

Создание эффективного государственно-частного партнерства в противодействии финансированию терроризму



Исполнительный Директорат
Контртеррористического Комитета Совета Безопасности
Организации Объединенных Наций (ИДКТК)

Аналитическая
справка ИДКТК
Декабрь 2023

Содержание

ПРЕДИСЛОВИЕ И МЕТОДОЛОГИЯ	3
ОБЗОР	4
ОСНОВЫ ГОСУДАРСТВЕННО-ЧАСТНОГО ПАРТНЕРСТВА	8
Обмен стратегической информацией.....	11
Оперативные партнерства	12
Условия выстраивания партнерства	13
УСТРАНЕНИЕ ПРОБЕЛОВ И ПРОБЛЕМ, ВЫЯВЛЕННЫХ В РАМКАХ ГЧП	15
Недостаток ресурсов и потенциала	15
Ограничение сферы применения ГЧП традиционными финансовыми институтами	16
Нечеткая нормативно-правовая база.....	18
Односторонняя связь и ограничения на обратную связь и рекомендации	20
Непредвиденные последствия, включая влияние на права человека	21
Использование новых или развивающихся технологий для обмена информацией с частным сектором	24
ЗАКЛЮЧЕНИЕ	26

Авторские права @ Исполнительный Директорат Контртеррористического Комитета СБ ООН

Перевод с английского языка на русский язык подготовлен Антитеррористическим центром государств – участников СНГ

Фотографии: [iStock.com/metamorworks](https://www.iStock.com/metamorworks) & [iStock.com/matdesign24](https://www.iStock.com/matdesign24)

Декабрь 2023

ПРЕДИСЛОВИЕ И МЕТОДОЛОГИЯ

Настоящая аналитическая справка подготовлена Исполнительным директором Контртеррористического комитета (ИДКТК) в соответствии с резолюцией 2395 (2017), в которой Совет Безопасности поручает ИДКТК проводить аналитическую работу по возникающим проблемам, тенденциям и событиям и предоставлять свои аналитические материалы в рамках всей системы Организации Объединенных Наций. В дальнейшем в своей резолюции 2617 (2021) Совет подтвердил важную роль, которую ИДКТК играет в Организации Объединенных Наций в выявлении и оценке проблем, тенденций и событий, связанных с выполнением соответствующих контртеррористических резолюций, включая резолюцию 2462 (2019) о противодействии финансированию терроризма (ПФТ).

Аналитические справки ИДКТК предназначены для предоставления Контртеррористическому комитету Совета Безопасности, учреждениям Организации Объединенных Наций и руководителям краткого анализа конкретных проблем, тенденций и событий, выявленных в ходе взаимодействия ИДКТК с государствами-членами по вопросу выполнения ими соответствующих резолюций Совета. Они также включают данные, собранные ИДКТК, в том числе посредством взаимодействия с его партнерами по Организации Объединенных Наций; международными, региональными и субрегиональными организациями; организациями гражданского общества (ОГО); и членами Глобальной исследовательской сети ИДКТК (ГИС).

Настоящая аналитическая справка основана на информации, собранной в ходе взаимодействия ИДКТК с государствами-членами, в частности, в ходе оценочных визитов, проведенных ИДКТК от лица Контртеррористического комитета, которая также была проанализирована и отражена в открытых отчетах о пробелах в реализации ключевых положений резолюций Совета Безопасности по проблематике ПФТ.¹ Сбор данных также осуществлялся в ходе взаимодействия ИДКТК с партнерами Организации Объединенных Наций, международными и региональными организациями, включая Группу разработки финансовых мер борьбы с отмыванием денег (ФАТФ) и ее Глобальную сеть,² а также с ОГО, ГИС и

¹ ИДКТК, «Тематическая сводная оценка пробелов в реализации ключевых положений резолюций Совета Безопасности с области противодействия финансированию терроризма», декабрь 2022 г., доступ по ссылке: www.un.org/securitycouncil/ctc/content/thematic-summary-assessment-gaps-implementing-key-counteracting-financing-terrorism-provisions.

² Помимо ежегодного Консультативного форума частного сектора, ФАТФ реализует постоянную практику проведения консультаций с частным сектором в контексте своих аналитических уведомлений о тенденциях и/или разработки руководящих указаний по реализации политики. В рамках работы в соответствующих проектных группах ИДКТК также имел доступ к полученным отзывам.

структурами частного сектора,³ а также в процессе участия в соответствующих международных и региональных мероприятиях. В целях подготовки данной аналитической справки ИДКТК также провел ряд консультаций с экспертами из государств, в которых созданы государственно-частные партнерства (ГЧП), включая Французскую группу финансовых расследований (TRACFIN); Контртеррористический отдел Федерального полицейского управления Германии во взаимодействии с Институтом Макса Планка; Целевую группу по борьбе с финансированием терроризма при Центре финансовой экспертизы (FEC) в Королевстве Нидерландов; Сеть финансовой разведки Малайзии; и Western Union (Южная Африка).

Признавая необходимость в изучении эффективности и любых потенциальных непредвиденных последствий ГЧП в сфере ПФТ, а также отслеживании новых разработок в использовании новых и перспективных технологий в целях повышения эффективности реализации мер по борьбе с отмытием денег (ПОД)/мер ПФТ, ИДКТК будет продолжать прилагать усилия и работать на этом направлении.

ОБЗОР



Как Совет Безопасности, так и Контртеррористический комитет призывают национальные власти устанавливать партнерские отношения с частным сектором, включая финансовые учреждения, компании, работающие в области финансовых технологий (финтех-компании), а также интернет-компаниями и социально-сетевыми компаниями, в частности, в отношении эффективного внедрения отчетности и требований к раскрытию информации, использования и обмена соответствующей финансовой информацией с частным сектором, а также обмена информацией об изменении тенденций, источников и методов финансирования терроризма.⁴

Как отмечено в ряде рекомендаций и основных выводах ФАТФ, крайне важно, чтобы осуществлялся своевременный и эффективный обмен информацией о финансовой деятельности, которая может быть связана с преступностью и

³ Например, технические сессии под руководством ИДКТК на тему «Угрозы и возможности, связанные с новыми платежными технологиями и методами сбора средств», организованные в рамках подготовки к специальному заседанию Комитета в г. Дели (сентябрь 2022 г.); консультации ИДКТК по ряду необязательных руководящих принципов «Противодействие использованию новых и новейших технологий в террористических целях: угрозы и возможности, связанные с новыми платежными технологиями и методами сбора средств», май 2023 г.

⁴ Резолюция 2462 (2019) Совета Безопасности, п. 22; Делийская декларация о противодействии использованию новых и новейших технологий в террористических целях, октябрь 2022, п. 15 и 25.

терроризмом, между государственным и частным секторами. Соответствующий обмен информацией может позволить всем участникам отношений более эффективно использовать имеющиеся ресурсы и использовать новые технологии и бизнес-модели для разработки инновационных методов борьбы с отмыванием денег и финансированием терроризма.⁵ Учитывая большой спектр правовых и операционных проблем, связанных с обменом информацией между государственным и частным секторами, ФАТФ выпустила специальное руководство по этому вопросу, подчеркнув, среди прочего, что эффективные двусторонние отношения между государственным и частным секторами могут быть обеспечены, если у правоохранительных органов имеются соответствующие механизмы обмена стратегической, оперативной, тактической и целевой информацией с частным сектором.⁶

Частный сектор, включая финансовые учреждения и определенные нефинансовые предприятия и специальности, играет важную роль в ПФТ. В частном секторе есть подотчетные организации, которые в рамках деятельности, направленной на ПОД/ФТ, и по закону обязаны передавать информацию о подозрительной деятельности в подразделения финансовой разведки (ПФР) и/или правоохранительные органы. Затем эта информация анализируется и используется органами власти для предотвращения, выявления и пресечения преступлений, связанных с финансированием терроризма. Такая информация также важна для того, чтобы органы власти могли получить более полное представление о текущих и возникающих угрозах и тенденциях финансирования терроризма.

При том, что крупные банки традиционно были основными источниками информации, предоставляемой в рамках деятельности, направленной на ПОД/ФТ, в настоящее время появляется все больше компаний в сфере финансовых технологий, Интернета и социальных сетей, а также таких ключевых секторах экономики, как добыча и использование природных ресурсов, фармацевтика, недвижимость и строительство, которые могут не быть субъектами отчетности в государствах-членах, но уже давно стали надежным и зачастую недооцениваемым источником выявления перемещения средств, принадлежащих или предназначенных для террористов и террористических группировок. Надлежащее использование информации, которую они могут предоставлять, позволяет лучше выявлять террористические риски, отслеживать активы и определять место совершения транзакций, связанных с терроризмом.

⁵ ФАТФ, *Руководство по обмену информацией в частном секторе*, (Париж, 2017), доступ по ссылке: www.fatf-gafi.org/en/publications/Fatfgeneral/Guidance-information-sharing.html.

⁶ ФАТФ, *Руководство по обмену информацией в частном секторе*, (Париж, 2017), стр. 27, доступ по ссылке: www.fatf-gafi.org/en/publications/Fatfgeneral/Guidance-information-sharing.html.

На нескольких экспертных встречах, в которых участвовал ИДКТК,⁷ некоторые компании-платформы по сбору средств поделились своими взглядами на взаимодействие с сообществом, что важно для понимания клиентов и их сетей. Социально-сетевые компании и другие нефинансовые онлайн-сервисы также играют роль в отслеживании схем сбора средств и финансовых коммуникаций, например, благодаря знанию своих клиентов, при этом провайдеры платежных услуг обладают необходимой информацией для изучения сетей этих клиентов. В результате исследователи и партнеры из частного сектора подчеркнули необходимость сотрудничества и согласованности действий в регулировании деятельности финансовых учреждений (которые уже подлежат контролю в рамках ПОД/ФТ), краудфандинговых сайтов и социальных сетей (к которым было бы целесообразно применить принципы «знай своего клиента» (KYC) и требование надлежащей проверки клиента (CDD) в части касающейся сбора средств) как участников отношений, задействованных в одном и том же процессе и обладающих взаимодополняющей информацией. Некоммерческие организации и посреднические организации, предоставляющие услуги краудфандинга через специализированные платформы, а также социальные сети и приложения для обмена сообщениями признают, что сталкиваются с проблемами в части предотвращения и выявления злоупотреблений их услугами в целях финансирования терроризма. Следственные органы и прокуратура сталкиваются с аналогичными проблемами из-за сложного и псевдонимного характера транзакций.⁸

Быстрое развитие финансовых технологий не позволяет органам властям полагаться исключительно на соблюдение требований ПОД/ФТ, в частности, на сообщения о подозрительных транзакциях (СПО). Кроме того, характер финансирования терроризма, который может включать в себя транзакции на небольшие суммы, не достигающие пороговых значений для попадания на мониторинг или в отчетность, и при котором могут использоваться различные способы, позволяющие избежать выявления и сохранять анонимность, также привел к росту потребности со стороны частного сектора в получении дополнительных рекомендаций от ПФР, правоохранительных органов и других ведомств в части касающейся методов и тенденций финансирования терроризма, а также соответствующих индикаторов риска. В этом отношении ГЧП дает возможность расширить потенциал частного сектора по минимизации высоко

⁷ См., например, совместное экспертное совещание ФАТФ (апрель 2023 г., г. Дели); семинар по противодействию финансированию терроризма, проведенный под председательством Испании в Совете ЕС (сентябрь 2023 г., Мадрид).

⁸ Например, см. ФАТФ, *Использование краудфандинга для финансирования терроризма*, (Париж, 2023), доступ по ссылке: www.fatf-gafi.org/en/publications/Methodsandtrends/crowdfunding-for-terrorism-financing.html; и Азиатско-Тихоокеанская группа по борьбе с отмыванием денег (АТГ) и Целевая группа по финансовым мерам для стран Ближнего Востока и Северной Африки (МЕНАФАТФ), «Социальные сети и финансирование терроризма», январь 2019 г., доступ по ссылке: www.menafatf.org/sites/default/files/Newsletter/FINAL-TM-SF-en.pdf.

рискованной деятельности и, следовательно, улучшить поддержку со стороны органов власти в предотвращении и выявлении финансирования терроризма.

Хотя правительства склонны ожидать, что частный сектор будет осуществлять самоконтроль, адекватная база для этого зачастую отсутствуют. Чтобы избежать риск, частный сектор может прибегать к различным чрезмерным мерам, направленным на снижение рисков, таким как принудительное удаление профиля администрацией социальной сети (деплатформинг) и отказ в предоставлении других услуг, в то время как со стороны государственного сектора реакция в этом направлении либо минимальна, либо практически отсутствует. Помимо дискриминации, потенциальной маргинализации и нарушений прав человека, такая практика представляет собой упущенные возможности для сбора информации о подозреваемых лицах и сетях, потенциально вынуждая их переходить на платформы с затруднительным доступом (включая частные чаты). И наоборот, совместное определение основ работы позволяет частному сектору и регулирующим органам вместе выявлять риски и регулировать нормативную базу и рабочие механизмы на взаимопонятных условиях.

Кроме того, Совет Безопасности призвал к полному использованию новых и перспективных финансовых и регуляторных технологий для расширения финансовой доступности и содействия эффективной реализации мер ПОД/ФТ. Действительно, как показывает работа ФАТФ, новые технологии также обладают потенциалом, позволяющим ускорить, удешевить и повысить эффективность мер ПОД/ФТ как в государственном, так и в частном секторах. При ответственном и пропорциональном использовании технологии могут облегчить сбор, обработку и анализ данных, а также помочь субъектам выявлять риски финансирования терроризма и управлять ими более эффективно и практически в режиме реального времени. Это еще одна важная область, где надежное ГЧП имеет решающее значение.

Подход с участием различных участников отношений, то есть такой, который включает в себя различные государственные органы, частный сектор, гражданское общество и научные круги, является ключевым на всех этапах разработки и реализации мер ПФТ: от оценки рисков до разработки и внедрения риск-ориентированных мер и оценки их эффективности и любых неблагоприятных или непреднамеренных воздействий.

В подготовленной в 2022 году тематической сводной оценке требующих дополнительных действий пробелов и областей в реализации ключевых положений резолюций Совета, касающихся ПФТ,⁹ ИДКТК отмечал, что большинству государств, прошедших оценку в течение отчетного периода, не хватало надежных механизмов ГЧП для обмена информацией, понимания складывающихся тенденций, в том числе лучшего понимания связи между терроризмом и организованной преступностью, повышения уровня знаний и квалификации соответствующих экспертов, а также укрепления целостности финансового сектора.

В настоящей аналитической справке подчеркивается необходимость выделения государствами достаточных ресурсов для участников отношений как от государственного, так и от частного сектора, а также продолжения укрепления основ сотрудничества между компетентными национальными органами (не только ПФР, но и любыми другими ведомствами, участвующими в ПФТ, например, правоохранительными органами, таможней) и частным сектором для эффективного противодействия финансированию терроризма при условии полного соблюдения международного права, включая международное право прав человека, международное гуманитарное право и международное право беженцев. Такие основы должны включать четкие положения о том, какая информация может и не может обмениваться, при каких обстоятельствах и между какими участниками отношений, а также механизмы надзора и отчетности в целях обеспечения прав на защиту частной жизни и данных.

ОСНОВЫ ГОСУДАРСТВЕННО-ЧАСТНОГО ПАРТНЕРСТВА



Поскольку лица, финансирующие террористическую деятельность, используют различные инструменты в разных областях частного сектора, некоторые государства-члены признают, что ГЧП – это способ, позволяющий структурам частного сектора, которые часто не могут обмениваться важной информацией друг с другом, предупредить отрасль/сектор о том, как лица, финансирующие террористическую деятельность, используют соответствующие продукты и услуги. ГЧП могут стать инструментами, которые предоставляют возможности для активного обмена соответствующей информацией, что обеспечивает раннее выявление угроз. Они

⁹ ИДКТК, «Тематическая сводная оценка пробелов в реализации ключевых положений резолюций Совета Безопасности с области противодействия финансированию терроризма», декабрь 2022 г., доступна на www.un.org/securitycouncil/ctc/content/thematic-summary-assessment-gaps-implementing-key-counteracting-financing-terrorism-provisions.

также могут выступать в качестве механизмов решения проблемы обмена информацией, требующей немедленных и срочных действий.

В партнерстве с частным сектором заложен потенциал для совершенствования основ обмена информацией в целях реализации результативных мер ПФТ. В частности, в противодействии финансированию терроризма решающее значение имеет своевременность обмена информацией. Таким образом, правильно организованные ГЧП являются дополнительным уровнем структурированного и доверительного сотрудничества и расширяют обмен информацией между частным и государственным секторами, сохраняя преимущества двустороннего обмена информацией, обмена соответствующей информацией, включая раннее предупреждение, выдачу предупреждений в режиме реального времени о новых тенденциях и взаимную поддержку в ведении борьбы с такими тенденциями эффективным способом и пропорционально реальным рискам.

Частный сектор имеет в своем распоряжении данные и необходимые технологии для аналитики, а правоохранительные органы обладают опытом противодействия угрозам. ГЧП может стать связующим звеном между ними. Ответственное использование технологий и данных, включая блокчейн и искусственный интеллект, может улучшить оперативный и тактический анализ, составить карту финансовых сетей террористов, а также отслеживать и информировать о подозрительной деятельности.

Однако существует и определенная асимметрия и несогласованность целей.¹⁰ Предприятия частного сектора в основном сосредоточены на создании процессов и процедур, направленных на соблюдение законодательных и нормативных положений и избежание рисков и потенциального репутационного ущерба. В результате частный сектор будет стремиться ограничить обмен информацией с государственным сектором только тем, что строго требуется по закону. С другой стороны, правоохранительные органы обычно весьма деликатно относятся к вопросам терроризма, и иногда им законодательно запрещено обмениваться информацией с организациями частного сектора. Ввиду закрытого характера информации, которой владеет государственный сектор, частный сектор часто «лишен» информации, которая могла бы помочь ему в принятии обоснованных решений о том, чем можно инициативно и выгодно поделиться с государственным сектором.

Как отмечает ФАТФ, благодаря таким партнерствам информация передается правоохранительным органам, подразделениям финансовой разведки и одобренным участникам из частного сектора, а также в некоторых случаях международным партнерам. Установленный процесс сбора данных,

¹⁰ Cf. Patrick Hardouin, "Banks governance and public-private partnership in preventing and confronting organized crime, corruption and terrorism financing", *Journal of Financial Crime*; Vol. 16, Issue 3, (July 2009), P. 199-209.

оперативного анализа и сканирования частным сектором при взаимном обмене данными с государственным сектором способствует более комплексному анализу транзакций и поведения клиентов для заполнения потенциальных пробелов в аналитической работе. Инициативами можно также управлять в частном секторе, например, посредством обмена информацией внутри одной и той же группы финансовых организаций, отечественных и зарубежных филиалов или межбанковского форума для обмена информацией о последних тенденциях преступности, методах работы и типологиях среди участников с поддержкой и в сотрудничестве с правоохранительными и надзорными органами. В таких случаях «безопасные гавани» могут обеспечить специальную правовую защиту, позволяющую обмениваться информацией между финансовыми учреждениями в целях ПОД/ФТ.¹¹

Оценки ИДКТК показывают, что государства-члены сталкиваются с проблемами в институционализации партнерства с частным сектором в области обмена финансовой информацией, и, в частности, в сфере ПФТ. После создания такие партнерства могут принимать различные формы, не все из которых полностью эффективны или достаточно защищены.

Благодаря обмену информацией в режиме реального времени ГЧП с участием различных участников отношений позволяют разрабатывать более эффективные и комплексные стратегии расследования, поскольку они дают возможность государственным органам активнее работать с частным сектором в части отслеживания, определения месторасположения и выявления террористических сетей. Это особенно полезно в ситуациях, когда задействованы разные сектора, и не все из них подчиняются одним и тем же правилам или не все имеют доступ к одной и той же информации. Например, кампания по привлечению средств, проводимая с помощью краудфандинговых платформ или социальных сетей, может также включать официальный финансовый сектор и/или поставщиков услуг виртуальных активов, а также некоммерческий сектор в качестве бенефициара. Каждый из указанных участников отношений действует на основании разной нормативно-правовой базой, осуществляет различные проверки и контроль (если вообще осуществляет их), и лишь немногие из них будут обязаны сообщать о любой подозрительной информации соответствующим органам. Кроме того, те, кто сообщает информацию, могут иметь только определенные элементы, которые они обязаны отслеживать, в то время как другая важная информация остается у других участников отношений, которые не сообщают и не делятся ею. В результате у органов власти не будет всей информации, необходимой для анализа полной картины.

¹¹ ФАТФ, *Руководство по обмену информацией в частном секторе*, (Париж, 2017), доступно на www.fatf-gafi.org/en/publications/Fatfgeneral/Guidance-information-sharing.html.

Создание четкой правовой базы для обмена информацией между государственным и частным секторами имеет важное значение не только для обеспечения возможности такого обмена, но и для определения точных критериев и целей, для которых информация может быть передана, а также структур, с которыми она может обмениваться. Кроме того, наличие стандартов и процедур механизмов обратной связи между правоохранительными органами, подразделениями финансовой разведки и подотчетными организациями из соответствующих секторов может помочь повысить качество отчетов и информации финансовой разведки, а также обеспечить мониторинг тенденций и стратегический анализ. При разработке систем данных и процессов, которые облегчают доступ, поиск и анализ соответствующей информации (в том числе посредством использования машинного обучения и автоматизации обнаружения рисков финансовых преступлений), наличие стандартов и протоколов обмена информацией не только облегчает обмен информацией между различными субъектами ПФТ, но также обеспечивает защиту прав человека, включая право на защиту частной жизни и данных. Определение механизмов надзора на основе разработанных стандартов также гарантирует, что соответствующие ГЧП будут соблюдать обязательства по защите данных или обеспечению конфиденциальности в соответствии с национальным законодательством, а также применимыми международными стандартами.

Среда ГЧП для обмена финансовой информацией характеризуется большим разнообразием, при этом большинство ГЧП имеют более широкую сферу применения, выходя за рамки исключительно ПФТ. Важно понимать эти нюансы, поскольку не существует единой конкретной модели, лежащей в основе термина «ГЧП». На практике оно включает в себя различные механизмы обмена информацией между государственным и частным секторами, происходящее как в рамках четко обозначенного ГЧП, так и посредством других механизмов.

Обмен стратегической информацией



Некоторые формы сотрудничества между национальными властями и частным сектором называются ГЧП, но по сути они носят более стратегический характер и, в первую очередь, служат целям совместной разработки типологий и информационных продуктов, охватывающих угрозы и соответствующие индикаторы риска. Как правило, эти продукты не содержат конфиденциальной или персональной информации о конкретных подозреваемых и организациях. Например, во Франции Управление разведки и противодействия подпольным финансовым схемам (TRACFIN) может публиковать «призывы к бдительности», распространяемые среди подотчетных

организаций. Цель состоит в том, чтобы помочь им реализовать подходы, основанные на риске, привлекая их внимание к конкретной ситуации. В 2019 году TRACFIN опубликовало одиннадцать «призывов к бдительности» по линии финансирования терроризма. Такие уведомления могут касаться конкретных уязвимых секторов, но могут иметь отношение и ко всей отрасли. ПФР Канады - Канадский центр анализа финансовых операций и отчетов (FINTRAC) представляет собой еще один пример повышения осведомленности о распространении информации по конкретным темам. Продукты стратегической разведки FINTRAC предоставляют аналитические взгляды на природу, масштабы и угрозы, создаваемые финансированием терроризма для конкретных секторов, ключевые закономерности подозрительных операций, связанных с терроризмом и актами насильственного экстремизма на почве ксенофобии, расизма и других форм нетерпимости или совершаемых во имя религии или убеждений, а также индикаторы деятельности по финансированию терроризма в отношении иностранных боевиков-террористов.

Оперативные партнерства



Созданы другие формы ГЧП, которые носят более оперативный характер и позволяют обмениваться информацией о происшествиях, субъектах и организациях, а также их финансовых операциях. Эти формы ГЧП предполагают обмен более конфиденциальной информацией, которая может быть использована в финансовой разведке и следственных операциях, и где частный сектор не только обеспечивает соблюдение правил регулирования финансовых преступлений, но и становится участником следственных действий.¹² Одновременно он помогает частному сектору повысить эффективность комплексной проверки клиентов¹³ и выявлять клиентов с повышенным риском.¹⁴ Оперативные ГЧП не обязательно включают в себя несколько субъектов частного сектора, а вместо этого выделяют более уязвимые и ключевые учреждения/сектора для разработки механизмов обмена информацией с более

¹² Например, см. Евразийская группа по противодействию легализации преступных доходов и финансированию терроризма, «Легализация (отмывание) преступных доходов от киберпреступлений, а также финансирование терроризма за счет указанной преступной деятельности, в том числе с использованием электронных денег и виртуальных активов и инфраструктуры их провайдеров (2022)», стр. 10–11, доступ по ссылке:

[https://eurasiangroup.org/files/uploads/files/other_docs/WGTYP_\(2022\)_12_rev_1_eng.pdf](https://eurasiangroup.org/files/uploads/files/other_docs/WGTYP_(2022)_12_rev_1_eng.pdf).

¹³ Caribbean Financial Action Task Force Research Desk, “The importance of public private partnerships in AML/CFT”, 2022, стр. 5.

¹⁴ ФАТФ, *Руководство по обмену информацией в частном секторе*, (Париж, 2017), стр. 13, доступ по ссылке: www.fatf-gafi.org/en/publications/Fatfgeneral/Guidance-information-sharing.html.

целенаправленным подходом. Наиболее известными примерами являются Объединенная оперативная группа по борьбе с отмыванием денег Соединенного Королевства Великобритании и Северной Ирландии, результатом которой стал ряд успешных следственных операций, а также Сеть по борьбе с финансовыми преступлениями Министерства финансов США. Совсем недавно подразделение финансовой разведки Королевства Нидерландов установило дружественные отношения с банками для осуществления совместной работы с массивами отчетов и СПО. Созданная сеть финансовой разведки Малайзии также преследует реализацию тактических целей, таких как обмен информацией по конкретным делам для дальнейшего рассмотрения подотчетными учреждениями.¹⁵

Условия выстраивания партнерства



В рамках реализации совместных планов некоторые ГЧП создают специальные рабочие пространства, доступ к которым предоставлен только уполномоченному персоналу или ключевым участникам, что обеспечивает возможность сотрудничества в режиме реального времени по конкретным делам или операциям, как это реализуется, например, в Латвийской группе по координации сотрудничества. Некоторые же отдают приоритет развитию специализированных коммуникационных платформ для обмена информацией, примером чего является Сингапурское отраслевое партнерство по борьбе с отмыванием денег и финансированием терроризма. Если говорить об организации управления, то в большинстве своем руководство ГЧП находится в руках компетентных органов. В ряде партнерств предусмотрены механизмы надзора, которые предоставляют возможность как представителям правительственных структур, так и отрасли контролировать деятельность и формулировать повестку будущей работы. Примером тому является австралийский альянс Fintel, который предоставил федеральной полиции разведывательные данные о подозреваемых, что позволило пресечь террористический акт.¹⁶

Также оказалось возможным эффективное сотрудничество между двумя секторами, ориентированное на достижение конкретных целей. Например, ПФР Франции (TRACFIN) подписало двусторонние протоколы обмена информацией с

¹⁵ Это привело к аресту, судебному преследованию и депортации 22 лиц по подозрению в причастности к терроризму и финансированию распространения оружия массового уничтожения в Малайзии.

¹⁶ ФАТФ, *Создание партнерства в борьбе с финансовыми преступлениями: Защита информации, технологии и обмен информацией с частным сектором*, (Париж, 2022), стр. 64, доступ по ссылке: www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf.coredownload.pdf.

Также см. Азиатский банк развития (АБР), Публикация АБР «Financial crimes compliance: the power of partnerships», № 180, июль 2021, доступ по ссылке: <https://www.adb.org/publications/financial-crimes-compliance-power-partnerships>.

отдельными организациями частного сектора, а в 2019 году учредило специальный комитет по борьбе с финансированием терроризма для формализации обмена информацией между TRACFIN и подотчетными организациями.

Некоторые ГЧП созданы на наднациональном уровне, некоторые предусматривают наличие более постоянной структуры. Примером тому является государственно-частное партнерство Агентства Европейского Союза по сотрудничеству правоохранительных органов (Europol) в области финансовой разведки, установленное в 2017 году. Другие партнерства более ориентированы на реализацию проектов, развитие передового опыта, наращивание потенциала и сетевые инициативы с участием государственных и частных участников отношений. Инициатива BeCaNet (лучшая практика, наращивание потенциала и сетевая инициатива между государственными и частными участниками отношений в борьбе с финансированием терроризма) представляет собой двухлетнюю программу, реализуемую Федеральной уголовной полицией Германии в сотрудничестве с властями Франции, Испании и США для создания сетей частных и государственных заинтересованных участников отношений в целях противодействия финансированию терроризма.

На региональном уровне структуры по типу ФАТФ реализуют инициативы по более тесному сотрудничеству с частным сектором. Ярким примером является серия консультативных форумов, проводимых Евразийской группой по противодействию отмыванию денег и финансированию терроризма с 2006 года с целью налаживания взаимодействия между государственным и частным секторами для совершенствования системы ПОД/ФТ, а также обмена руководящими принципами и мнениями обоих секторов и решения возникающих проблем, связанных с новыми способами оплаты. Такие консультативные форумы позволяют формулировать рекомендации на взаимопонятных условиях. В 2013 году Альянс за финансовую инклюзивность при Группе по борьбе с отмыванием денег в Восточной и Южной Африке (ESAAMLG) подготовил отчет о проведенном исследовании в государственном и частном секторах по финансовой безупречности, основам финансовой инклюзивности и практике соблюдения требований, а также оценил уровень взаимодействия с частным сектором и влияние снижения рисков. Аналогичным образом, в отчете Межправительственной группы действий по борьбе с отмыванием денег в Западной Африке (GIABA) за 2020 год об оценке деятельности по борьбе с финансированием терроризма были выявлены пробелы в отчетности частного сектора о подозрительной деятельности и предложен ряд рекомендаций.

УСТРАНЕНИЕ ПРОБЕЛОВ И ПРОБЛЕМ, ВЫЯВЛЕННЫХ В РАМКАХ ГЧП

Недостаток ресурсов и потенциала



Одной из общих проблем на пути эффективного ГЧП в области ПОД/ФТ является недостаточный объем инвестиций в материальные, финансовые и человеческие ресурсы как в частном секторе, так и в государственных органах, включая ПФР.¹⁷

В этой связи правительствам следует больше инвестировать в ресурсы, связанные с ПОД/ФТ, и способствовать эффективной координации целевых мероприятий по наращиванию потенциала для накопления национального опыта.¹⁸ Еще одной передовой практикой является реорганизация соответствующих служб для оптимизации человеческих ресурсов и отслеживания максимального количества дел, затрагивающих интересы государства.¹⁹ Кроме того, принимая во внимание и оценивая эффективность потока информации через ГЧП, как государственный, так и частный секторы могли использовать в своих интересах выгоды от таких партнерств, например, назначив в специализированных подразделениях контактных лиц для координации действий в конкретных областях. Дополнительным преимуществом объединения контактных лиц является установление взаимопонимания и доверия между ними, что, в свою очередь, обеспечивает защиту конфиденциальности обмениваемой информации.

¹⁷ Отмечено в ходе взаимодействия ИДКТК с соответствующими участниками отношений. Эта проблема также упоминается, например, в *Отчете GIABA «Оценка проблем, связанных с расследованием, судебным преследованием и вынесением решения по делам, связанным с отмыванием денег и финансированием терроризма в Западной Африке», «Отчет об оценке»* (Дакар, 2021 г.), п. 188, доступ по ссылке: www.giaba.org/media/f/1302_An%20Assessment%20of%20Challenges.pdf; ESAAMLG, *Отчет об отмывании денег через рынок ценных бумаг в в регионе ESAAMLG*, (2015), стр. 56–58, доступ по ссылке: <https://www.esaamlg.org/reports/Report%20on%20ML%20&%20TF%20through%20the%20Securities%20Market%20Industry%20in%20the%20ESAAMLG%20Region..pdf>.

¹⁸ Ibid., стр. 54; и ibid., стр. 58.

¹⁹ GIABA «Оценка проблем, связанных с расследованием, судебным преследованием и вынесением решения по делам, связанным с отмыванием денег и финансированием терроризма в Западной Африке», «Отчет об оценке» (Дакар, 2021 г.), стр. 31, доступен на www.giaba.org/media/f/1302_An%20Assessment%20of%20Challenges.pdf.

Ограничение сферы применения ГЧП традиционными финансовыми институтами



На фоне растущего числа финтех-компаний и децентрализованных финансовых услуг клиенты все чаще обращаются к различным формам финансовых продуктов и услуг вместо традиционных банковских услуг. Как следствие, данные о клиентах становятся все более разрозненными, что затрудняет получение информации о финансировании терроризма на основе данных из одного учреждения. Сообщается, что террористические группировки используют множество методов, включая трансграничную перевозку наличных денег и систему денежных переводов «Хавала» в сочетании с новыми и перспективными способами оплаты (например, предоплаченные карты, системы мобильных платежей, виртуальные и онлайн-обмены и кошельки, а также виртуальные активы). Установление партнерства с каждым таким сектором сопряжено со своими проблемами.

На этом фоне сформированные ГЧП в первую очередь ориентированы на сотрудничество с финансовыми учреждениями, особенно с розничными банками, и включают в себя ограниченное число участников от частного сектора в сравнении с организациями, регулируемые в целях ПОД/ФТ. Принимая это во внимание, некоторые государства-члены разрабатывают ГЧП на основе пилотных инициатив с целью расширения сферы их деятельности и включения в перспективе большего количества участников. Например, в Королевстве Нидерландов Целевая группа по борьбе с финансированием терроризма, состоящая в основном из крупнейших банков страны, изучает возможность привлечения других участников частного сектора. Другим примером является инициатива Южноафриканской объединенной целевой группы по борьбе с отмыванием денег, которая была предложена в 2022 году и реализуется в партнерстве с организацией United for Wildlife в целях пресечения финансовых преступлений, связанных с незаконной торговлей дикими животными.

Отвечая на вопрос о представительстве частного сектора в ГЧП, некоторые эксперты подчеркнули важность доверия, которое зависит от управляемого объема данных для сохранения конфиденциальности передаваемой разведывательной информации и обеспечения эффективного принятия решений. Однако это может противоречить необходимости гибкости и динамичности, поскольку ключевые участники отношений могут быстро меняться, также как и могут достаточно быстро происходить изменения в способах использования новых финансовых технологий террористами. Что касается сотрудничества с компаниями, связанными с финансовыми технологиями, Интернетом и социальными сетями, в борьбе с финансированием терроризма, государства-

члены, особенно ПФР, в первую очередь сообщали о снижении рисков финансирования терроризма посредством выпуска типологий и индикаторов риска в целях повышения осведомленности. Например, во Франции TRACFIN использует социальные сети для обмена типологиями и практическими примерами, а также организует вебинары и семинары по ПОД/ФТ. Ярким примером является ее последнее видео, демонстрирующее использование анонимных ваучеров, конвертированных в виртуальные активы, транснациональными террористическими сетями, использующими комбинацию традиционных систем перевода денег, таких как «хавала», со сложным набором инструментов и методов, включающих новые технологии.

Несмотря на то, что ГЧП имеют усовершенствованные механизмы обмена информацией в рамках усилий государств по ПОД/ФТ, нынешние партнерства могут не уделять достаточного внимания соответствующей информации в ключевых и особенно уязвимых областях. В частности, ПФТ требует активного сотрудничества с уязвимыми секторами, не ограничивающегося сотрудничеством между традиционными финансовыми секторами и подразделениями финансовой разведки/правоохранительными органами. В качестве примеров уязвимых секторов можно привести те, которые используют новые способы оплаты, услуги по переводу денежных ценностей, предприятия, торгующие природными ресурсами, в частности в золотодобывающем секторе, рынки антиквариата и искусства, а также компании, работающие в зонах свободной торговли. Целью будет разработка целевых механизмов сотрудничества между ключевыми областями частного сектора, которые характеризуются более высоким уровнем финансирования терроризма, и соответствующим государственным сектором.

При отборе и определении приоритетности участников ГЧП от частного сектора необходимо руководствоваться актуальной национальной оценкой рисков финансирования терроризма, подкрепленной комплексной и эффективной стратегией борьбы с финансированием терроризма. Например, как подчеркивается в последнем отчете о деятельности TRACFIN, половина СПО от краудфандинговых платформ связана с финансированием терроризма.²⁰

²⁰ Для получения дополнительной информации о практике и проблемах, связанных с использованием краудфандинга для финансирования терроризма, см. последний отчет о деятельности TRACFIN, ПОД/ФТ: *Обзор подотчетных структур 2022*, (2022), доступ по ссылке: www.economie.gouv.fr/files/2023-06/TRACFIN_2022_EN_Web.pdf ; и ФАТФ, *Краудфандинг для финансирования терроризма*, (Париж, 2023), доступ по ссылке: www.fatf-gafi.org/publications/Methodsandtrends/crowdfunding-for-terrorism-financing.html .

Нечеткая нормативно-правовая база



Наличие в государствах законодательства, в соответствии с которыми подотчетные структуры обязаны сообщать информацию при наличии подозрений в совершении преступления или финансировании терроризма, является лишь одним из способов информирования в рамках ПФТ и не охватывает все имеющиеся варианты, включая обмен информацией на добровольной основе. Препятствиями для сотрудничества являются законодательные запреты, в том числе законы об обеспечении конфиденциальности данных, которые в целом ограничивают возможности правоохранительных органов в получении информации, необходимой для расследований.²¹ Имеются исследования, в которых изучались масштабы неформального, не предусмотренного законом информационного обмена, который осуществлялся через прямые контакты. При этом обмен информацией осуществлялся, исходя из принципа служебной необходимости, в независимости от наличия какого-либо действующего соглашения. Этому также способствует, когда сотрудники государственного сектора переходят на работу в частный сектор и имеют возможность поддерживать личные контакты. Однако роль обмена информацией между государственным и частным секторами в интересах текущих расследований ставит вопрос о взаимосвязи уголовного процессуального права и законодательства в сфере ПОД/ФТ. Неофициальная практика обмена информацией в ходе уголовных расследований через ГЧП может привести к серьезным проблемам в части применимости информации в качестве доказательств в уголовном судопроизводстве, а также к отсутствию четкости в понимании роли и правовых последствий для подотчетных организаций, что в некоторых случаях может привести к утрате доверия и возникновению препятствий для раскрытия информации. В попытке внести больше определенности некоторые ГЧП проводят консультации с частным сектором, прежде чем предпринимать какие-либо действия, чтобы обеспечить общее понимание и подход. Такие подходы могут помочь избежать непредвиденных последствий. Например, подотчетные организации могут быть заранее проинформированы о том, что им следует строго запретить передавать уведомление о рисках и его содержание третьим лицам без предварительного разрешения, и что они не должны предпринимать никаких действий, которые могут поставить под угрозу любое расследование.

²¹ См. GIABA «Оценка проблем, связанных с расследованием, судебным преследованием и вынесением решения по делам, связанным с отмыванием денег и финансированием терроризма в Западной Африке», «Отчет об оценке» (Дакар, 2021 г.), стр. 8, доступ по ссылке: www.giaba.org/media/f/1302_An%20Assessment%20of%20Challenges.pdf.

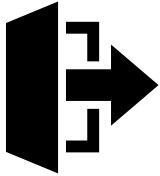
В связи с этим широко распространенная практика неформальных отношений как возможности для сотрудничества с частным сектором подчеркивает необходимость в наличии предметной и более четкой нормативно-правовой базы, которая также будет принимать во внимание права и обязанности частного сектора, включая гарантии защиты информации и ее источника.

Пробелы в нормативно-правовом регулировании также затрагивают социально-сетевые компании и некоторые краудфандинговые платформы, которые не являются субъектами предоставления отчетности, но, тем не менее, могут быть использованы террористами для сбора и перемещения средств. Благодаря проведению агитационно-пропагандистских мероприятий и реализации инициатив по повышению осведомленности ГЧП могут обеспечить, чтобы усилия социально-сетевых компаний и краудфандинговых структур, направленные на ПФТ, были информационно поддержаны и эффективными. Это даст определенную защиту их деятельности и снабдит их инструментами, позволяющими понимать риск-индикаторы и, в конечном итоге, минимизировать подозрительную деятельность и/или сообщать о таковой. В докладе APG/MENAFATF «Социальные сети и финансирование терроризма» представлены тематические исследования и набор соответствующих комплексных рекомендаций.²²

Как отметила ФАТФ, национальная стратегия ПФТ, основанная на тщательной и современной оценке рисков, укрепляет нормативно-правовую базу и обеспечивает прочную основу для оперативного сотрудничества между соответствующими ведомствами и частным сектором, особенно в отношении новых и перспективных финансовых технологий, которые представляют собой общую проблему для государств-членов в части выявления алгоритмов подозрительной деятельности и при проведении расследований.

²² Доступ по ссылке: www.menafatf.org/sites/default/files/Newsletter/FINAL-TM-SF-en.pdf.

Односторонняя связь и ограничения на обратную связь и рекомендации



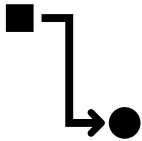
Во многих государствах ГЧП ограничиваются односторонними каналами связи, по которым информация предоставляется или запрашивается на разовой основе, без последующей проверки результатов или регулярной обратной связи, и поэтому такое информационное взаимодействие не полностью реализуют свой потенциал. Обратная связь имеет решающее значение для совершенствования оценки полезности предоставляемой информации, повышения ее качества или целеполагания будущего информационного взаимодействия, а также в целом для обеспечения доверительного и постоянного диалога. Руководство должно быть направлено на устранение имеющихся пробелов в знаниях или реализации. Бремя сбора и, что наиболее важно, обработки огромного количества финансовых данных (включая, например, общедоступные данные о транзакциях с виртуальными активами) должно быть распределено между секторами.

Эффективные ГЧП требуют понимания операционных и транзакционных реалий, а также сосредоточения внимания на обмене и получении полезной информации. В рамках инициативы Australia and New Zealand Banking Group Limited²³ и проекта Fintel Alliance, возглавляемого Австралийским центром отчетности и анализа, ежегодно собирается более 160 миллионов отчетов о транзакциях, которые после обработки становятся ценной оперативной информацией, используемой при проведении расследований.²⁴ Для понимания тенденций необходимо, чтобы правоохранительные органы были знакомы с реалиями и практическими аспектами финансовых операций, а частный сектор был осведомлен о алгоритмах ФТ. Крайне важно повышать знания и квалификацию соответствующих экспертов на обоих концах информационного взаимодействия. Например, частный сектор может быть сориентирован на устранение ангажированности и ошибочных данных в моделях обнаружения, в том числе через обратную связь между людьми, наиболее эффективным способом с соблюдением прав человека. Особое внимание при этом следует уделить новым секторам, таким как новые поставщики платежных услуг и специалисты по цифровым и децентрализованным финансам.

²³ В данной инициативе участвуют 12 стран Тихоокеанского региона.

²⁴ ADB, Публикация «Financial crimes compliance: the power of partnerships», № 180, июль 2021, доступ по ссылке: www.adb.org/publications/financial-crimes-compliance-power-partnerships.

Непредвиденные последствия, включая влияние на права человека



В государствах-членах с развитыми ГЧП имеются нормативно-правовые основы, которые различаются в зависимости от множества возможных конфигураций методов обмена информацией для частного и государственного секторов и регулируют цели и средства обмена информацией, включая обработку персональных данных. Однако государства, которые полагаются на неформальное сотрудничество или слабые ГЧП, могут не принять адекватных правовых мер для обеспечения того, чтобы ГЧП соблюдали право на неприкосновенность частной жизни, конфиденциальность данных и принципы защиты данных в соответствии с международными стандартами прав человека.

ГЧП обязательно должно включать разработку систем и процессов обработки данных, которые обеспечивают доступ и анализ большого объема информации, часто содержащей конфиденциальные данные, которая может привести к нарушениям прав человека, если будет раскрыта произвольным и незаконным способом. Новые технологии еще больше повысили эффективность информационного обмена. Правила защиты данных и защита источников получения информации по-прежнему остаются в числе сложных вопросов, что в случае уголовных разбирательств, возбужденных в рамках ГЧП, может оказать серьезное влияние на клиентов и частные структуры. Частный сектор, связанный законодательством о защите данных, также обязан уважать права человека.²⁵ Без надлежащих гарантий обмен информацией между государственным и частным секторами может привести к предвзятости, а также расовому, политическому или религиозному профилированию.²⁶ В этом смысле, соблюдая баланс требований эффективного информационного потока, правоохранительные органы и ПФР должны проявлять осторожность в отношении того, что они запрашивают у частного сектора, при этом обеспечивать ясность и давать конкретные рекомендации, чтобы избежать недопонимания или предоставления ненужной информации.

Меры по борьбе с терроризмом позволяют государствам вводить определенные ограничения на общие принципы защиты данных, когда это необходимо и соразмерно целям предотвращения, расследования, выявления или преследования уголовных преступлений, включая терроризм, а также в целях

²⁵Руководящие принципы предпринимательской деятельности в аспекте прав человека, осуществление рамок ООН в отношении «защиты, соблюдения и средств правовой защиты», 2011, доступ по ссылке: www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf.

²⁶ Benjamin Vogel, "Public- private partnerships in the fight against the financing of terrorism", Department of Criminal Law, Max Planck Institute for the study of crime, security and law, 2022. Доступ по ссылке: <https://csl.mpg.de/en/projects/fight-financing-terrorism>.

защиты от угроз общественной безопасности. Эти процессы могут сопровождаться недостаточным судебным надзором, низкой прозрачностью и недостаточными средствами правовой защиты в случае нарушений. Как отмечалось выше, расплывчатые и двусмысленные правовые рамки могут привести к тому, что частный сектор будет придерживаться реактивного подхода и может чрезмерно соблюдать требования, чтобы избежать репутационных рисков или угрозы судебного иска. Неопределенность и отсутствие ясности могут непреднамеренно привести к неправомерному вмешательству в право на неприкосновенность частной жизни и иметь другие негативные последствия для свободы убеждений, выражения мнения, проведения собраний, а также религии или вероисповедания.²⁷ Например, когда власти имеют возможность влиять на поисковые алгоритмы частного сектора, «косвенная» обработка личных или стратегических данных органами власти несет в себе риск их неправомерного использования.

В рамках конституционных и/или других национальных законов необходимо достичь консенсуса относительно того, что возможно при обмене данными. Существует множество судебных решений по защите данных, но ее влияние на обмен информацией в сфере ПОД/ФТ еще не до конца изучено. Поскольку ГЧП становится более универсальным инструментом в рамках ПОД/ФТ, создание правил и политик, которые четко и с достаточной точностью определяют допустимые основания, предварительные условия и процедуры разрешения, регулирующие сбор или мониторинг финансовых данных или информации, а также меры защиты, будет способствовать укреплению легитимности ГЧП и эффективности мер ПФТ.²⁸

В таком процессе государства-члены должны обеспечить, чтобы стандарты и протоколы обмена данными, а также механизмы надзора облегчали обмен информацией по линии ПФТ, одновременно обеспечивая защиту прав человека, включая право на защиту частной жизни и данных в соответствии с национальным законодательством, принципами недискриминации и применимыми международными стандартами. Частному сектору рекомендуется использовать ГЧП в качестве платформы для управления и минимизации рисков, а также избегать неоправданного ограничения доступа к финансовым услугам или задержки транзакций. Оба сектора должны работать синхронно, используя общий подход и понимание.

²⁷ Н. Пуртова, «Между Общим регламентом по защите данных и директивой для полиции: как пройти через лабиринт обмена информацией в рамках государственно-частного партнерства», 2018.

²⁸ ФАТФ, *Создание партнерства в борьбе с финансовыми преступлениями: Защита информации, технологии и обмен информацией с частным сектором*, (Париж, 2022), стр. 64, доступ по ссылке: www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf.coredownload.pdf.

Несмотря на значительные усилия по предотвращению того, чтобы меры ПФТ приводили к снижению рисков подотчетных организаций с одновременным ростом проблем доступа к финансовым услугам, данные организации по-прежнему могут налагать необоснованные ограничения и меры контроля на деятельность своих клиентов и прекращать отношения с ними, исходя исключительно из восприятия риска.²⁹ Первоначальные подозрения органов уголовного правосудия или ПФР иногда основаны на непроверенной информации, и впоследствии подозрения могут оказаться необоснованными, а ограничения с их стороны прав подозреваемых обычно увязываются с процессуальными гарантиями защиты. Субъекты частного сектора могут реагировать на представленную информацию и использовать ее для закрытия счетов или прекращения отношений с клиентами, опасаясь принудительных действий со стороны органов надзора в сфере ПОД/ФТ, и/или репутационных рисков.

Такие действия, предпринимаемые организациями частного сектора в рамках ГЧП, могут серьезно повлиять на клиентов и репутацию частного предприятия. И поскольку такая реакция возникает в результате обмена информацией в рамках ГЧП, компетентным органам не могут не разделить ответственность. Следовательно, в рамках ГЧП необходимо тщательно оценить баланс между эффективным обменом информацией и гарантиями защиты от потенциального вреда.³⁰

С другой стороны, партнерства с частным сектором должны также предоставлять возможности для содействия значимому участию гражданского общества в обеспечении того, чтобы такие партнерства не ущемляли финансовую инклюзивность и гражданское пространство, в том числе, чтобы не ограничивали законную деятельность некоммерческих организаций и исключительно гуманитарную деятельность.³¹

Еще одной проблемой, которая касается более широких усилий государств-членов по ПФТ, является эффективная институционализация гендерных аспектов в мерах ПФТ, в том числе в рамках сотрудничества с частным сектором. В этой связи поступает информация о недостаточных усилиях, предпринимаемых государствами в части учета гендерных вопросов в рамках ГЧП и создания механизмов мониторинга и оценки результатов. Поскольку государства заключают все больше соглашений об обмене информацией с частным сектором,

²⁹ «Синописис высокого уровня результатов анализа непреднамеренных последствий стандартов ФАТФ», 27 октября 2021 г.

³⁰ Benjamin Vogel, "Potentials and limits of public-private partnerships against money laundering and terrorism financing", 2022, available at <https://eucrim.eu/articles/potentials-and-limits-of-public-private-partnerships-against-money-laundering-and-terrorism-financing/>.

³¹ Глобальный контртеррористический форум, Меморандум о передовой практике реализации мер по борьбе с финансированием терроризма при одновременной защите гражданского пространства, сентябрь 2021 г., доступ по ссылке: www.thegctf.org/Portals/1/Documents/Links/Meetings/2021/19CC11MM/CFT%20GP%20Memo/CFT%20Memo_ENG.pdf?ver=fahs72uclYyYOTj7WDwBkO%3D%3D.

важно обеспечить, чтобы разработанные типологии и превентивные меры или тактическая информация, которой обмениваются в рамках ГЧП, не оказывали непропорционального влияния на какой-либо гендерный фактор, в том числе путем ограничения доступа к финансовым средствам.

По мере развития обмена информацией между частным и государственным секторами компетентным органам необходимо будет все больше учитывать потенциальное влияние профилактических мер и соответствующим образом вносить изменения в рабочие механизмы и стандарты.

Использование новых или развивающихся технологий для обмена информацией с частным сектором



Поскольку как государственные, так и частные субъекты обрабатывают более сложные данные, важную роль играют технологии. ГЧП часто предполагает использование таких технологий, как коммуникационные платформы или инструменты анализа данных, для анализа и обмена информацией. Ряд государств сообщили, что они разработали коммуникационные платформы, позволяющие обмениваться информацией между государственным и частным секторами. Использование новых технологий в ГЧП представляет собой важную возможность, поскольку они могут быть созданы для безопасной обработки данных для конкретной цели более точным и своевременным способом, особенно по сравнению с государствами, которые полагаются на бумажные системы.³²

В то же время разработка технологий, способствующих расширению обмена информацией между частным и государственным секторами, требует ответственных и инновационных подходов, ориентированных на актуальность и эффективность, но которые также включают соответствующие меры по минимизации последствий. Согласно Стандартам ФАТФ, эти меры должны соответствовать принципам необходимости, пропорциональности, законности и недискриминации согласно международному праву в области прав человека, а также подходу, основанному на оценке риска.³³ Например, технологии повышения конфиденциальности также могут помочь решить проблемы, связанные с

³² ФАТФ, *Возможности и вызовы использования новых технологий в целях ПОД/ФТ*, (Париж, 2021), доступ по ссылке: www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf.coredownload.pdf.

³³ Технические сессии ИДКТК: Основные моменты по вопросу «Угрозы и возможности, связанные с новыми платежными технологиями и методами сбора средств», доступ по ссылке: www.un.org/securitycouncil/ctc/news/cted%E2%80%99s-tech-sessions-highlights-%E2%80%9Cthreats-and-opportunities-related-new-payment-technologies-0.

защитой данных (например, когда технологии позволяют анализировать зашифрованные данные, не раскрывая личности отдельных лиц).

Помимо сложностей и затрат, связанных с разработкой или обновлением систем, направленных на внедрение инноваций в основы ПОД/ФТ, таких как технологии регулирования (regtech) и технологии надзора (suptech), обмену информацией между заинтересованными сторонами могут препятствовать операционные проблемы, связанные с различными форматами данных, отсутствием совместимости между системами, или отсутствие безопасных коммуникационных платформ.

В свете этого критической проблемой стала важность конфиденциальности данных и этичного обращения с данными. Например, ПФР Королевства Нидерландов недавно сообщило о своем намерении интегрировать конфиденциальность данных и этическую обработку данных в процесс разработки технологий и партнерских отношений. Данная работа в настоящее время проводится.

Более того, консультации ИДКТК показывают, что существующие основы ГЧП находятся на ранней ступени развития и недостаточно обеспечивают эффективный обмен информацией. Было бы полезно иметь правила, позволяющие частному сектору предоставлять данные в электронном формате и по определенному стандарту.

ЗАКЛЮЧЕНИЕ

Поскольку государства все чаще обращаются к частному сектору для совершенствования основ ПОД/ФТ и реагирования на меняющуюся тактику финансирования терроризма, существует острая необходимость в сотрудничестве на основе нормативно-правовой базы, определяющей условия, при которых компетентные органы могут получить доступ к информации, связанной с финансированием терроризма, и опыту, имеющемуся в частном секторе.

Развитие финансовых методов также требует взаимодействия с более широким кругом заинтересованных сторон, помимо традиционных финансовых институтов. Тот факт, что существующие партнерские отношения с частным сектором в основном заключаются с традиционными финансовыми субъектами, затрудняет для государств всестороннее понимание возникающих угроз.

Создание прочных и четких правовых основ, соответствующих определенным стандартам в области прав человека, в частности, прав на защиту данных и конфиденциальность, для продвижения эффективных ГЧП, является ключом к эффективному обмену информацией между компетентными национальными органами власти и организациями частного сектора. Более инклюзивное партнерство с расширенным кругом заинтересованных сторон оказалось полезным для того, чтобы ГЧП работало в нынешней ситуации в финансовой отрасли.

Хорошо зарекомендовавшие себя ГЧП могут служить ценными моделями успешного партнерства для других государств-членов, а извлеченные уроки помогут убедить компетентные органы выделить достаточные ресурсы, время и усилия. В этой связи ИДКТК будет продолжать отслеживать тенденции и развитие усилий государств-членов в части эффективного сотрудничества с частным сектором, действуя совместно со всеми соответствующими партнерами и заинтересованными сторонами (включая ФАТФ и ее Глобальную сеть) с целью выявления передовой практики и выработки рекомендаций по укреплению потенциала государств-членов в этой области.

