Аналитический доклад ИДКТК: биометрия и борьба с терроризмом

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

Photo Credit: iStock.com/ktsimage

Перевод с английского языка на русский язык подготовлен при поддержке Научно-исследовательского института проблем безопасности СНГ

СПРАВОЧНАЯ ИНФОРМАЦИЯ

Настоящий Аналитический доклад подготовлен ИДКТК в соответствии с резолюцией 2395 (2017) Совета Безопасности ООН, в которой поручается ИДКТК проводить аналитическую работу по новым проблемам, тенденциям и изменениям и обеспечить доступность результатов его аналитической работы в рамках всей системы ООН.

Целью аналитических докладов является предоставление Контртеррористическому комитету, учреждениям ООН, лицам, отвечающим за принятие политических решений, точного анализа специфических проблем, тенденций и изменений, выявленных в ходе взаимодействия ИДКТК с государствами-членами по вопросу имплементации ими соответствующих резолюций Совета Безопасности. В доклады также включается необходимая информация, собранная ИДКТК, в том числе во общения с его партнерами из ООН, международными, региональными и субрегиональными организациями, организациями гражданского общества (ОГО) и членами Глобальной исследовательской сети ИДКТК (ГИС).

ВВЕДЕНИЕ

Биометрией называется использование физических характеристик человека или личных черт для идентификации или подтверждения заявленной идентичности конкретного лица[1]. К ним могут относиться отпечатки пальцев, лицо, рисунок вен, глаза, радужная оболочка, ДНК, кровь, голос, походка или подпись[2]. Частные организации и государственные органы все чаще используют биометрию для подтверждения или идентификации лиц, чтобы предоставить или ограничить доступ к определенным местам, услугам или устройствам. В государственном секторе биометрия используется в работе правоохранительных ведомств и органов безопасности, уголовного правосудия, миграции и органов социальной защиты (в том числе для предотвращения мошенничества с идентичностью и кражи личности), а также для аутентификации бенефициаров гуманитарной помощи[3].

С момента принятия резолюций 2322 (2016) и 2396 (2017) Совета Безопасности использование биометрии в контртеррористических целях, особенно в контексте управления границами и их охраны, получило широкое распространение. Резолюция 2322 (2016) Совета Безопасности призывает государства-члены обмениваться информацией об иностранных боевиках-террористах (ИБТ) и других отдельных террористах и террористических организациях, включая биометрию и биографическую информацию.

В своей резолюции 2396 (2017) Совет Безопасности решил, что государства должны разработать и имплементировать системы для сбора биометрических данных, которые могут включать в себя отпечатки пальцев, фотографии, распознавание лиц и другие релевантные идентификационные биометрические данные с тем, чтобы ответственным и надлежащим образом идентифицировать террористов, включая ИБТ, в соответствии с национальным законодательством и международными правами человека. Совет Безопасности также призывает государства-члены ответственно обмениваться такой информацией с соответствующими государствами-членами и компетентными международными органами, включая Международную организацию уголовной полиции (Интерпол).

В рамках работы, направленной на продвижение имплементации указанных резолюций государствами-членами, ИДКТК выявил эффективные практики, вопросы, пробелы и вызовы

---

[1] Woodward, J.D., Biometrics: Facing Up to Terrorism (2001).
[2] Biometrics Institute, What are biometrics?
[3] Zureik, E. and Hindle, K. Governance, Security and Technology: The Case Of Biometrics (2004).

в использовании биометрии в контртеррористических целях. В данном Аналитическом докладе будут рассмотрены тенденции в использовании этой технологии в контртеррористических целях, основные вызовы и рекомендации, разработанные с тем, чтобы гарантировать ответственное использование соответствующими заинтересованными сторонами данной технологии. Вопрос использования биометрии в контртеррористической деятельности поднимался в рамках многих оценочных визитов и аналитических обзорах, проводимых ИДКТК от имени Контртеррористического комитета. В представленном ниже анализе содержатся основные изменения, выявленные ИДКТК в ходе общения с государствами-членами и в рамках взаимодействия с ОГО (в частности, с Институтом биометрии на основании Соглашения о сотрудничестве, подписанного обеими сторонами).

ОСНОВНЫЕ ТЕНДЕНЦИИ

Использование биометрии в контртеррористической деятельности

Быстро расширяющийся диапазон связанных с контртеррористической деятельность приложений для биометрических систем включает в себя оборудование для аутентификации и верификации, например, биометрические паспорта («е-паспорта»), биометрические «умные» выходы [на посадку] и считыватели паспортов, а также цифровую криминалистику[4].

Пандемия COVID-19 создала для государств нетривиальную проблему в части использования биометрии для облегчения международных перевозок в связи с широким использованием масок и боязни передачи заболевания контактным способом, что ограничило эффективность применяемых методов идентификации, в том числе распознавание лица и сканнеры отпечатков пальцев. В результате многие государства стали вводить бесконтактные устройства и сканнеры радужной оболочки, которые могут подтвердить идентичность даже при надетой маске[5].

Биометрия стала чаще использоваться в мероприятиях по выявлению преступников, известных террористов и лиц, подозреваемых в совершении террористических преступлений, в том числе в общественных местах, при этом системы распознавания лиц используются совместно с камерами наружного наблюдения. Технологии распознавания также используются совместно с беспилотными летательными системами (БПЛС) в правоохранительной деятельности и охране границ, что позволяет контролировать большие скопления людей и облегчает идентификацию лиц в общественных местах (как это было указано в соответствующем оповещении ИДКТК о тенденциях)[6].

Использование биометрии в борьбе с терроризмом зачастую связывают с разработкой и применением новых технологий. Сюда относятся технологии идентификации объектов заинтересованности, например, камеры высокого разрешения, алгоритмы сопоставления, искусственный интеллект (ИИ), иногда во взаимодействии с подключенными базами данных (например, списков разыскиваемых террористов), использование биометрии (в том числе мультибиометрические системы управления доступом) для защиты мест и объектов критической инфраструктуры, а также «мягких» целей от террористических атак[7].

---

4 United Nations, United Nations Compendium of Recommended Practices for the Responsible Use & Sharing of Biometrics in Counter-Terrorism (2018).

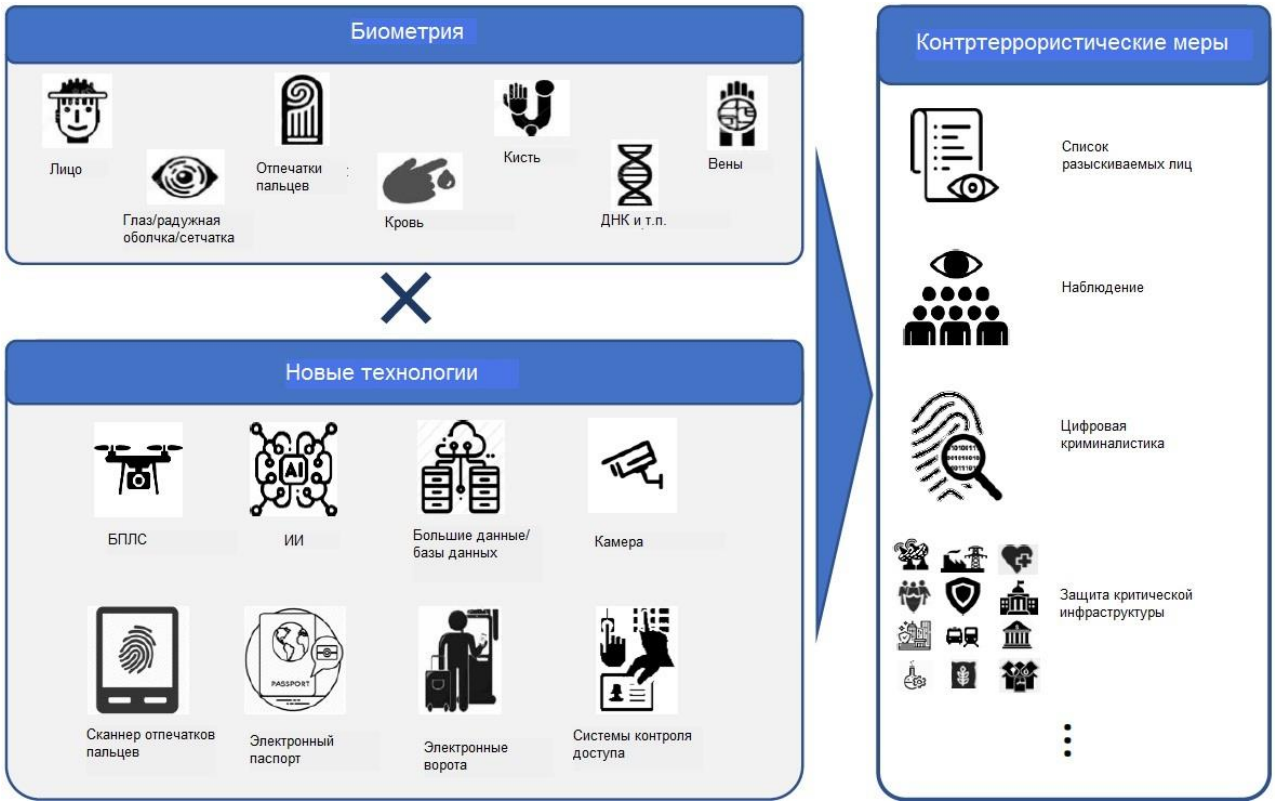
5 CTED, The impact of the COVID-19 pandemic on terrorism, counter-terrorism and countering violent extremism (2020).

6 CTED, CTED Trends Alert: Greater Efforts Needed to Address the Potential Risks Posed by Terrorist Use of Unmanned Aircraft Systems (2019).

7 Chaurasiaa,P., Yogarajaha, P., Condella, J., Prasada, G., McIlhattonb, D., and Monaghanc, R., Countering terrorism, protecting critical national infrastructure and infrastructure assets through the use of novel behavioral biometrics (2016).

Как отмечено в последнем докладе Группы по противодействию легализации преступных доходов и финансированию терроризма (ФАТФ)[8], технологии биометрии также могут оказать значительную помощь в противодействии финансированию терроризма, предлагая расширения для процессов «знай своего клиента» (KYC) и комплексной клиентской проверки (CDD), а также в качестве альтернативных инструментов для мониторинга финансовыми институтами банковских отношений.

Таблица 1: Тенденции в использовании биометрии в борьбе с терроризмом



Использование биометрии государствами-членами

В ходе диалога ИДКТК с государствами-членами, проводимом от имени Комитета, было выяснено, что, хотя масштабы и опыт использования биометрии значительно варьируются, в 118 из 193 государств-членов ООН достигнут, пусть и незначительный, но прогресс в ведении биометрии в контртеррористических целях[9] *(см. таблицу 2).*

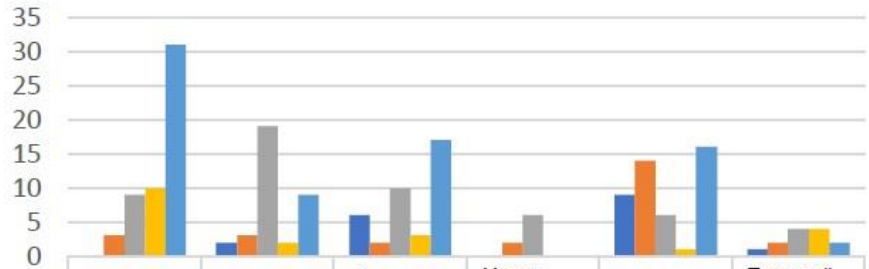
В этой области прослеживаются четкие региональные тенденции. Биометрия широко используется почти в половине европейских государств-членов, но скудно представлена в странах Ближнего Востока. Более половине африканских государств-членов еще только предстоит ввести биометрию.

---

8 http://www.fatf-gafi.org/media/fatf/documents/reports/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf (June 2021). также см. Руководство ФАТФ по цифровому удостоверению личности.

9 От имени Комитета ИДКТК предоставил всем 193 государствам-членам ООН свои обзоры реализации государствами соответствующих резолюций Совета Безопасности (по состоянию на 18 ноября 2021 г.).

Таблица 2: государства, использующие биометрию в борьбе с терроризмом (по состоянию на 30 ноября 2021 г.)



	Африка	Сев. и Юж. Америки	Азия и ТОР	Центр. Азия	Европа	Ближний Восток
Да	0	2	6	0	9	1
В основном	3	3	2	2	14	2
Частично	9	19	10	6	6	4
Незначительно	10	2	3	0	1	4
Нет/нет информации	31	9	17	0	16	2

В ходе взаимодействия ИДКТК с соответствующими заинтересованными сторонами были выявлены следующие тенденции в использовании государствами-членами биометрических технологий в контртеррористических целях:

• Государства расширяют область физического пространства (например, пункты пересечения границы, общественные места и т.д.) и цифрового пространства (например, социальные сети), где используется подтверждение биометрических данных.
• Государства используют новые и все более сложные технологии для сбора, накопления, обработки и анализа биометрических данных.
• Широкий круг сотрудников государственных органов (например, органов безопасности, национальной и местной полиции, пограничной службы, миграционной службы) и некоторые акторы частного сектора (например, подрядчики) уполномочены на доступ к биометрическим данным.
• В некоторых государствах ускорен обмен биометрическими данными в рамках контртеррористического сотрудничества и мер, направленных на обмен информацией.
• Государства наращивают составление список разыскиваемых террористов и баз данных, которые связаны или осуществляют перекрестную проверку по базам биометрических данных, в том числе путем проведения биометрических проверок по уведомлениям и базам данных Интерпола с целью идентификации и выявления преступников и террористов.

ВЫЗОВЫ

По результатам анализа и взаимодействия с соответствующими заинтересованными сторонами ИДКТК выявил спектр вопросов, относящихся к ответственному использованию биометрических технологий в борьбе с терроризмом. К ним относятся:

• Технологические недостатки и ограничения
• Недостаточный потенциал
• Несовершенная правовая и административная база
• Недостаточные меры надзора, обеспечения защиты и безопасности конфиденциальности и данных, а также сроки хранения данных

• Усиление существующей дискриминации и неравенства
• Потенциальное злоупотребление и вызовы для находящихся под защитой свобод религии, выражения и собрания
• Ограниченный обмен биометрическими данными и информацией
• Недостаток эффективных мер правовой защиты в случае нарушений
• Риск мошенничества и злоупотребления биометрическими данными

Несмотря на то, что развитие биометрических технологий значительно продвинулось в части точности и надежности, технологические недостатки по-прежнему могут отрицательно влиять на их эффективность. Внешние факторы, такие как угол обзора камеры, освещение и выражение лица могут влиять на эксплуатационные условия биометрических систем, что потенциально может приводить к ошибочным совпадениям (некорректное сопоставление с образом другого человека) или несовпадению (отсутствию совпадения с правильным образцом)[10]. И хотя в лучших системах, представленных на внутреннем рынке, эти проблемы уже решены, лишь небольшое число государств имеют доступ к таким системам. Разработка базы экспертных пользователей также может помочь минимизировать эти ошибки, но для проведения необходимого обучения требуются значительные ресурсы и опыт.

Тем не менее, результаты диалога ИДКТК с государствами-членами, в том числе в рамках страновых оценочных визитов Комитета, дают основания предположить, что, хотя эти вопросы технологического потенциала (в том числе стоимость приобретения и эксплуатации системы) являются немаловажными, ими можно решать и они уже решаются. На этом фоне более сложными являются проблемы, связанные с разработкой управленческой, институциональной и нормативно-правовой базы.

Такая нормативно-правовая база, которая должна быть разработана до внедрения биометрических систем, является критическим необходимым условием для эффективного и ответственного использования биометрии на национальном уровне[11]. Отсутствие защитных механизмов, которые бы предотвратили злоупотребление или неправомерно использование биометрических технологий и данных (включая нарушения прав человека) также могут отрицательно повлиять на международное сотрудничество и потенциально подорвать контртеррористические усилия на региональном и международном уровнях.

Из анализа ИДКТК следует, что многие государства столкнулись со значительными вызовами в части нарушения прав человека при использовании ими биометрических инструментов и протоколов обмена данными. К этим вызовам относится несовершенные основы защиты конфиденциальности и данных по национальному законодательству и отсутствие четких процедурных механизмов защиты и эффективного надзора за применением биометрической технологии[12] [13]. В отсутствие такой базы биометрические технологии могут представлять угрозу для защиты конфиденциальности и персональных данных, в том числе в связи с их использованием в более широких целях, таких как тотальная слежка, что может привести к стереотипированию и дискриминации, зачастую в отношении маргинализированных групп, включая женщин, меньшинства и просителей убежища.

---

[10] Lukasik, K., The Physiognomy Of Biometrics: The Face Of Counterterrorism (2004).

[11] См. United Nations Compendium of Recommended Practices for the Responsible Use & Sharing of Biometrics in Counter-Terrorism (2018).

[12] Huszti-Orbán, K. and Ní Aoláin, F. Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business? (2020)

[13] В рамках оценочных визитов от имени Контртеррористического комитета ИДКТК рекомендовал некоторым государствам обеспечить ответственную разработку и имплементацию биометрических инструментов и предусмотреть соответствующие механизмы защиты, такие как защита конфиденциальности и данных, в соответствии с резолюцией 2396 (2017).

Все большие опасения вызывает расовая дискриминация при разработке и использовании таких технологий, особенно в сочетании с другими новыми цифровыми технологиями, такими как машинное обучение и алгоритмы, которые, как показывает практика, усиливают существующие неравенства, основанные на расовой, этнической и национальной принадлежности. Специальным докладчиком по продвижению и защите прав человека и фундаментальных свобод в борьбе с терроризмом подчеркивается, что дискриминационное воздействие новых технологий в борьбе с терроризмом может быть как прямым, так и косвенным, и что это особенно актуально в отношении базовых алгоритмических функций таких технологии[14].

ФАТФ на днях отметила, что использование биометрии в целях широкого доступа к финансовым услугам, включая удаленную регистрацию и предоставление финансовых услуг (потребность в которых значительно возросла во время кризиса COVID-19), может усугубить финансовую изоляцию среди определенных групп населения (чаще всего женщин в связи с цифровыми барьерами по гендерному принципу), которые не имеют доступа к электронным устройствам, не доверяют властям или не знакомы с возможностями таких устройств.

В связи с такой обеспокоенностью и широким риском возможного использования биометрии с нарушением прав на защиту конфиденциальности и данных, человеческого достоинства, самоопределения и доступа к эффективным средствам защиты, ОГО озвучивался ряд проблем и делался призыв к мораторию на развитие и внедрение всех биометрических технологий до тех пор, пока не будут предусмотрены механизмы защиты всех жизненно важных прав человека[15].

Возможно, что в связи с имеющимися вызовами в части ответственного использования биометрии, обмен биометрической информацией в рамках борьбы с терроризмом по-прежнему носит несогласованный характер, хотя резолюция 2396 (2017) рекомендует государствам обмениваться такой информацией, сообразно обстоятельствам, друг с другом; с Интерполом; и с другими соответствующими международными органами. В ходе взаимодействия ИДКТК со странами-членами было выявлено, что обмен биометрическими данными и информацией об ИБТ имеет тенденцию носить ограниченных характер, даже между государствами-членами с достаточным потенциалом. Также было выявлено, что обмен такой и доступ к базам данных соответствующих национальных органов в ряде государств ограничен.

Более того, серьезную озабоченность вызывает риск кражи или взлома биометрических данных, особенно через кибератаки. Несмотря на то, что использование биометрии значительно затрудняет подделку личных данных, считывание (или незаконный захват) данных и потребность хранения биометрических образцов в удаленных базах данных представляют риск угроз или взлома, что делает биометрические данные потенциально уязвимыми для неправомерного или злоумышленного использования. Более того, биометрическая информация (например, голос, лицо и отпечатки пальцев) могут легко собираться и легко доступны (в отличие от паролей или PIN-кодов). С развитием искусственного интеллекта (ИИ) технологии «глубоких фейков» (гипер-реалистичные видеосюжеты, в которых представляется какой-то человек, который говорит или делает то, что он на самом деле никогда не говорил или не делал) с большой долей вероятности будут доступны для организованной преступности и контрабандистов[16].

---

[14] См. заявление от 25 июня 2021 г.

[15] См., например, веб-страницу Статьи 19.

[16] Westerlund, M., The Emergence of Deepfake Technology: A Review (2019).

Эти многосторонние вызовы демонстрируют потребность в скоординированном предоставлении технической помощи и содействия в повышении потенциала для государств-членов (особенно, государствам Африки, Центральной и Юго-Восточной Азии, а также Южной Америки), которые столкнулись с проблемой внедрения и использования биометрии, а также потребность в государствах с опытом ответственного использования биометрии для поддержки таких инициатив[17]. Частный сектор также играет важную роль в ответственной и согласующейся с правами человека разработке биометрических систем, включая мероприятия по кибербезопасности для защиты собранных данных. Было создано уже много соответствующих государственно-частных партнерств, и эти инициативы должны поддерживаться и продвигаться на национальном, региональном и международном уровнях при этом должна осознаваться важность гарантирования того, что в рамках таких партнерств будут уважаться права человека и реализовываться подход, учитывающий гендерную проблематику.

МЕЖДУНАРОДНЫЕ РУКОВОДСТВА И ИНЦИАТИВЫ

• В принятой резолюции 2322 (2016) было впервые отмечено, что Совет Безопасности призывает государства-члены обмениваться биометрическими данными для выявления и идентификации террористов, включая ИБТ. Резолюция 2396 (2017) Совета превратила этот призыв в обязательное требование в соответствии главой VII Устава ООН.

• В Дополнении к руководящим принципам в отношении иностранных боевиков-террористов (2018) (S/2018/1177) даются дополнительные руководства государствам по эффективным мерам реагирования и имплементации, с особым акцентом на новых требованиях, введенных резолюцией 2396 (2017). Руководство может применяться или использоваться в качестве отсылочной нормы государствами в рамках их усилий на национальном уровне. Руководящий принцип № 38 раскрывается на тех элементах, которые относятся к «ответственному» использованию и обмену биометрией.

• В декабре 2019 года Совет выпустил Техническое руководство Контртеррористического комитета по имплементации резолюции 1373 (2001) Совета Безопасности и других резолюций (S/2019/998), которые также касаются использования биометрии в рамках соответствующих резолюций Совета по борьбе с терроризмом.

• В июне 2021 года по итогам Седьмого обзора Глобальной контртеррористической стратегии ООН (A/RES/60/288) Генеральная Ассамблея ООН вновь подтвердила Стратегию, приняв резолюцию A/RES/75/291. В соответствии со Стратегией, все государства-члены призываются обратить внимание на угрозу роста потока международных рекрутов в ряды террористических организаций, в том числе через выполнение обязательств по использованию биометрических данных при полном уважении прав человека и фундаментальных свобод.

• ИДКТК и Контртеррористическое управление ООН (КТУ ООН) во взаимодействии с Институтом биометрии и в рамках Глобального договора по координации контртеррористической деятельности подготовили «Сборник рекомендованных практик Организации Объединенных Наций по ответственному использованию и обмену биометрией в борьбе с терроризмом», который был издан в июне 2018 г. Сборник был разработан в целях содействия усилиям по укреплению реализации биометрических систем и продвижения

[17] В рамках оценочных визитов, проведенных от имени Контртеррористического комитета, ИДКТК рекомендовал, чтобы государства, обладающие соответствующим потенциалом и возможностями, предоставляли техническое содействие и поддержку по повышению потенциала для государств, которые в этом нуждаются.

ответственного и надлежащего использования и обмена биометрией, как этого требует резолюция 2396 (2017).

• В июне 2020 года Специальный докладчик по продвижению и защите прав человека и фундаментальных свобод в борьбе с терроризмом издал отчет «Использование биометрических данных для идентификации террористов: передовая практика или рискованный бизнес?»

• Интерпол разработал проект First, который предназначен для содействия государствам в обмене биометрическими данными ИБТ и других лиц, подозреваемых в терроризме, продвижения перехода культуры «необходимо знать» к культуре «необходимо делиться» и нацелен на совершенствование идентификации и выявления террористов и их пособников за счет использования последних технологий обработки цифровых изображений и распознавания лиц. Он также разработал проект Hotspot, целью которого является увеличение количества данных, которые государства вносят в базы данных. Связанные с пограничным контролем.

• Международная организация гражданской авиации (ИКАО) разработала Директория открытых ключей ИКАО (ДОК) - центральный репозитарий для обмена информацией, необходимой для аутентификации биометрических паспортов, который предоставляет эффективный инструмент для государств для загрузки своей информации и выгрузки информации других государств. Действуя в качестве централизованного посредника, ДОК гарантирует, чтобы информация соответствовала техническим стандартам, необходимым для достижения и поддержания взаимодействия.

• ФАТФ разработала подробное Руководство по цифровому удостоверению личности[18], чтобы помочь правительствам, финансовым институтам, провайдерам услуг в сфере виртуальных активов и другие регулируемым органам определять, соответствует ли цифровое удостоверение личности целям комплексной клиентской проверки. В изданном в июне 2021 года Докладе о возможностях и вызовах новых технологий для ПОД /ПФТ ФАТФ также отмечает, что смешанные подходы (когда официальные удостоверения личности предоставляются совместно с биометрической идентификацией) позволяю осуществить более тщательные процессы идентификации и подтверждения. В отчет подчеркивается, что биометрическая информация, собранная частными компаниями, должна признаваться защищаемой информацией и отвечать правовым стандартам, предъявляемым к такой информации в соответствии с международными правовыми документами, а ее использование должно быть ограничено принципами пропорциональности и необходимости.

• В партнерстве с Контртеррористическим центром ООН (КТЦ ООН) Глобальный контртеррористический форум (ГКФ) разработал «Передовые практики в области пограничной безопасности и управления в контексте борьбы с терроризмом и пресечения потока “иностранных боевиков-террористов”, которые были одобрены на Седьмом министерском пленарном заседании ГКФ, проведенном в сентябре 2016 года. Передовые практики подготовлена в целях информации и руководства правительств при выработке политики, программ и подходов для эффективного управления безопасностью границами, трансграничного сотрудничества и охраны границ в рамках борьбы с терроризмом.

• В 2020 году Контртеррористический центр ООН (КТЦ ООН) разработал Справочник по детям, затронутым феноменом иностранных боевиков-террористов: реализация подхода, основанного на обеспечении прав детей.

[18] https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-on-Digital-Identity.pdf.

• КТЦ ООН и ИДКТК также организовали серию региональных экспертных семинаров в целях повышения осведомленности и компетентности государств-членов в обеспечении ответственного использования и обмена биометрическими данными для выявления, пресечения, расследования и уголовного преследования по террористическим преступлениям и другим тяжким преступлениям на границе.

ИДКТК продолжит работать по различным инициативам, нарабатывать и делиться своим опытом в вопросах ответственного использования биометрических технологий во взаимодействии с государствами-членами; другими учреждениями ООН; международными, региональными и субрегиональными организациями; местными властями; ОГО; частным сектором; и научным сообществом (через ГИС).