому учету «Доходы организации» ПБУ 9/99. Напомним, что к обычным видам деятельности хозяйствующего субъекта относятся: выручка от производства и реализации продукции; операции по закупке сырья, необходимого для текущего производственного процесса и реализации продукции; получение кредитных средств для текущей деятельности. Кроме того, признаком обычных операций является постоянное совершение операций, необходимых для обеспечения непрерывной деятельности.

К необычным операциям для целей финансового учета относятся операции, выходящие за пределы обычного вида деятельности: совершение крупной сделки, увеличение масштабов деятельности за счет диверсификации, реорганизация и т. д.

В настоящее время не существует единого определения понятия «необычные операции в целях ПОД/ФТ», которое было бы закреплено на законодательном уровне, но данный вопрос нашел отражение во многих документах международных организаций и российского ЦБ. Так, Базельский комитет по банковскому надзору под необычными операциями понимает «Операции, которые носят необычных или запутанный характер, выделяющиеся необычно крупными суммами денежных средств и необычными схемами их оборота, не имеющие очевидной экономической или законной цели» [3].

Росфинмониторинг под необычными операциями понимает «сделку, которая имеет необычный или запутанный характер, не имеющая очевидного экономического смысла или очевидной законной цели, и которые вызывают подозрение у правоохранительных органов» [4].

ЦБ РФ под необычными операциями понимает «операции, осуществляемые клиентами кредитных организаций, имеющие необычный характер и признаки отсутствия явного экономического смысла и очевидных законных целей, которые могут проводиться для вывода капитала из страны, финансирования "серого" импорта, перевода денежных средств из безналичной в наличную форму и последующего ухода от налогообложения, а также для финансовой поддержки коррупции и других противозаконных целей» [5].

Итак, из приведенных определений можем сформулировать признаки необычных операций в сфере противодействия (легализации) отмыванию преступных доходов:

- не имеют экономической цели совершения операции;
- запутанный характер операции;
- крупная сумма сделки;
- обналичивание денежных средств.

Несмотря на многочисленность определений они разделяют смысл: необычные операции — это индикатор, один из инструментов, закладывающих фундамент риск-ориентированному подходу в ПОД/ФТ.

Угрозы отмывания доходов реализовываются злоумышленниками при помощи нескольких операций, которые сложно идентифицировать в общем их объеме. Так, за 9 месяцев 2023 г. при помощи одних только карт кредитных

организаций было совершено более 56 млрд операций. Субъекты финансового мониторинга не могут осуществлять надзор за каждой операцией своих клиентов. Приостановление обслуживания до момента полного разбирательства и другие подобные процедуры по каждой транзакции, сведут эффективность работы надзорных органов на нет. Поэтому необходимо определить специальные признаки, в виде пороговых значений, различных индикаторов — «красных флагов», сосредоточившись на которых субъекты финансового мониторинга смогут направить их ограниченные надзорные ресурсы на самые рискованные операции и при этом бесперебойно продолжать свою деятельность. К таким признакам относятся: размер операции, после превышения которого субъект финансового мониторинга должен провести обязательный контроль, типологии отмывочных операций (необычные операции), требующие анализа и др.

Перечень признаков («красных флагов») дается Росфинмониторингом в Приказе № 103 «Об утверждении Рекомендаций по разработке критериев выявления и определению признаков необычных сделок». На данный момент он утратил силу, но не потерял своего методологического значения. Примером этому служит Положение Банка России от 2 марта 2012 г. № 375-П «О требованиях к правилам внутреннего контроля кредитной организации в целях ПОД/ФТ», находящееся в силе, в котором ЦБ РФ использовал, разработанный Росфинмониторингом перечень подозрительных операций, но для подотчетных ему кредитных организаций.

Опираясь на вышеуказанные документы, в схематичном виде можно представить жизненный цикл необычной сделки, представленный на рис. 1.

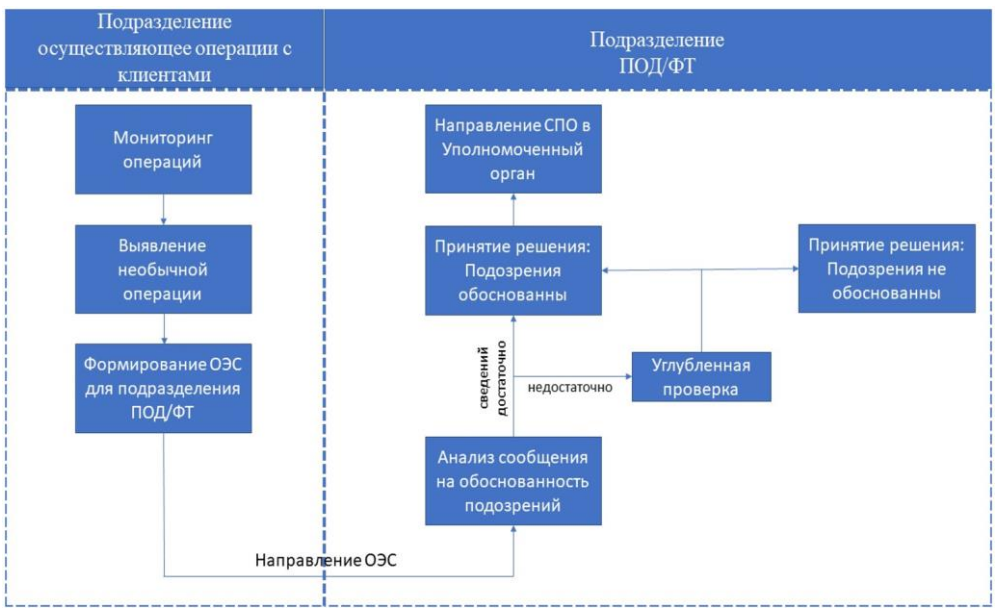

Рис. 1. Жизненный цикл необычной операции

Источник: составлено автором по данным [6].

Используя классификаторы ЦБ РФ, Ассоциации банков России или собственные классификаторы (разработанные сотрудником финансового мониторинга), можно выявлять признаки необычных операций [7]. Затем, не позднее следующего дня, исполнитель-контролер, выявивший признаки необычных операций, должен составить отчет в виде электронного сообщения (ОЭС) и отправить его в подразделение, ответственное за ПОД/ФТ.

Направленное в подразделение сообщение визируется Ответственным сотрудником для принятия решения: классифицировать ли эту операцию как подозрительную. В случае, если сведений, предоставленных сотрудником, выявившим операцию, недостаточно, Ответственный сотрудник может инициировать углубленную проверку. Ее итогом должно стать подтверждение или опровержение возникших подозрений. В ходе углубленной проверки могут проводиться следующие мероприятия:

– запрашивать дополнительную информацию у сотрудника, выявившего признаки необычных операций (документы, подтверждающие право возникновения собственности на активы в результате использования специальных финансовых инструментов: договора новации, факторинга, акты взаимозачета и др.);

– требовать письменные пояснения от руководителя структурного подразделения, ответственного за совершение финансовой операции;

– запрашивать информацию о периодичности обновления данных о контрагентах, поставщиках, бенефициарных владельцах;

– проводить проверку соответствия цели финансовой операции кодам ОКВЭД и другие мероприятия.

В России проводятся различные исследования для оценки уровня распространения финансовых преступлений. Одним из таких исследований является анализ данных правоохранительных органов, официальной статистики о преступности, а также проведение опросов и анкетирование населения и предпринимателей.

Если рассматривать данные, размещенные на официальном сайте МВД, то за первый квартал 2023 года правоохранительные органы выявили 45 829 экономических преступлений, куда входят и совершенные финансовые преступления. Это приблизительно на 4 000 меньше, чем за аналогичный период в прошлом году.

В период за январь-сентябрь в 2023 году было выявлено экономических преступлений на сумму 87,8 тыс. рублей, из них следствие обязательно на 77,3 тыс. рублей (см. рис. 2).

Основным направлением совершенствования программы выявления необычных операций субъектами финансового мониторинга автор считает обеспечение специальных подразделений всей необходимой информацией для вынесения обоснованных решений о подозрительности операций. Ссылаясь на статистику, приведенную экспертами ФАТФ, Росфинмониторинг ежедневно получает порядка 55 000 СПО. Каждое из них представляет дело для возможного финансового расследования. С этой целью необходимо повысить качество анализа операций, что приведет к их фильтрации еще на этапе рассмотрения в подразделении ПОД/ФТ субъекта финансового мониторинга. С этой целью органам контроля необходимо разработать общие базы данных по своим клиентам, которые позволили бы достовернее проводить углубленную проверку, а значит формировать более качественные СПО.

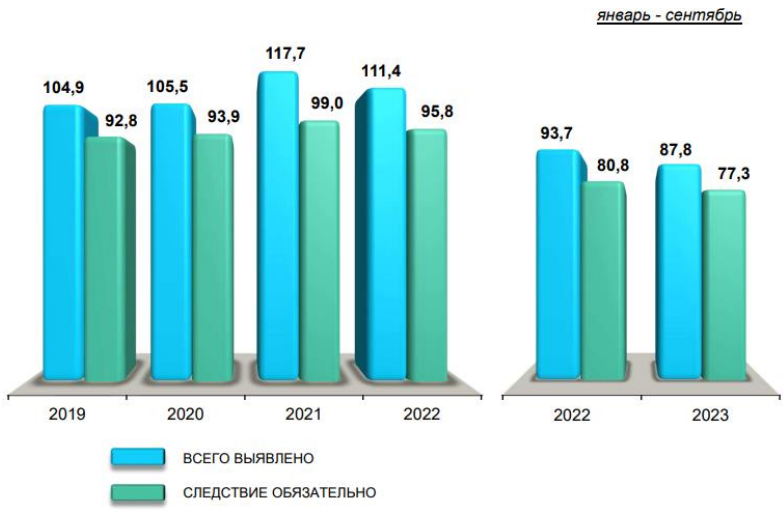

Рис. 2. Выявленные финансовые преступления экономической направленности, тыс. руб.

Источник: составлено автором по данным [8].

Другим не менее важным направлением является внедрение современных технологий в этот бизнес-процесс. Например, искусственный интеллект (ИИ) представляет собой самую привлекательную перспективу, способную значительно повысить эффективность ответственных сотрудников. Используя машинное обучение, можно «научить ИИ»:

– распознавать подозрительные триггеры, которые могли быть не замечены сотрудником. Под триггерами в контексте данного исследования понимаются оставленные «следы» в информационной системе, которые могут носить как положительный, так и отрицательный характер. Следует отметить, что положительные триггеры благоприятно влияют на финансовые результаты хозяйственной деятельности, обеспечивают максимальную величину добавленной стоимости. При этом отрицательные триггеры, наоборот снижают эффективность хозяйственной деятельности за счет совершения мошеннических действий, уклонения от уплаты налоговых платежей, хищения бюджетных средств, перевод безналичных денежных средств в наличную форму и т. д.;

– помогать сотруднику выносить решение о подозрительности после анализа доступной информации.

Последние отчеты о проверке рисков отмывания доходов международными организациями ФАТФ и ЕАГ, рекомендуют внедрять современные методы выявления необычных операций, одним из которых является внедрение поведенческого профиля клиента, контрагента, поставщиков. Это очень важно, так как внедрение процессов поведенческого профиля клиента в деятельность субъектов финансового мониторинга, обеспечивает выполнение поручения Президента РФ (перечень поручений по реализации послания Президента РФ Федеральному собранию 24.02.2024) по переходу от выездных проверок на осуществление профилактических мероприятий по хозяйствующим субъектам, имеющим средний и низкий риск отмывания доходов.

В экономике триггер в первую очередь рассматривается как фактор (риск, событие), содержащий определенные признаки, по которым можно будет выявить и оценить эти факторы [9]. Отсюда основными задачами специалистов финансового мониторинга хозяйствующего субъекта являются:

– выявление и установление поведенческих триггеров в целях противодействия отмыванию незаконных доходов;

– организация поведенческого контроля на основе разработки правил и стандартов поведения контрагентов и сотрудников хозяйствующего субъекта [10].

Несомненно, перечень потенциальных поведенческих факторов, по мнению автора, должен быть прописан в локальных внутренних документах (программа внутреннего контроля, Кодекс корпоративного поведения и других документах). Примерная матрица потенциальных поведенческих факторов может выглядеть следующим образом (табл. 1).

Таблица 1

Матрица потенциальных поведенческих факторов

Виды факторов	*Смысловое содержание факторов*	*Примеры обстоятельств*
Мотивация	Может возникнет вследствие финансовых затруднений правонарушителя	- желание получения необоснованных материальных ценностей или услуг; - получение займа в кредитных или парабанковских организациях; - отсутствие гарантии занятости в организации-работодателя
Способность	Может возникнет, когда предыдущее суждение должно быть переоценено субъектом управления, ранее вынесшим это суждение	- умение войти в сговор с «нужными» людьми; - распознание среды, в которой возможно совершение преступления; - уверенность в собственных силах
Возможность	Может возникнет, когда делегирование полномочий не соответствует организационной структуре	- отсутствие контроля или ненадлежащий контроль за осуществлением фактов хозяйственной деятельности; - контрольная процедура не охватывает существенные бизнес-процессы; - знание слабых сторон системы внутреннего контроля
Осведомленность	Может возникнет, когда не обеспечивается сохранность персональных данных и коммерческой тайны	- наличие у правонарушителя намерения нарушить правила поведения; - принимает на себя возможные риски ответственности за совершение правонарушения

Источник: разработано автором.

Как видно по данным указанной таблицы, матрица потенциальных поведенческих факторов может базироваться на четырехугольнике мошенничества, представленный на рис. 1. Но при этом каждый хозяйствующий субъект,

исходя из масштабов и видов деятельности, может разрабатывать другие факторы, влияющие на поведенческие действия контрагентов, клиентов, поставщиков и сотрудников хозяйствующего субъекта.

Сведения о поведенческих действиях контрагентов, клиентов, поставщиков необходимо отразить в анкете (досье) клиентов, которые будут свидетельствовать о наличии потенциальных возможностей в их негативном поведении.

Подводя итог, можно сказать, что выявление необычных и подозрительных операций субъектами финансового мониторинга в ходе ПОД/ФТ является одним из ключевых аспектов антиотмывочной системы. Эффективные методы и технологии, применяемые для выявления подозрительных операций, играют важную роль в поддержании стабильности финансовой системы, предотвращении преступной деятельности и обеспечении безопасности граждан и страны в целом.

С появлением и развитием новых технологий и цифровизации деятельности человека появляется все больше способов и инструментов организации незаконной легализации доходов. Именно поэтому необходимо постоянно обмениваться опытом и практиками контроля за финансовой сферой с целью обеспечения развития системы противодействия отмыванию доходов во всем мире и повышения эффективности пресечения подобных преступлений.

Постоянное совершенствование методов и технологий в этой области является ключевым аспектом обеспечения финансовой безопасности и защиты интересов общества.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Рогатенюк Э.В. Сущность и виды необычных операций / Э.В. Рогатенюк // Экономика строительства и природопользования. — 2019. — № 3 (72). — С. 89-95. – URL: https://cyberleninka.ru/article/n/suschnost-i-vidy-neobychnyh-operatsiy/viewer (дата обращения: 17.02.2024).
2. Земсков В.В. Оценка рисков необычных операций в процедурах внутреннего контроля / В.В. Земсков // Аудитор. — 2000. — № 3. — С. 19-25.
3. Базельский Комитет: BIS: сайт. — URL: https://www.bis.org/BCBS/ (дата обращения: 03.04.2024).
4. Федеральная служба по финансовому мониторингу: официальный сайт. — URL: http://www.fedsfm.ru/ (дата обращения: 03.04.2024).
5. Банк России: официальный сайт — URL: https://www.cbr.ru/ (дата обращения: 03.04.2024).
6. Типовые правила внутреннего контроля кредитной организации (утв. АРБ) (ред. от 13.03.2013) // КонсультантПлюс. — URL: http://www.consultant.ru/document/cons_doc_LAW_52144/ (дата обращения: 26.01.2023).
7. Аникина И.Д. Современные механизмы контроля и аудита финансовых рисков банков / И.Д. Аникина, А.С. Алтамими // Научное обозрение: теория и практика. — 2022. — Т. 12, вып. 4. — С.1307-1311.
8. Министерство внутренних дел: официальный сайт. — URL: https://мвд.рф/reports/item/42989123/?ysclid=ltbg7r4c5r937212306 (дата обращения: 03.04.2024).
9. Суровцева В.В. Поведенческий контроль и поведенческие риски в коммерческом банке / В.В. Суровцева // Экономика и предпринимательство. — 2019. — № 4. — С. 1307-1311.
10. Деминг Э. Выход из кризиса. Новая парадигма управления людьми, системами и процессами. пер. с англ. — Москва: Альпина Паблишер, 2019. — 417 с.