Организация Объединенных Наций S/2025/22*

Совет Безопасности

Distr.: General
10 January 2025
Russian
Original: English

Письмо Председателя Совета Безопасности, действующего в отсутствие Председателя Комитета Совета Безопасности, учрежденного резолюцией 1373 (2001) о борьбе с терроризмом, от 9 января 2025 года на имя Председателя Совета Безопасности

От имени Комитета Совета Безопасности, учрежденного резолюцией 1373 (2001) о борьбе с терроризмом, имею честь сослаться на не имеющие обязательной силы руководящие принципы, касающиеся предотвращения, выявления и пресечения использования новых и новейших финансовых технологий в террористических целях (см. приложение) и известные под названием «Алжирские руководящие принципы», которые были подготовлены в соответствии с Делийской декларацией о противодействии использованию новых и новейших технологий в террористических целях, в которой Комитет постановил разработать набор не имеющих обязательной силы руководящих принципов для оказания помощи государствам-членам в противодействии угрозе, связанной с применением новых и новейших технологий в террористических целях.

Я хотел бы обратиться с просьбой об издании настоящего письма и приложения к нему в качестве документа Совета Безопасности.

(*Подпись*) Амар **Бенджама**
Председатель Совета Безопасности, действующий
в отсутствие Председателя Комитета Совета Безопасности,
учрежденного резолюцией 1373 (2001) о борьбе с терроризмом

* Переиздано по техническим причинам 23 апреля 2025 года.

Приложение

Не имеющие обязательной силы руководящие принципы для государств-членов по предотвращению, выявлению и пресечению использования новых и новейших финансовых технологий в террористических целях[1]

1. Новые и новейшие технологии обеспечивают масштабные потенциальные преимущества во многих областях, включая здравоохранение, пограничный контроль, правоохранительную деятельность, транспорт, гуманитарную помощь и системы связи.

2. Принося существенную пользу обществу, новые и новейшие технологии в то же время применяются в террористических целях ИГИЛ (ДАИШ), «Аль-Каидой», связанными с ними группировками, другими террористическими организациями и их сторонниками. Государства-члены уже сталкиваются со значительной и растущей угрозой применения новых и новейших технологий в поддержку широкого спектра террористической деятельности.

3. Памятуя об усиливающейся угрозе неправомерного применения новых и новейших технологий, а также о многочисленных полезных возможностях использования технологий для борьбы с терроризмом, Контртеррористический комитет провел 29 октября 2022 года в Индии специальное заседание по противодействию применения новых и новейших технологий в террористических целях и принял Делийскую декларацию.

4. Контртеррористический комитет выразил также намерение разработать при поддержке Исполнительного директората Контртеррористического комитета набор не имеющих обязательной силы руководящих принципов в целях оказания государствам-членам помощи в противодействии угрозе применения новых и новейших технологий в террористических целях, в том числе на основе обобщения передового опыта в части возможностей, предоставляемых тем же набором технологий для противодействия этой угрозе, в соответствии с международным правом прав человека и международным гуманитарным правом. В порядке содействия разработке упомянутых руководящих принципов Исполнительный директорат организовал от имени Комитета всеобъемлющий консультативный процесс по каждой из трех тем с соответствующими экспертами из учреждений Организации Объединенных Наций и международных и региональных организаций-партнеров, а также с рядом соответствующих заинтересованных сторон из Глобальной контртеррористической исследовательской сети Исполнительного директората, включая частный сектор, академические круги и гражданское общество.

5. Совет Безопасности вновь заявил, что государства-члены должны обеспечивать, чтобы любые меры, принимаемые в целях борьбы с угрозой применения новых и новейших технологий в террористических целях, соответствовали всем их обязательствам по международному праву, в частности по международному праву прав человека, международному беженскому праву и международному

[1] Цель и направленность настоящих не имеющих обязательной силы руководящих принципов заключаются в оказании помощи государствам-членам в усилении национальных мер и активизации международного сотрудничества; не имеющие обязательной силы руководящие принципы не предполагают наложения на государства каких-либо юридических обязательств.

гуманитарному праву; подчеркнул, что эффективные контртеррористические меры и уважение прав человека, основных свобод и принципа верховенства права взаимно дополняют и подкрепляют друг друга и являются важнейшей частью успешных усилий по борьбе с терроризмом; и отметил важность учета гендерного фактора в качестве сквозного вопроса в соответствии с резолюцией 2617 (2021) Совета.

6. Настоящий набор не имеющих обязательной силы руководящих принципов разработан Контртеррористическим комитетом в стремлении оказать государствам-членам помощь в противодействии — в соответствии с нормами международного права — применению новых и новейших технологий в террористических целях.

7. Нижеследующие руководящие принципы призваны дополнить другие материалы в качестве ориентира для государств-членов и деятельности Контртеррористического комитета и его Исполнительного директората по оказанию поддержки государствам в выполнении ими резолюций Совета Безопасности 1373 (2001), 1624 (2005), 2178 (2014), 2370 (2017), 2396 (2017), 2462 (2019), 2617 (2021) и других соответствующих документов Совета по борьбе с терроризмом[2]. Многие из руководящих принципов, изложенных в настоящем документе, основаны на работе и рекомендованной передовой практике Совета Безопасности и Генеральной Ассамблеи, организаций — партнеров Организации Объединенных Наций и других ключевых заинтересованных сторон, таких как Группа разработки финансовых мер.

Угрозы, создаваемые использованием новых и новейших финансовых технологий в террористических целях

8. Как признал Совет Безопасности, инновации в сфере финансовых технологий могут открывать значительные экономические возможности[3]. Кроме того, они могут создавать риск их неправомерного использования, в том числе в террористических целях[4]. Растущие масштабы их неправомерного использования с тех пор были отмечены в нескольких докладах Организации Объединенных Наций, Группы разработки финансовых мер и региональных групп по типу Группы разработки финансовых, а также членами Глобальной контртеррористической исследовательской сети Исполнительного директората и партнерами из частного сектора[5].

---

[2] К ним относятся руководящие принципы в отношении иностранных боевиков-террористов (S/2015/939); добавление к руководящим принципам в отношении иностранных боевиков-террористов (2018 год) (S/2018/1177); техническое руководство по осуществлению резолюции 1373 (2001) Совета Безопасности и других резолюций (S/2019/998); рамочный документ, касающийся поездок Контртеррористического комитета в государства-члены (S/2020/731); и глобальный обзор осуществления государствами-членами резолюции 1373 (2001), публиковавшийся в 2009, 2011, 2016 и 2021 годах (S/2009/620, S/2011/463, S/2016/49 и S/2021/972).

[3] Резолюция 2462 (2019) Совета Безопасности, десятый пункт преамбулы; см. также Financial Action Task Force, *Opportunities and Challenges of New Technologies for AML/CFT* (Paris, 2021), URL: https://www.fatf-gafi.org/en/publications/Digitaltransformation/Opportunities-challenges-new-technologies-for-aml-cft.html.

[4] Резолюция 2462 (2019) Совета Безопасности, десятый пункт преамбулы; также подтверждается в резолюции 2617 (2021), двадцать пятый пункт преамбулы.

[5] Для получения более подробной информации см. восемнадцатый доклад Генерального секретаря об угрозе, создаваемой ИГИЛ (ДАИШ) для международного мира и безопасности, и о масштабах усилий Организации Объединенных Наций по оказанию поддержки государствам-членам в противодействии этой угрозе (S/2024/117), п. 14;

9. В зависимости от регионального и экономического контекста, имеющихся средств и целей, которые ставят перед собой террористы, масштабы и виды злоупотреблений значительно различаются с точки зрения источников и способов финансирования. В области финансирования терроризма набирает обороты тенденция к смешанному использованию старых и новых способов сбора и перемещения средств[6], и такая практика, по сути, сочетает в себе проблемы и сложности, связанные с каждым из способов, — от выявления физической трансграничной перевозки наличных денежных средств до отслеживания сложных виртуальных транзакций. Поэтому государствам следует применять комплексный и основанный на оценке рисков подход к противодействию финансированию терроризма (ПФТ), чтобы не пренебрегать гарантиями в отношении способов и каналов, используемых террористами. Таким образом, для ослабления множества факторов уязвимости, связанных с финансированием терроризма, необходимо наличие основанной на оценке рисков, актуальной и эффективной системы противодействия отмыванию денег и финансированию терроризма (ПОД/ФТ), соответствующей нормам международного права.

10. Примеры способов сбора средств на террористические цели с помощью новых и новейших технологий включают в себя использование в злонамеренных целях социальных сетей (их использование для сбора пожертвований с помощью традиционных способов оплаты), услуг размещения информации, онлайновой торговли товарами и краудфандинговых платформ[7]. В своем последнем докладе Группа разработки финансовых мер указала, что из всех различных форм краудфандинга наиболее вероятно использование в целях финансирования терроризма краудфандинга на основе пожертвований[8]. Четыре основные категории злонамеренного использования краудфандинга в целях финансирования

тридцать четвертый доклад Группы по аналитической поддержке и наблюдению за санкциями, представленный в соответствии с резолюцией 2734 (2024) по ИГИЛ (ДАИШ), «Аль-Каиде» и связанным с ними лицам и организациям (S/2024/556), пп. 94–97; Исполнительный директорат Контртеррористического комитета, информационный брифинг о последних тенденциях в использовании криптовалюты террористическими группами, связанными с ДАИШ (ИГИЛ)/«Аль-Каидой» и их сторонниками, 4 марта 2024 года (см. https://www.un.org/securitycouncil/ctc/news/cted-hosts-insight-briefing-%E2%80%9Clatest-trends-use-cryptocurrency-terrorist-groups-and-their); Financial Action Task Force, “Public statement on the financing of ISIL, Al Qaeda and affiliates”, 21 October 2021, and subsequent non-public updates; и Asia/Pacific Group on Money Laundering, *APG Yearly Typologies Report 2021* (Sydney, 2021), URL: www.apgml.org/includes/handlers/get-document.ashx?d=6bfd011b-8edd-40f4-93e4-f219e1c6d73e. См. также, например, Elliptic, *Preventing Financial Crime in Cryptoassets: Typologies Report 2022*, URL: www.elliptic.co/resources/typologies-report-2022; TRM, *Illicit Crypto Ecosystem Report* (2023), URL: www.trmlabs.com/illicit-crypto-ecosystem-report-2023; TRM, “Terrorist financing: six crypto-related trends to watch in 2023”, 16 February 2023, URL: https://www.trmlabs.com/post/terrorist-financing-six-crypto-related-trends-to-watch-in-2023; и TRM, “TRM finds mounting evidence of crypto use by ISIS and its supporters in Asia”, 21 July 2023, URL: https://www.trmlabs.com/post/trm-finds-mounting-evidence-of-crypto-use-by-isis-and-its-supporters-in-asia.

[6] Это также стало одним из важных выводов, сделанных по итогам последнего совместного совещания экспертов Группы разработки финансовых мер и проведенного совместно Группой разработки финансовых мер и Управлением Организации Объединенных Наций по наркотикам и преступности практикума по вопросам финансирования терроризма с помощью «хавалы» и аналогичных услуг (Нью-Дели, апрель 2023 года).

[7] S/2024/556, п. 94; см. ссылки на источники, приведенные на сайте www.un.org/securitycouncil/ctc/news/cted%E2%80%99s-tech-sessions-highlights-%E2%80%9Cthreats-and-opportunities-related-new-payment-technologies-0.

[8] Financial Action Task Force, *Crowdfunding for Terrorism Financing* (Paris, 2023), para. 38, URL: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Crowdfunding-Terrorism-Financing.pdf.coredownload.inline.pdf.

терроризма, указанные в докладе, включают следующее: использование в злонамеренных целях гуманитарной, благотворительной или некоммерческой деятельности; использование специальных краудфандинговых платформ или вебсайтов; использование социальных сетей и приложений для обмена сообщениями; и использование краудфандинга в сочетании с виртуальными активами. Тем не менее регулятивный надзор за сферой краудфандинга в мире по-прежнему носит фрагментарный характер, в том числе в части распространения на эту сферу правил, касающихся ПОД/ФТ[9]. Несмотря на неоднократные случаи использования террористами социальных сетей и краудфандинговых платформ для осуществления финансовой деятельности, с некоторыми платформами или приложениями для обмена сообщениями возникают трудности при адаптации систем самоконтроля и модерации контента для борьбы с финансированием терроризма, которое может осуществляться через соответствующие платформы или приложения[10]. Поскольку тенденции и подходы продолжают меняться, для сбора средств существуют и другие возможности, которые могут быть задействованы с помощью онлайн-технологий и использованы в террористических целях, например функция «суперчата» или рекламирование брендов и монетизация ресурсов путем размещения контента террористической направленности.

11. Исследователи, национальные власти и многосторонние директивные органы отмечают, что, хотя преобладающими способами перемещения средств в террористических целях остаются использование наличных средств и использование систем типа «хавала», на долю которых приходится бóльшая часть переводов, связанных с финансированием терроризма, наблюдается также рост использования этих способов в сочетании с новыми технологиями и способами совершения платежей. Мобильные платежные системы, виртуальные активы и онлайновые биржи и кошельки уже используются в террористических целях, и ожидается, что их использование в злонамеренных целях станет еще более распространенным и значительным[11]. Зачастую запутанный путь движения денежных средств при использовании этих способов создает сложности как для финансовых следователей, так и для финансовых учреждений в процессе их взаимодействия. Некоторые виртуальные активы позволяют осуществлять трансграничные переводы средств непосредственно между пользователями с использованием псевдонима[12] и без участия поставщика услуг по проведению операций с виртуальными активами. Эти риски усугубляются сохраняющимися пробелами в применении странами стандартов Группы разработки финансовых мер в отношении виртуальных активов и поставщиков услуг по проведению операций с виртуальными активами, прежде всего рекомендации 15 и соответствующей пояснительной записки. Хотя децентрализованные финансы и некастодиальные кошельки составляют лишь часть общей экосистемы виртуальных активов, они

[9] Ibid., paras. 27, 28 and 30. В докладе отмечается, что только в четырех юрисдикциях глобальной сети Группы разработки финансовых мер регулируется как инвестиционный, так и основанный на пожертвованиях краудфандинг в рамках их систем ПОД/ФТ.

[10] Например, согласно закону Европейского союза о цифровых услугах, крупные платформы обязаны проводить собственную оценку рисков и удалять незаконный контент по получении уведомления от властей, однако в этом законе нет прямого указания на финансирование терроризма как на разновидность незаконного контента. Как отмечалось на вышеупомянутых совещаниях экспертов, платформа GoFundMe в настоящее время является единственной краудфандинговой платформой, в правилах которой содержатся конкретные положения, касающиеся финансирования терроризма.

[11] S/2024/556, п. 95.

[12] Информацию об использовании ИГИЛ и связанными с ней группами криптовалют с повышенной анонимностью (также известных как анонимные криптовалюты), в частности Monero — криптовалюты, использующей криптографические технологии, предназначенные для сокрытия деталей операций, см. там же, пп. 96 и 97.

несут в себе риски, связанные с финансированием терроризма и другими финансовыми преступлениями. Некоторые юрисдикции сообщили о трудностях, связанных с уменьшением этих рисков.

12. Совет Безопасности призвал все государства-члены оценить и устранить потенциальные риски, связанные с использованием виртуальных активов, а в соответствующих случаях — и риски, связанные с использованием новых финансовых инструментов, включая, в частности, краудфандинговые платформы, которые могут использоваться в злонамеренных целях для финансирования терроризма, и принять меры к обеспечению того, чтобы на поставщиков таких услуг распространялись обязательства, касающиеся ПОД/ФТ[13].

13. Кроме того, Совет Безопасности настоятельно призвал все государства-члены выполнять всеобъемлющие международные стандарты, закрепленные в пересмотренных 40 рекомендациях по противодействию отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения, сформулированных Группой разработки финансовых мер[14]. В рекомендации 15, касающейся новых технологий (пересмотрена в 2018 году и дополнена пояснительной запиской в 2019 году) указано, что странам и финансовым учреждениям необходимо выявлять 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. Для управления рисками, возникающими в связи с виртуальными активами[15], и их снижения страны должны принять меры к обеспечению того, чтобы деятельность поставщиков услуг по проведению операций с виртуальными активами регулировалось в целях ПОД/ФТ и чтобы поставщики таких услуг были лицензированы или зарегистрированы и имели эффективные системы мониторинга и обеспечения соблюдения соответствующих мер, предусмотренных рекомендациями Группы разработки финансовых мер, либо чтобы в противном случае их деятельность была запрещена в соответствующей стране[16]. В феврале 2023 года Группа разработки финансовых мер приняла дорожную карту для улучшения выполнения рекомендации 15. Однако, согласно результатам анализа, проведенного Группой разработки финансовых мер, по состоянию на июнь 2024 года многие юрисдикции не добились достаточного прогресса в выполнении основных требований Группы в отношении виртуальных активов и поставщиков услуг по проведению операций с виртуальными активами[17].

---

[13] Резолюция 2462 (2019), п. 20 d).

[14] Там же, п. 4.

[15] Более подробная информация представлена в публикации Financial Action Task Force, Focus on Virtual Assets, URL: https://www.fatf-gafi.org/en/topics/virtual-assets.html.

[16] Более подробная информация представлена в публикации Financial Action Task Force, “Targeted update on implementation of the FATF standards on virtual assets and virtual asset service providers”, June 2024, pp. 4 and 5, URL: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2024.html; и в публикации Financial Action Task Force, *Updated Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers* (Paris, 2021), paras. 31–43.

[17] Financial Action Task Force, “Targeted update on implementation of the FATF standards on virtual assets and virtual asset service providers”. В своем докладе Группа разработки финансовых мер отмечает, что, несмотря на прогресс, достигнутый некоторыми юрисдикциями во внедрении правил, касающихся ПОД/ФТ, в глобальном масштабе эти правила применяются все еще в недостаточной степени. Правительствам некоторых стран еще предстоит предпринять какие-либо существенные шаги по регулированию этого сектора, и этим странам необходимо уделять первоочередное внимание внедрению в срочном порядке стандартов Группы разработки финансовых мер в полном объеме.

14. Кроме того, Совет Безопасности призвал использовать все возможности, открывающиеся благодаря новым и новейшим финансовым и регуляторным технологиям, для расширения доступа к финансовым услугам и содействия эффективной реализации мер в области ПОД/ФТ в соответствии с международным правом. Так, как показала работа Группы разработки финансовых мер, новые технологии также способны обеспечить более оперативное принятие мер в области ПОД/ФТ, удешевить такие меры, сделать их более прозрачными и повысить степень их инклюзивности как в государственном, так и в частном секторе при обеспечении их надежности и безопасности[18]. При ответственном и соразмерном использовании технологии могут облегчить сбор, обработку и анализ данных и помочь субъектам выявлять риски финансирования терроризма и управлять такими рисками более эффективным образом и в более близком к реальному времени режиме[19].

15. Важно также напомнить, что Совет Безопасности потребовал «от государств-членов обеспечения того, чтобы все меры, принимаемые для противодействия терроризму, включая меры, принимаемые для противодействия финансированию терроризма в соответствии с настоящей резолюцией, сообразовывались с их обязательствами по международному праву, включая международное гуманитарное право, международное право прав человека и международное беженское право»[20]. Совет далее настоятельно призвал к тому, чтобы, «вырабатывая и применяя меры по противодействию финансированию терроризма, государства принимали во внимание потенциальное воздействие этих мер на сугубо гуманитарную деятельность, в том числе медицинскую, которая проводится беспристрастными гуманитарными субъектами сообразно с международным гуманитарным правом»[21]. Кроме того, при разработке и осуществлении мер по

Согласно данным из 130 докладов о взаимной оценке и последующих мерах, опубликованных после принятия пересмотренной рекомендации 15 в 2019 году, 75 процентов юрисдикций соблюдают лишь частично или не соблюдают требования Группы разработки финансовых мер, что соответствует показателю по состоянию на апрель 2023 года (75 процентов, или 73 из 98 юрисдикций соблюдают частично или не соблюдают указанные требования) и свидетельствует о практически полном отсутствии улучшений. См. также Financial Action Task Force, “Status of implementation of recommendation 15 by FATF members and jurisdictions with materially important VASP activity”, March 2024, URL: https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/VACG-Table-Jurisdictions-2024.pdf.coredownload.pdf; Counter-Terrorism Committee Executive Directorate, “Thematic summary assessment of gaps in implementing key countering the financing of terrorism provisions of Security Council resolutions”, December 2022, pp. 16–18, URL: www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/cted_2022_cft_gaps_assessment_final.pdf.

[18] См. также Financial Stability Board, “G20 roadmap for enhancing cross-border payments: priority actions for achieving the G20 targets”, 23 February 2023, URL: https://www.fsb.org/2023/02/g20-roadmap-for-enhancing-cross-border-payments-priority-actions-for-achieving-the-g20-targets/.

[19] См., например, Financial Action Task Force, *Opportunities and Challenges of New Technologies for AML/CFT*.

[20] Резолюция 2462 (2019), п. 6; см. также резолюцию 2617 (2021), в которой Совет Безопасности напомнил о важности полного уважения прав на свободное выражение мнений и свободу ассоциации с другими лицами в рамках гражданского общества, а также на свободу религии или убеждений и подчеркнул важность принятия в отношении некоммерческих организаций эффективных и соразмерных мер по противодействию финансированию терроризма.

[21] Резолюция 2462 (2019), п. 24; см. также резолюцию 2482 (2019), п. 16, согласно которому это требование распространяется на все меры, принимаемые для противодействия терроризму. Кроме того, некоторые финансовые операции, определенные в пункте 1 резолюции 2664 (2022) и необходимые для обеспечения своевременной доставки

противодействию финансированию терроризма государства-члены должны принимать во внимание непредвиденные последствия и воздействие на гуманитарную деятельность и права человека, а также на законную деятельность некоммерческих организаций и гражданского общества.

16. Учитывая темпы развития новых и новейших финансовых технологий, позволяющих осуществлять трансграничное перемещение средств в режиме реального времени, государствам-членам следует разработать меры по выявлению соответствующих угроз, их оценке и противодействию им, пока в рамках глобальной системы регулирования не будут выработаны механизмы контроля и требования к представлению отчетности в отношении соответствующих организаций. Необходимо расширять обмен информацией и опытом в этой области между соответствующими органами, гражданским обществом, академическими кругами и частным сектором; наращивать международное сотрудничество и оказание взаимной правовой помощи; углублять понимание возникающих рисков; анализировать возможности, которые открываются благодаря современным финансовым технологиям, и связанные с ними риски в контексте борьбы с терроризмом; и изучать пути обеспечения более комплексного глобального подхода.

Не имеющий обязательной силы руководящий принцип 1: углубление понимания рисков финансирования терроризма, связанных с новыми и новейшими финансовыми технологиями и способами сбора средств

17. Понимание характера и масштабов указанной угрозы остается первым и важнейшим шагом для выработки соответствующих ответных мер, особенно учитывая потенциальные преимущества этих технологий в том, что касается борьбы с терроризмом и противодействию его финансированию. Способы использования новых технологий террористами могут существенно различаться в зависимости от близости террористов и масштабов террористической деятельности, доступности технологий, финансовых потребностей террористов, а также региональных и экономических условий. Уделение чрезмерного внимания рискам, связанным с определенными видами новых продуктов или услуг, при одновременном игнорировании более традиционных и широко используемых для целей финансирования терроризма продуктов и услуг[22] не соответствует подходу, основанному на оценке риска. Поэтому понимание рисков должно опираться на оценку финансовой стратегии террористов с учетом конкретных условий, с тем чтобы выяснить, как, когда и почему террористы используют новые и новейшие технологии для финансирования своей деятельности. Ответные меры, основанные на предполагаемых, а не на доказанных рисках финансирования терроризма, зачастую являются ненужными и несоразмерными тем преимуществам, которые обеспечивают новые финансовые технологии, включая их

гуманитарной помощи или для содействия осуществлению других видов деятельности, способствующих удовлетворению основных человеческих потребностей человека, разрешены в случаях, когда действуют целевые финансовые санкции Совета Безопасности, и не являются нарушением соответствующих мер по замораживанию активов (см. также резолюцию 2761 (2024)).

[22] Террористы продолжают получать средства различными способами, в том числе под прикрытием законной предпринимательской деятельности, путем эксплуатации природных ресурсов, под прикрытием некоммерческих организаций, в виде пожертвований и в виде доходов от преступной деятельности, такой как похищение людей с целью получения выкупа, вымогательство и торговля людьми, культурными ценностями, наркотиками и оружием. Средства, связанные с финансированием терроризма, по-прежнему перемещаются через официальные финансовые учреждения, неофициальные системы и курьеров, перевозящих наличные деньги.

потенциал для решения проблемы финансовой изоляции, и чреваты нарушением международного права, в том числе международного права прав человека.

18. В рамках своих усилий по анализу угроз, рисков и уязвимостей, связанных с использованием новых и новейших финансовых технологий в целях финансирования терроризма, государствам-членам следует рассмотреть:

a) возможность проведения регулярных, всеохватных и основанных на фактических данных национальных оценок рисков финансирования терроризма с учетом уникальной оперативной обстановки и условий в каждом государстве, а также глобальных и региональных тенденций в области финансирования терроризма. Для поддержания актуальности необходимо периодически проводить комплексные оценки рисков (и дополнять их отраслевыми оценками рисков в надлежащих случаях);

b) возможность включения в свои национальные оценки рисков анализа рисков финансирования терроризма, связанных с новыми и новейшими платежными технологиями и способами сбора средств, и выявлять уязвимости конкретных продуктов и услуг согласно резолюции 2462 (2019) и соответствующим рекомендациям Группы разработки финансовых мер;

c) возможность расширения исследований и анализа соответствующих угроз, связанных с финансированием терроризма, с максимально широким охватом различных террористических групп, включая те, деятельность которых мотивирована ксенофобией, расизмом и другими формами нетерпимости, или которые действуют во имя религии или убеждений, и отслеживать региональные и глобальные тенденции[23], а также стремиться выявлять методы и инструменты финансирования, используемые отдельными группами;

d) возможность проведения активной работы с международными партнерами в юрисдикциях, где были выявлены связи с финансированием терроризма;

e) возможность использования подхода с участием многих заинтересованных сторон, включая эффективное взаимодействие и обмен мнениями между соответствующими национальными органами, частным сектором, гражданским обществом и академическими кругами, с тем чтобы получить всеобъемлющую картину существующих и меняющихся рисков финансирования терроризма с учетом разнообразия опыта и точек зрения и лучше понять как преимущества этих технологий, так и масштабы угрозы и последствия для различных секторов и групп населения, включая местные общины, а также реалии конкретного региона, что позволит выработать индивидуальные и соразмерные ответные меры;

f) возможность проведения основанных на фактических данных оценок рисков финансирования терроризма, связанных с социальными сетями. Это включает в себя определение конкретных функций, используемых для интеграции с платежными сервисами[24];

g) возможность изучения представленных соответствующими многосторонними организациями современных методик проведения регулярных, всесторонних и основанных на фактических данных национальных оценок рисков

[23] См. также S/2021/972, приложение, п. 668.

[24] См. также Asia/Pacific Group on Money Laundering and Middle East and North Africa Financial Action Task Force, “Social media and terrorism financing”, January 2019, URL: www.apgml.org/includes/handlers/get-document.ashx?d=2446bd89-b2cc-4c3c-b378-5f03658dc906.

финансирования терроризма и при необходимости обращаться за технической помощью в проведении таких оценок;

h) возможность проведения работы по информированию всех соответствующих секторов и заинтересованных сторон о выявленных преимуществах, рисках и уязвимостях;

i) возможность принятия мер по обеспечению того, чтобы финансовые учреждения проводили собственную оценку рисков до представления новых продуктов, внедрения новой деловой практики либо использования новых или разрабатываемых технологий, и соответствующих мер по управлению этими рисками и их снижению, как указано в рекомендации 15 Группы разработки финансовых мер.

Не имеющий обязательной силы руководящий принцип 2: разработка и внедрение основанного на оценке рисков, соразмерного регулирования, мониторинга и надзора для предотвращения злонамеренного использования новых технологий в целях финансирования терроризма

19. Как отмечалось в ходе консультаций по подготовке этих не имеющих обязательной силы руководящих принципов, государства должны постоянно пересматривать и при необходимости адаптировать свои существующие нормативно-правовые акты, чтобы обеспечить их актуальность, целенаправленность и эффективность для устранения уязвимостей, возникающих в связи с появлением новейших финансовых технологий. Для успешного выполнения этой задачи ответные меры государств должны быть целенаправленными, должны быть основаны на оценке рисков, проведенной исходя из фактических данных, а не предполагаемых уязвимостей, и должны соответствовать подходу, основанному на оценке рисков, согласно стандартам Группы разработки финансовых мер. Кроме того, они должны носить сбалансированный характер с учетом потенциала новых финансовых технологий в плане расширения доступа к финансовым услугам как одного из ключевых факторов достижения различных целей в области устойчивого развития, а также для внедрения новаторских способов совершения платежей и средств для их безопасного осуществления в кризисных ситуациях. Как отметила Группа разработки финансовых мер, «инновационные финансовые технологии и другие финансовые продукты могут содействовать осуществлению деятельности [некоммерческих организаций], особенно доставке помощи в труднодоступные районы» и способствовать обеспечению большей отслеживаемости финансовых операций, «тем самым не только снижая риск перенаправления денежных средств, но и способствуя обеспечению надежного контрольного следа для доставки помощи»[25]. И наоборот, несоразмерно ограничительные регулирование цифровых платежных платформ и надзор за ними могут неоправданно ограничивать права человека и препятствовать предоставлению беспристрастными гуманитарными организациями в соответствии с международным гуманитарным правом гуманитарной помощи тем, кто в ней больше всего нуждается, особенно в районах, пострадавших от конфликтов или терроризма, где недоступны банковские или иные регулируемые финансовые услуги. Без надлежащих сдержек и противовесов, включая мониторинг и надзор, чрезмерное регулирование цифровых платежных услуг может стать тяжелым бременем в том, что касается гуманитарной работы и законной экономической

[25] Financial Action Task Force, *Best Practices: Combating the Terrorist Financing Abuse of Non-Profit Organizations* (Paris, 2023), para. 129, URL: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/BPP-Combating-TF-Abuse-NPO-R8.pdf.coredownload.inline.pdf.

деятельности или деятельности некоммерческих организаций[26]. Совет Безопасности в своей резолюции 2462 (2019) с большой обеспокоенностью отметил злонамеренное использование террористами некоммерческих организаций для сбора, перемещения и перевода средств; призвал государства-члены применять подход, основанный на оценке рисков, и работать в сотрудничестве с некоммерческим сектором над недопущением использования таких организаций, в том числе подставных, террористами и в интересах террористов; и напомнил о соответствующих рекомендациях и имеющихся руководящих документах Группы разработки финансовых мер на этот счет, в частности о ее рекомендации 8. Группа разработки финансовых мер также отметила, что стремление минимизировать негативные последствия для законных бенефициаров деятельности некоммерческих организаций не отменяет необходимости принятия незамедлительных и эффективных мер для решения безотлагательной задачи, заключающейся в прекращении финансирования терроризма или других форм поддержки терроризма со стороны некоммерческих организаций[27]. Основная цель рекомендации 8 Группы разработки финансовых мер заключается в обеспечении того, чтобы некоммерческие организации не использовались террористами.

20. В своих усилиях по обеспечению надлежащего регулирования деятельности поставщиков новых и новейших платежных услуг, мониторинга их деятельности и надзора за их деятельностью государствам-членам следует рассмотреть:

a) возможность разработки основанных на оценке рисков систем регулирования и надзора для соответствующих секторов, включая поставщиков услуг по проведению операций с виртуальными активами, в соответствии с резолюциями Совета Безопасности и стандартами Группы разработки финансовых мер, а также в полном соответствии с нормами международного права;

b) возможность проведения постоянного анализа существующих нормативно-правовых документов со всеми соответствующими заинтересованными сторонами, с тем чтобы эти документы оставались актуальными с учетом новых и меняющихся рисков, и распространения действия таких документов на поставщиков новых и новейших услуг, сообразно обстоятельствам, с выявлением пробелов и возможного дублирования усилий или чрезмерного регулирования;

c) возможность укрепления механизмов, обеспечивающих межведомственное сотрудничество, в целях активизации своевременного обмена оперативной финансовой информацией на национальном и международном уровнях[28] в соответствии с применимыми рекомендациями Группы разработки финансовых мер;

d) возможность обеспечения того, чтобы национальные системы ПОД/ФТ, основанные на оценке рисков, охватывали поставщиков услуг по проведению операций с виртуальными активами в соответствии со стандартами Группы разработки финансовых мер для обеспечения отслеживаемости операций, в том числе путем внедрения так называемого «правила контроля переводов Группы разработки финансовых мер», которое требует от поставщиков услуг по проведению операций с виртуальными активами и других финансовых

[26] В этой связи и со ссылкой на резолюцию 2462 (2019) Группа разработки финансовых мер также признает важность обеспечения того, чтобы выполнение ее рекомендаций, в частности рекомендации 8, призванной не допустить использования некоммерческих организаций террористами и террористическими организациями, не оказывало негативного и непропорционального воздействия на некоммерческие организации и не создавало неоправданных препятствий для деятельности гражданского общества и оказания гуманитарной помощи (ibid., para. 113).

[27] Группа разработки финансовых мер, пояснительная записка к рекомендации 8, п. 5 d).

[28] См. также резолюцию 2462 (2019); и S/2021/972, приложение, п. 673.

учреждений обмениваться соответствующей информацией об отправителе и получателе при совершении определенных операций с виртуальными активами;

e) возможность разработки надлежащих и эффективных национальных рамок и механизмов для выявления незарегистрированных поставщиков, предоставляющих новые и новейшие финансовые услуги и осуществляющих операции с денежными средствами с использованием новых технологий;

f) возможность повышения эффективности контроля за соблюдением зарегистрированными поставщиками финансовых услуг, использующими новые и новейшие технологии (включая операторов, предоставляющих услуги мобильных денежных переводов), путем разработки эффективных программ надзора за соблюдением требований, в том числе путем обеспечения надлежащей подготовки сотрудников и соблюдения принципа должной осмотрительности в отношении клиентов;

g) возможность тестирования рыночных инноваций на предмет их соответствия потребностям целевых аудиторий при соблюдении нормативных стандартов (например, использовать так называемые «регулятивные песочницы», позволяющие при определенных условиях предоставлять тот или иной продукт при отсутствии возражений со стороны регулирующего органа). При совместной работе такие механизмы позволят частному сектору и регулирующим органам сообща выявлять риски, добиваться взаимопонимания и тестировать нормативно-правовую базу;

h) возможность разработки нормативно-правовых документов для отслеживания, выявления и пресечения случаев злонамеренного использования социальных сетей в целях финансирования терроризма при полном соблюдении применимого международного права;

i) возможность проведения на постоянной основе информационно-разъяснительной работы среди соответствующих поставщиков услуг и других потенциально уязвимых сторон, на которых не распространяются обязательства по представлению отчетности в сфере ПОД/ФТ, включая социальные сети и некоторые краудфандинговые платформы, в целях информирования их о связанных с финансированием терроризма рисках, категориях и тревожных сигналах, а также о действующих правилах и имеющихся инструментах для снижения рисков и/или сообщения о подозрительной деятельности;

j) возможность использования многостороннего подхода с активным участием, в частности, частного сектора, гражданского общества и общественности при разработке мер по снижению рисков финансирования терроризма.

Не имеющий обязательной силы руководящий принцип 3: эффективное выявление и пресечение злонамеренного использования новых технологий в целях финансирования терроризма

21. Государствам следует избегать политизации вопросов международного сотрудничества в борьбе с терроризмом, в том числе в сфере ПОД/ФТ, и продолжать наращивать свой потенциал для эффективного выявления и пресечения злонамеренного использования новых технологий в целях финансирования терроризма, в том числе путем проведения расследований и обеспечения уголовного преследования виновных, укрепления межведомственного и международного сотрудничества, создания и использования соответствующих механизмов оказания взаимной правовой помощи и развития государственно-частного

партнерства. Как отмечает Группа разработки финансовых мер[29], стратегии пресечения финансирования терроризма включают в себя широкий спектр инструментов и практик, применяемых многочисленными органами по борьбе с терроризмом/пресечению финансирования терроризма, действующими в координации друг с другом и своевременно обменивающимися информацией. В этом отношении основополагающую роль в разработке и реализации эффективных стратегий пресечения финансирования терроризма играют национальные координационные комитеты. Национальная стратегия борьбы с терроризмом/пресечения финансирования терроризма, основанная на тщательной и актуальной оценке рисков, обеспечивает рамочную основу для оперативного сотрудничества между соответствующими ведомствами, а также между соответствующими ведомствами и частным сектором, в том числе в отношении новых и новейших финансовых технологий. Таким образом, стратегии пресечения финансирования терроризма выходят за рамки проведения следственных действий при выявлении нарушений и направлены на использование всего спектра междисциплинарных правовых, административных и политических мер для пресечения деятельности террористических групп и снижения их оперативного потенциала. Спектр целенаправленных мер по пресечению финансирования терроризма может включать в себя введение целевых финансовых санкций; выпуск непубличных рекомендаций и предупреждений; создание препятствий для физического перемещения и хранения денежных средств; применение уголовных санкций против террористов, пособников и тех, кто их финансирует; и применение конфискации без вынесения обвинительного приговора в отношении структур, связанных с терроризмом. Соответствующие ответные меры будут зависеть от особенностей каждого способа финансирования и причастных к финансированию субъектов.

22. В своих усилиях по эффективному выявлению и пресечению злонамеренного использования новых технологий в целях финансирования терроризма государствам-членам следует рассмотреть:

a) возможность разработки межведомственных и, в надлежащих случаях, многосторонних координационных механизмов, охватывающих соответствующие директивные органы, судебные и правоохранительные органы, подразделения финансовых расследований, надзорные и регулирующие органы, для обмена информацией и оперативными данными[30];

b) возможность создания рамок и процедур для механизмов обратной связи между правоохранительными органами, подразделениями финансовой разведки и представляющими отчетность организациями из соответствующих секторов для повышения качества отчетности и данных финансовой разведки, а также для содействия отслеживанию тенденций и проведению стратегического анализа;

c) возможность развития и укрепления на постоянной основе потенциала соответствующих национальных органов для более эффективного отслеживания денежных средств, в том числе путем проведения параллельных финансовых расследований по делам о терроризме, с использованием новых аналитических методов, инструментов и технологий, а также необходимых независимых механизмов надзора и проверки. Необходимо продолжать инвестировать в технологии и обучение, мобилизовать лучших специалистов, а также вкладывать средства в технологии повышения конфиденциальности для защиты конфиденциальной информации;

[29] Financial Action Task Force, “Terrorist financing disruption strategies”, October 2018 (непубличный доклад).

[30] См. также резолюцию 2462 (2019), п. 19.

d) пути обеспечения оптимального использования всех возможностей, открывающихся благодаря новым и новейшим финансовым и регуляторным технологиям, для содействия эффективной реализации мер в области ПОД/ФТ[31]. Технологии должны использоваться ответственно, чтобы облегчить сбор, обработку и анализ данных и помочь в выявлении рисков финансирования терроризма и управлении такими рисками более эффективным образом и в более близком к реальному времени режиме;

e) возможность установления соответствующих гарантий и характеристик для новых решений в области ПОД/ФТ, включая подотчетность и прозрачность процессов и результатов, надзор со стороны людей, конфиденциальность и защиту данных[32], а также соответствие глобальным техническим стандартам и передовой практике;

f) возможность разработки и внедрения правил и процедур для правоохранительных и других компетентных органов по расследованию случаев использования Интернета и социальных сетей для финансирования терроризма и своевременному получению доступа к доказательствам в полном соответствии с применимым международным правом[33]. Расширение возможностей по проведению расследований в отношении социальных сетей в связи с финансированием терроризма имеет большое значение, равно как и разработка специальных регламентов для взаимодействия с операторами и поставщиками услуг в других юрисдикциях[34];

g) возможность обеспечения того, чтобы существующие механизмы, позволяющие безотлагательно выполнять требования о замораживании активов террористов, фактически распространялись на активы, которые были получены с помощью новых и новейших финансовых технологий, включая виртуальные активы, при наличии надлежащей правовой процедуры и процессуальных гарантий;

h) возможность включения адресов кошельков, непосредственно связанных с лицами, отнесенными к террористам, или структурами, отнесенными к террористическим, в идентификационную информацию, передаваемую частному сектору;

i) возможность оперативного обмена информацией по типу раннего предупреждения и, при необходимости, оперативной финансовой информацией между государствами[35], в том числе в отношении подозрительной деятельности поставщиков услуг по проведению операций с виртуальными активами, учитывая трансграничный характер угрозы;

---

[31] См. Financial Action Task Force, *Opportunities and Challenges of New Technologies for AML/CFT*.

[32] См. также рекомендацию 2 Группы разработки финансовых мер, в которой подчеркивается, что обмен информацией должен включать сотрудничество и координацию между соответствующими органами «для обеспечения соответствия требований [в области противодействия финансированию терроризма] правилам в отношении защиты данных и конфиденциальности и другим аналогичным положениям (например, в отношении обеспечения безопасности данных/локального хранения и обработки данных)».

[33] См. также Asia/Pacific Group on Money Laundering and Middle East and North Africa Financial Action Task Force, “Social media and terrorism financing”.

[34] См. также Tom Keatinge and Florence Keen, “Social media and terrorist financing: what are the vulnerabilities and how could public and private sectors collaborate better?”, Global Research Network on Terrorism and Technology: Paper No. 10 (Royal United Services Institute for Defence and Security Studies, 2019), доступно на веб-сайте https://static.rusi.org/20190802_grntt_paper_10.pdf.

[35] См. также резолюцию 2462 (2019), п. 28 a).

j) пути использования в полной мере международных и региональных инструментов для обмена информацией и сотрудничества, включая соответствующие базы данных и аналитические досье Международной организации уголовной полиции, и возможность обмена приобретенным опытом и знаниями для их использования другими государствами-членами;

k) возможность укрепления сотрудничества с Исполнительным директоратом Контртеррористического комитета, Группой разработки финансовых мер, региональными органами, созданными в рамках Группы разработки финансовых мер, и другими соответствующими международными и региональными организациями для изучения дальнейших путей повышения эффективности международных мер в ответ на использование новых способов совершения платежей и сбора средств в террористических целях и дальнейших путей налаживания регулярного обмена действенными наработками в этой области;

l) возможность налаживания надежного государственно-частного партнерства для обмена информацией, углубления понимания формирующихся тенденций, повышения уровня знаний и навыков соответствующих экспертов и заинтересованных сторон, включая специалистов по контролю, и содействия укреплению целостности финансового сектора[36]. Такое партнерство должно включать в себя диалог между подразделениями финансовой разведки и соответствующим сектором финансовых технологий в отношении обмена данными в рамках процедуры сообщения о подозрительной деятельности[37] при наличии четкой правовой основы для обмена информацией, включая критерии и цели, для которых информация может быть передана, и структуры, которым она может быть передана. Что касается социальных сетей, то такое государственно-частное партнерство помогает обеспечить со стороны социальных сетей основанные на имеющейся информации и эффективные усилия в области ПОД/ФТ[38]. Государственно-частное партнерство также обеспечивает властям полезную возможность для распространения регулярных рекомендаций для частного сектора, включая индикаторы риска;

m) возможность опереться на эффективное государственно-частное партнерство для использования имеющихся технологий и данных, включая блокчейн, в целях повышения результативности оперативного и тактического анализа, выявления финансовых сетей террористов, а также отслеживания подозрительной деятельности и сообщения о ней.

Не имеющий обязательной силы руководящий принцип 4: проведение оценки воздействия мер по противодействию финансированию терроризма на новые и новейшие технологии

23. Перед регулирующими органами стоит сложная задача, заключающаяся в том, чтобы найти баланс между необходимостью поощрять развитие новых

[36] См. там же, п. 22. В ходе технических заседаний, проходивших под руководством Исполнительного директората Контртеррористического комитета, в качестве примера успешной практики сотрудничества и обмена информацией между государственным и частным секторами был приведен опыт Целевой группы по борьбе с финансированием терроризма Экспертного центра по финансовым вопросам Королевства Нидерландов. В целом, в тех государствах, где налажено активное государственно-частное партнерство, отмечается повышение качества и увеличение количества поступающих сообщений о подозрительных операциях, связанных с финансированием терроризма. См. также S/2020/493, п. 68; и S/2021/972, приложение, п. 677.

[37] См. также Stephen Reimer and Matthew Redhead, *Bit by Bit: Impacts of New Technologies on Terrorism Financing Risks*, RUSI Occasional Paper (Royal United Services Institute for Defence and Security Studies, 2022).

[38] См. также Keatinge and Keen, “Social media and terrorist financing”.

платежных технологий на благо общества и необходимостью обеспечить эффективную систему регулирования, предотвращающую злонамеренное использование таких технологий в преступных и террористических целях. Как отмечалось выше, технологии способны улучшить отслеживаемость финансовых операций и упростить соблюдение принципа должной осмотрительности в банковской сфере и тем самым могут уменьшить нагрузку и задержки в работе некоммерческих организаций и гуманитарных структур. В то же время, как подчеркивает Группа разработки финансовых мер, необходимо «обеспечить, чтобы эти технологические решения не носили дискриминационного характера и не использовались дискриминационным образом»[39].

24. В своих усилиях по оценке воздействия новых мер в области ПОД/ФТ, связанных с новыми технологиями, и их любых непредвиденных последствий в том, что касается прав человека, доступности финансовых услуг, законной деятельности некоммерческих организаций, а также исключительно гуманитарной деятельности, осуществляемой беспристрастными гуманитарными организациями в соответствии с международным гуманитарным правом[40], и для эффективного смягчения этих последствий государствам следует рассмотреть:

a) возможность внедрения четких, прозрачных, соответствующих международным стандартам в области прав человека и учитывающих гендерную специфику инструкций, обеспечивающих рекомендации относительно использования новых технологий и тщательный учет потенциальных рисков и последствий;

b) возможность использования подхода с участием многих заинтересованных сторон при проведении анализа любого потенциального и фактического негативного воздействия связанных с новыми технологиями мер в области противодействия финансированию терроризма на права человека и при осуществлении активного регулирования такого воздействия, возможность разработки руководящих принципов, инструментов анализа и контрольных показателей для оценки такого воздействия и возможность разработки мер по смягчению такого воздействия с привлечением соответствующих национальных органов, частного сектора, гражданского общества и академических кругов. Кроме того, наличие специальных механизмов, платформ или каналов может помочь гражданскому обществу и другим заинтересованным сторонам действенным образом сообщать о любых непредвиденных негативных последствиях новых мер в области противодействия финансированию терроризма для осуществления ими своих прав и законной деятельности и в соответствующих случаях добиваться их пересмотра в судебном порядке;

c) возможность обеспечения при разработке систем и процессов обработки данных, облегчающих доступ к соответствующей информации и ее поиск и анализ (в том числе с использованием машинного обучения и автоматизации выявления рисков финансовых преступлений), наличия рамок и протоколов обмена данными для содействия обмену информацией между различными структурами, участвующими в работе по противодействию финансированию терроризма, в соответствии с международным правом прав человека;

[39] Financial Action Task Force, *Best Practices: Combating the Terrorist Financing Abuse of Non-Profit Organizations*, para. 129. Группа разработки финансовых мер отмечает, в частности, что «при использовании алгоритмов может потребоваться человеческий контроль, чтобы избежать закрепления существующих предубеждений (религиозных, этнических, гендерных и прочих)».

[40] См. также резолюцию 2462 (2019), пятый пункт преамбулы и пп. 23 и 24.

d) возможность применения — при проведении оценки эффективности — основанного на данных и всеохватного подхода для получения значимых результатов. Регулярно изучая и анализируя соответствующие данные, директивные органы и заинтересованные стороны могут выявлять области, требующие улучшения, совершенствовать стратегии и повышать общую эффективность усилий по противодействию финансированию терроризма;

e) возможность укрепления — по мере развития финансовых технологий и расширения их использования в сфере ПОД/ФТ — механизмов независимого надзора и подотчетности в отношении соответствующих мер при соблюдении надлежащей правовой процедуры и процессуальных гарантий. Механизмы надзора должны также обеспечивать соблюдение соответствующими государственно-частными партнерствами обязательств в области защиты данных или сохранения конфиденциальности данных в соответствии с национальным законодательством и применимым международным правом;

f) пути обеспечения того, чтобы меры, направленные на устранение выявленных рисков финансирования терроризма, связанных с новыми платежными технологиями, не приводили к необоснованному нарушению законной деятельности некоммерческих организаций или к негативным последствиям для нее. Государствам следует рассмотреть вопрос о том, можно ли использовать для устранения этих новых рисков и уязвимостей целевые, соразмерные и основанные на оценке рисков меры, уже принятые в отношении подгруппы некоммерческих организаций, определенной Группой разработки финансовых мер [41], включая меры по саморегулированию и внутреннему снижению рисков;

g) возможность создания постоянных механизмов, платформ или каналов, позволяющих гражданскому обществу и другим заинтересованным сторонам сообщать о любых непредвиденных негативных последствиях новых мер в области противодействия финансированию терроризма для осуществления ими своих прав и законной деятельности и в соответствующих случаях добиваться их пересмотра в судебном порядке. Информационно-разъяснительная работа должна включать в себя содержательный и основанный на сотрудничестве диалог между правительством, частным сектором и гражданским обществом, в том числе по непредвиденным проблемам и последствиям;

---

[41] Для целей рекомендации 8 Группы разработки финансовых мер «некоммерческая организация» означает юридическое лицо или образование либо организацию, которые главным образом занимаются сбором или распределением средств в таких целях, как благотворительные, религиозные, культурные, образовательные, социальные или «братские цели», или для осуществления других видов «добрых дел». Эта рекомендация была пересмотрена в 2016 году, чтобы уточнить подгруппу некоммерческих организаций, которые должны являться объектом надзора и мониторинга. В рекомендации 8 и пояснительной записке к ней, дополнительно пересмотренных в ноябре 2023 года, содержится призыв к принятию «целевых, соразмерных и основанных на оценке риска мер, не приводящих безосновательно к нарушению законной деятельности [некоммерческих организаций] и возникновению препятствий для такой деятельности», с тем чтобы защитить сектор некоммерческих организаций от использования в целях финансирования терроризма. Согласно пояснительной записке к рекомендации 8 Группы разработки финансовых мер (п. 6):

«НКО [некоммерческие организации] в силу своего типа, своей деятельности или своих характеристик в различной степени подвержены риску использования в целях ФТ [финансирования терроризма], при этом большинству из них может быть присуща низкая степень риска. Без ущерба для требований, содержащихся в рекомендации 1:

a) страны должны определить организации, которые подпадают под определение «НКО» ФАТФ;

b) страны должны провести оценку рисков в отношении этих НКО, чтобы определить характер присущих им рисков ФТ».

h) возможность обеспечения того, чтобы новые правила, направленные на повышение отслеживаемости и прозрачности финансовых операций, не нарушали право на свободу от незаконного или произвольного вмешательства в частную жизнь и другие права человека и не приводили к слежке за получателями гуманитарной помощи, а способствовали защите неприкосновенности частной жизни путем законного использования личной информации;

i) возможность предоставления частному сектору рекомендаций относительно устранения предвзятости и ошибочных данных в моделях, используемых для выявления соответствующих случаев, в том числе с помощью механизмов получения обратной связи от людей, а также относительно наиболее эффективного способа передачи данных властям в соответствии с применимым международным правом прав человека;

j) возможность проведения дальнейших исследований и разработки минимальных стандартов, касающихся эффективности финансовых технологий и их влияния на различные группы заинтересованных сторон;

k) возможность документирования передового опыта и извлеченных уроков в области проектирования, разработки, анализа и оценки технологий ПОД/ФТ, отвечающих нормам международного права прав человека и обеспечивающих учет гендерной специфики, при участии частного сектора и гражданского общества.