GCTF
GLOBAL COUNTERTERRORISM FORUM

ИНСТРУМЕНТАРИЙ ДЛЯ ПРАКТИЧЕСКОЙ РЕАЛИЗАЦИИ

Цюрихско-Лондонских рекомендаций Глобального контртеррористического форума по предупреждению насильственного экстремизма и терроризма в сети Интернет и борьбе с ними

ИНСТРУМЕНТАРИЙ ДЛЯ ПРАКТИЧЕСКОЙ РЕАЛИЗАЦИИ

Цюрихско-Лондонских рекомендаций Глобального контртеррористического форума по предупреждению насильственного экстремизма и терроризма в сети Интернет и борьбе с ними

Содержание

Общие сведения

С момента своего возникновения Интернет предоставляет бесчисленные возможности для общества обеспечивая доступ к информации и способствуя упрощению коммуникаций, экономическому развитию, а также участию в жизни общества. Свободная, открытая, безопасная, стабильная, доступная и мирная цифровая среда необходима всем и требует эффективного взаимодействия между государствами в целях снижения рисков в области международного мира и безопасности[1]. Однако группировки насильственных экстремистов и террористов, и отдельные их представители, все чаще используют Интернет (в особенности платформы социальных сетей) для распространения пропаганды, рассылки способствующих этому материалов, привлечения денежных средств, запугивания, обучения, радикализации, вербовки и подстрекательства других лиц к совершению актов насильственного экстремизма и терроризма.

Генеральная Ассамблея (ГА) Организации Объединенных Наций (ООН) отметила важность сотрудничества между заинтересованными сторонами в области реализации Глобальной контртеррористической стратегии ООН, в том числе между государствами, международными, региональными и субрегиональными организациями, представителями частного сектора и гражданского общества, для решения проблем, связанных с возрастающей степенью использования информационно-коммуникационных технологий (ИКТ) террористами и их сторонниками, при соблюдении прав человека, основных свобод, и в соответствии с международным правом, а также с целями и принципами Устава ООН[2].

ГА ООН подчеркнула, что определяющее значение имеет разработка наиболее эффективных средств для борьбы с пропагандой терроризма, побуждением к совершению террористических актов и вербовкой в террористические группы, в том числе посредством сети Интернет, в соответствии с международным правом, включая международное право в области прав человека. Кроме того, ГА ООН рекомендовала государствам рассмотреть возможность реализации соответствующих рекомендаций, представленных в Докладе Генерального секретаря ООН «*План действий по предупреждению насильственного экстремизма*», с учетом национального контекста. В указанном докладе стратегические коммуникации, Интернет и социальные сети определены в качестве основных направлений действий в целях предупреждения насильственного экстремизма и терроризма и борьбы с ними[3].

На Седьмом пленарном заседании министров Глобального контртеррористического форума (ГКТФ), проходившем в Нью-Йорке 21 сентября 2016 г., члены ГКТФ одобрили начало процесса анализа и оценки существующих примеров реализуемой государствами передовой практики и опыта в области предупреждения насильственного экстремизма и терроризма в сети Интернет и борьбы с ними в рамках *Инициативы ГКТФ по решению проблемы жизненного цикла от радикализации к насилию.* Результатом этого стало официальное принятие *Цюрихско-Лондонских рекомендаций ГКТФ по предупреждению насильственного экстремизма и*

[1] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174), para 2, 22 July 2015 [Доклад Группы правительственных экспертов по достижениям в области информатизации и телекоммуникаций в контексте международной безопасности] (A/70/174), пункт 2, 22 июля 2015 г.]

[2] UN Global Counter-Terrorism Strategy Review (A/RES/70/291), para 42, 19 July 2016 [Обзор Глобальной контртеррористической стратегии ООН (A/RES/70/291), пункт 42, 19 июля 2016 г.]

[3] UN Global Counter-Terrorism Strategy Review, paras. 42f. and 40 [Обзор Глобальной контртеррористической стратегии ООН, пункты 42f и 40]; UN Secretary-General's Plan of Action to Prevent Violent Extremism (A/70/674), para. 55, 24 December 2015 [Доклад Генерального секретаря ООН «План действий по предупреждению насильственного экстремизма» (A/70/674), пункт 55, 24 декабря 2015 г.]

терроризма в сети Интернет и борьбе с ними («Цюрихско-Лондонские рекомендации») в сентябре 2017 года.

Данная Инициатива была основана на убеждении, что государствам следует принять собственные меры и поддержать соответствующие меры, предпринимаемые представителями отрасли ИКТ и гражданского общества, для предупреждения неправомерного использования цифрового пространства (в особенности Интернета и площадок социальных сетей) в целях насильственного экстремизма и терроризма и борьбы с таким неправомерным использованием. Не имеющие обязательной юридической силы Цюрихско-Лондонские рекомендации представляют собой неисчерпывающий список примеров передовой практики для государств в отношении того, каким образом аспекты стратегических коммуникаций и социальных сетей могут использоваться для предупреждения насильственного экстремизма и терроризма в Интернете и борьбы с ними. при соблюдении прав человека, основных свобод и принципа верховенства закона.

В 2018 году члены ГКТФ поддержали инициативу Австралии, Швейцарии и Великобритании, которая направлена на разработку пособия (Инструментария) для лиц, ответственных за разработку политики, и государственным экспертам, по практической реализации Цюрихско-Лондонских рекомендаций, содержащее передовые практики, реализуемые государствами различных стран, с указанием практических примеров, а также с ссылками на существующие международные и региональные инициативы и практики в области предупреждения насильственного экстремизма и терроризма в сети Интернет и борьбы с ними.

Разработка настоящего Инструментария преследует следующие цели:

- предоставить государственным экспертам и лицам, ответственным за разработку политики, доступ о предпринимаемых мерах и современных тенденциях в области предупреждения насильственного экстремизма и терроризма в сети Интернет и борьбы с ними;
- способствовать тому, чтобы меры, предпринимаемые государствами, обеспечивали соблюдение прав человека и основных свобод, таких как право на неприкосновенность частной жизни и свободу выражения мнения, объединений, мирных собраний, вероисповедания и убеждений, а также необходимость сохранения свободного потока информации и свободного и открытого Интернета;
- содействовать налаживанию эффективного и устойчивого сотрудничества между государственными учреждениями, ИКТ компаниями и гражданским обществом на основе принципа общей ответственности в области предупреждения насильственного экстремизма и терроризма в сети Интернет и борьбы с ними;
- стимулировать развитие инноваций посредством использования примеров передовой практики и полученного опыта, которые могут выходить за пределы предупреждения насильственного экстремизма и терроризма в сети Интернет и борьбы с ними, но при этом являются актуальными.

ЦЕЛЕВАЯ АУДИТОРИЯ

Целевой аудиторией настоящего Инструментария являются члены ГКТФ, а также основные партнеры ГКТФ и государственные учреждения других стран, заинтересованные в предупреждении насильственного экстремизма и терроризма в сети Интернет и борьбе с ними.

Подтверждая совместную ответственность государств, ИКТ компаний и гражданского общества за предупреждение насильственного экстремизма и терроризма в сети Интернет и борьбу с ними, настоящий Инструментарий также предназначен для экспертов, работающих по указанным проблематикам.

МЕТОДОЛОГИЯ

Целью настоящего Инструментария является предоставление удобного в использовании практического руководства для лиц, ответственных за разработку политики, и экспертов в области предупреждения насильственного экстремизма и терроризма в сети Интернет и борьбы с ними. Важно отметить, что настоящий

Инструментарий по своему характеру не является исчерпывающим, а представляет собой сборник передовых практик и практических примеров.

В основе настоящего Инструментария лежат примеры передовой практики, определенные Цюрихско-Лондонскими рекомендациями. Представленные в них практические примеры и примеры практики, применяемые заинтересованными сторонами, не выделяют какого-либо особого подхода к предупреждению насильственного экстремизма и терроризма в сети Интернет и борьбе с ними.

Они были выбраны, по причине уместности, а также в связи с тем, что они указывают на те факторы, которые необходимо учитывать для успешной практической реализации тех или иных мероприятий.

Цюрихско-Лондонскими рекомендациями меры реагирования на проявления насильственного экстремизма и терроризма в сети Интернет подразделяются на две основные категории:

1. **Меры реагирования по контенту**: усилия государства направленные на противодействие наличию и доступности террористической и сопряженной с насилием экстремистской пропаганды посредством международного сотрудничества с привлечением частных (ИКТ) компаний для совместной борьбы с терроризмом и насильственным экстремизмом в Интернете, включая фиксирование наличия подозрительного контента, удаление, фильтрацию и принятия соответствующих процедур/законодательных норм (которые разработаны в соответствии с обязательствами стран в сфере прав человека).
2. **Меры реагирования, основанные на коммуникациях**: усилия государства направленные на оказание поддержки или помощи в противодействии привлекательности сопряженной с насилием экстремистской и террористической пропаганды посредством стратегических коммуникаций (доведение информации), включая поддержку организаций гражданского общества для представления контраргументов и альтернативных нарративов как в Интернете, так и в реальной жизни.

Если эти две категории будут четко закреплены в стратегии, определяющей подход, основанный на вовлечении всех государственных учреждений и всего общества к вопросам предупреждения насильственного экстремизма и терроризма в сети Интернет и борьбе с ними, их использование может способствовать формированию более целостного подхода к предупреждению насильственного экстремизма и терроризма в сети Интернет и борьбе с ними в целом.

Таким образом, реализуемая государством стратегия по предупреждению насильственного экстремизма и терроризма в сети Интернет и борьбе с ними должна устанавливать ясные и измеримые цели, а также должна быть основана на принципе ясной «теории изменений», которая четко определяет, каким образом и почему меры реагирования, основанные как на мерах реагирования по контенту, так и на мерах реагирования по коммуникации, будут способствовать достижению целей, определенных в самой стратегии.

Меры реагирования по контенту:

1. Разработка и принятие связанных с контентом законодательства и политики

Настоящий раздел нацелен на оказание поддержки лицам, занимающимся разработкой законодательных актов, и ответственным за разработку политики, а также практикующим специалистам в разработке и принятии связанных с контентом законодательства и политики в целях эффективного предупреждения насильственного экстремизма и терроризма в сети Интернет и борьбы с ними. В частности, в настоящем разделе рассказывается о том, каким образом государства могут принять соответствующие правовые нормы в области предупреждения неправомерного использования сети Интернет в целях насильственного экстремизма и терроризма и борьбы с этими угрозами, находясь при этом в международном правовом поле в сфере обеспечения прав человека, включая, помимо прочего, свободу выражения мнений и право на неприкосновенность частной жизни. Данный раздел состоит из двух подразделов: «Принципы и рекомендации» и «Разработка системы мер».

Соответствующие примеры передовой практики из Цюрихско-Лондонских рекомендаций

Передовая практика 1. *Принятие и внедрение законодательных мер и соответствующей системы мер на национальном уровне для предотвращения и противодействия насильственному экстремизму и терроризму в Интернете.*

Передовая практика 7. *Принятие законов, положений и программ, направленных на противодействие наличию и доступности террористического и сопряженного с насилием контента в Интернете.*

Передовая практика 8. *Принятие во внимание соответствующих применимых и действующих международных стандартов и (или) принципов для решения проблем, связанных с наличием и доступностью террористического и сопряженного с насилием контента в Интернете и на платформах социальных сетей.*

ВВЕДЕНИЕ

Государства несут основную ответственность за предупреждение насильственного экстремизма и терроризма и борьбу с ними в рамках подхода, основанного на участии всего общества. В настоящее время только в некоторых государствах приняты правовые нормы, вводящие уголовную ответственность за подстрекательство к насилию; значительно большее число стран применяют правовые нормы, касающиеся совершения террористического акта, прославления терроризма и «оправдания терроризма». Принятие или обновление законодательства в соответствии с международным правом в области прав человека в целях формирования законодательной базы для решения проблем, связанных с наличием и доступностью контента с пропагандой насильственного экстремизма и терроризма в Интернете, имеет определяющее значение для обеспечения того, чтобы все соответствующие участники имели четкие обязательства и действенные рекомендации в области предупреждения насильственного экстремизма и терроризма в сети Интернет и борьбы с ними.

Государства обязаны обеспечить, чтобы частный сектор в процессе своей работы не допускал нарушений соответствующих национальных или международных законов. Разработка и внедрение эффективной национальной законодательной базы, будь то посредством введения нового законодательства, связанного с контентом, или посредством обновления существующих законов с добавлением элементов, связанных с контентом, представляет собой критическую исходную точку для всех государств в целях обеспечения того, чтобы проблема с незаконным контентом была решена, а также чтобы ИКТ компании также должным образом участвовали в предупреждении насильственного экстремизма и терроризма в сети Интернет и борьбе с ними.[4]

A. Принципы и рекомендации

Международные документы: принципы и рекомендации

Существует ряд международных документов, в которых излагаются соответствующие стандарты и принципы, которые государствам следует учитывать при разработке законодательства в области предупреждения насильственного экстремизма и борьбы с ним. Необходимость соблюдения международных обязательств неизменно подчеркивается в международных документах. Например, в Глобальной контртеррористической стратегии ООН отмечается, что государства и другие соответствующие участники должны принять меры в связи с возрастающей степенью использования ИКТ террористами и их сторонниками, при соблюдении прав человека, основных свобод и в соответствии с международным правом, а также с целями и принципами Устава ООН.[5]

Кроме того, неизменно подчеркивается необходимость соблюдения международного права в области прав человека и, в частности, права на свободу выражения мнения, а также права на неприкосновенность частной жизни (как это более подробно описано далее по тексту). В *Совместной декларации о свободе выражения мнения и противодействии насильственному экстремизму*[6] от 2016 года Специальный докладчик ООН по

[4] Для целей настоящего инструмента, термин «законодательство» используется для обозначения любого закона, иного нормативного правового акта, правила, текста или иного документа, имеющего силу закона или обязательный характер внутри соответствующей страны

[5] UN Global Counter-Terrorism Strategy Review, 2016 [Обзор Глобальной контртеррористической стратегии ООН, 2016 г.]

[6] *Joint Declaration on Freedom of Expression and Countering Violent Extremism* adopted by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media, the OAS Special Rapporteur on Freedom of Expression and the ACHPR Special Rapporteur on Freedom of Expression and Access to Information, 03 May 2016 *[Совместная декларация о свободе выражения мнения и противодействии насильственному экстремизму*, Специальный докладчик Организации Объединенных Наций (ООН) по вопросу о праве на свободу мнений и их свободное выражение, Представитель Организации по безопасности и сотрудничеству в Европе (ОБСЕ) по вопросам свободы средств массовой информации, Специальный докладчик Организации американских государств (ОАГ) по вопросам свободы выражения мнения и Специальный докладчик Африканской комиссии по правам человека и народов (АКПЧН) по вопросам свободы выражения мнения и доступа к информации, 03 мая 2016 г.] См. также: *Joint Declaration on Challenges to the Freedom of Expression in the Next Decade* 10 July 2019 *[Совместная декларация о вызовах свободе выражения мнения в следующем десятилетии*,

вопросу о праве на свободу мнений и их свободное выражение, а также его коллеги из Организации по безопасности и сотрудничеству в Европе (ОБСЕ), Организации американских государств (ОАГ) и Африканской комиссии по правам человека и народов (АКПЧН), рекомендовали следующее:

> *2. Конкретные рекомендации (...)*
>
> *(a) Государствам не следует выносить в отношении интернет-компаний – посредников обязательные к исполнению предписания об удалении или ином ограничении контента, за исключением случаев, когда контент ограничивается на законных основаниях в соответствии с изложенными выше правилами. Государствам следует воздерживаться от оказания давления, наказания или вознаграждения компаний-посредников в целях ограничения законного контента (...)*
>
> *(j) Государствам следует воздержаться от принятия или пересмотреть действующее законодательство и политические доктрины, предполагающие следующее:*
>
> *(i) Огульные запреты на шифрование и анонимность, которые не продиктованы необходимостью и по сути дела непропорциональны, а потому юридически неправомерны в качестве ограничений на свободу выражения мнения, в том числе в контексте принимаемых государствами мер реагирования на терроризм и другие виды насилия.*
>
> *(ii) Меры, ослабляющие имеющиеся инструменты обеспечения цифровой защищенности, такие, как использование обходных паролей и депонирование ключей, поскольку они могут несоразмерно ограничивать свободу выражения мнения и неприкосновенность частной жизни и делать сети связи более уязвимыми к кибератакам.*

Кроме того, Руководящие принципы ООН предпринимательской деятельности в аспекте прав человека от 2011 года, обеспечивающие практическую реализацию Рамок ООН в отношении «защиты, соблюдения и средств правовой защиты» от 2008 года, предоставляют дополнительные указания в части обязанностей государств и обязательств компаний по повышению стандартов и улучшению практики их предпринимательской деятельности в аспекте прав человека.[7] Первым основополагающим принципом Рамок является обязанность государства обеспечивать защиту от нарушений прав человека со стороны третьих лиц, в том числе в рамках предпринимательской деятельности, на своей территории или в пределах своей юрисдикции посредством принятия надлежащего законодательства или системы мер. Государства играют основную роль в предотвращении и устранении нарушений прав человека в корпоративном контексте.

Вторым основополагающим принципом является корпоративная обязанность соблюдать права человека: своими действиями третьи лица не должны нарушать права других, а также должны устранять отрицательное влияние на права человека. Хотя соблюдение прав человека не является обязательством, непосредственно налагаемым международным правом в области прав человека на третьих лиц, сегодня это распространенный ключевой элемент практически всех имеющихся документов, носящих добровольный или рекомендательный характер, которые касаются корпоративной ответственности и одобрены Советом по правам человека. Кроме того, обязанность бизнес-сообщества в части соблюдения прав может быть уже закреплена в национальном законодательстве. В ежегодном докладе Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение от 6 апреля 2018 г., который посвящен регулированию интернет-контента созданного пользователями[8], затрагиваются вопросы как государственных, так и корпоративных обязательств.

---

10 июля 2019 г.]

[7] *UN Guiding Principles on Business and Human Rights*, 2011 [*Руководящие принципы предпринимательской деятельности в аспекте прав человека ООН*, 2011 г.]

[8] *Annual Report of the Special Rapporteur to the Human Rights Council on online content regulation (A/HRC/38/35), 06 April 2018 [Ежегодный доклад Специального докладчика Совету по правам человека по вопросам регулирования интернет-контента (A/HRC/38/35), 06 апреля 2018 г.]*

Наконец, третий основополагающий принцип— действенные механизмы подачи и рассмотрения жалоб — играет важную роль как с точки зрения обязанности государства по защите, так и корпоративного обязательства по соблюдению. В рамках своих обязательств, государства должны принять надлежащие меры на своей территории и (или) в пределах своей юрисдикции, которые, при возникновении такого рода нарушений прав человека со стороны бизнес-сообщества, дают возможность тем, чьи интересы были затронуты, иметь доступ к эффективным средствам правовой защиты посредством судебных, административных, законодательных или иных соответствующих механизмов.

Свобода выражения мнения

Государствам следует обеспечить, чтобы любой закон в области решения проблем, связанных с наличием и доступностью контента с пропагандой насильственного экстремизма и терроризма в сети Интернет, соответствовал международным стандартам и принципам, в частности, с точки зрения свободы выражения мнения. Право на свободу выражения мнения является фундаментальным принципом международного права в области прав человека, а также неотъемлемой частью осуществления прочих прав человека, таких как право на свободу мирных собраний и объединений. Это всеобщее право закреплено в статье 19 Всеобщей декларации прав человека (ВДПЧ), в которой указано следующее: «Каждый человек имеет право на свободу убеждений и на свободное выражение их; это право включает свободу беспрепятственно придерживаться своих убеждений и свободу искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ».

Гарантии свободы выражения мнения также охватываются статьей 19 Международного пакта о гражданских и политических правах (МПГПР)[9]. Кроме того, свобода выражения мнения является элементом ряда документов регионального права в области прав человека, таких как Европейская конвенция о правах человека (ЕКПЧ), Американская конвенция о правах человека (АКПЧ) и Африканская хартия прав человека и народов (АХПЧН).

Ограничения на свободу выражения мнения

Пункт 3 статьи 19 МПГПП предусматривает два специфических случая, когда допускаются ограничения на свободу выражения мнения: для обеспечения уважения прав и репутации других лиц, а также в целях государственной безопасности, общественного порядка (*ordre public*), здоровья или нравственности населения. Важно подчеркнуть, что пункт 3 статьи 19, касающийся ограничений, надлежит истолковывать ограничительно. В *Сиракузских принципах толкования ограничений и отступлений от положений Международного пакта о гражданских и политических правах*, представлены полезные разъяснения относительно условий, изложенных в пункте 3 статьи 19, в части ограничения свободы выражения мнения: в контексте предупреждения насильственного экстремизма и терроризма в сети Интернет и борьбы с ними, охрана государственной безопасности и (или) общественного порядка являются наиболее значимыми причинами для ограничения свободы выражения мнения. Согласно Сиракузским принципам, отступления от прав и ограничения прав со ссылкой на интересы национальной безопасности допускаются «для оправдания мер по ограничению некоторых прав только в том случае, когда такие меры принимаются для защиты существования государства, его территориальной целостности или политической независимости от применения силы или угрозы ее применения».[10] Обоснования со ссылкой на интересы национальной безопасности «не могут

[9] Пункт 2 статьи 19 МПГПП предусматривает самые полные гарантии свободы выражения мнения, а также свободы искать, получать и распространять всякого рода информацию и идеи. Принцип свободы выражения мнения предусматривает любые формы выражения, в том числе устную, письменную, посредством печати или художественных форм выражения, таких как изображения, и любые средства их распространения, включая книги, газеты, брошюры, плакаты, баннеры, аудиовизуальные материалы, а также электронные и интернет-средства выражения. Обратите внимание, что не все государства-члены ГКТФ подписали или ратифицировали МПГПП.

[10] UN Commission on Human Rights, *The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights* (E/CN.4/1985/4), para 29, 28 September 1984 [Комиссия ООН по правам человека, *Сиракузские принципы толкования ограничений и отступлений от положений Международного пакта о гражданских и политических правах* (E/CN.4/1985/4), п. 29, 28 сентября 1984 г.]

использоваться в качестве предлога для введения неопределенных или произвольных ограничений, и на них можно ссылаться лишь при наличии адекватных гарантий и эффективных средств правовой защиты от нарушений».[11] Оправдание ограничения прав человека защитой общественного порядка принимается лишь в том случае, когда поставлена цель сохранить «совокупность норм, обеспечивающих жизнедеятельность общества или ряд основополагающих принципов, на которых построено общество».[12] В этом отношении Сиракузские принципы подчеркивают, что «уважение к правам человека является частью общественного порядка (*ordre public*)».[13]

Замечание общего порядка № 34 Комитета по правам человека ООН устанавливает, что такие правонарушения как «поощрение терроризма» и «экстремистская деятельность», а также правонарушения «восхваления», «прославления» или «оправдания» терроризма должны иметь четкие определения для гарантии того, что их применение не ведет к «неуместному или несоразмерному вмешательству» в осуществление права на свободное выражение мнений.[14]

Специальный докладчик ООН по вопросу о праве на свободу мнений и их свободное выражение рекомендует применять ограничения исключительно на индивидуальной основе и в соответствии с требованиями законности, необходимости, соразмерности и правомерности.[15]

- **Законность.** Любое ограничение должно быть предусмотрено законом. Такие законы должны быть приняты в рамках стандартных правовых процедур и сформулированы с достаточной степенью точности. Кроме того, такие законы должны быть доступны широкой общественности и должны предусматривать достаточные указания для лиц, ответственных за исполнение таких законов. Любое конкретное ограничение права должно соответствовать положениям о надлежащих правовых процедурах, установленным национальным законодательством, а надзор за ним должны осуществлять независимые контрольные органы, в частности — суды.
- **Необходимость и соразмерность** Любые ограничения должны являться необходимыми и предусматривающими наименьшее вмешательство для достижения законной цели. Согласно Докладу Специального докладчика по вопросу о праве на свободу мнений и их свободное выражение, платформы социальных сетей должны «приводить данные и примеры, позволяющие понять факторы, анализируемые при установлении нарушения, степень его тяжести и принятые в ответ на него меры».[16] Кроме того, в контексте ненавистнических высказываний, «разъяснение методов урегулирования конкретных дел может помочь пользователям лучше понять подход компаний к случаям, в которых сложно провести различие между оскорбительным контентом и разжиганием ненависти, или методику анализа в онлайн-контексте таких соображений, как намерение выступающего с заявлением лица или вероятность насилия».[17]
- **Правомерность.** Любые ограничения должны подпадать под одну из двух категорий особых ограничений, предусмотренных пунктом 3 статьи 19 МПГПП: для уважения прав и репутации других лиц, а также для охраны государственной безопасности, общественного порядка (*ordre public*),

---

[11] Там же, п. 31.

[12] Там же, п. 22.

[13] Там же

[14] UN Human Rights Committee, *General comment no. 34, Article 19, Freedoms of opinion and expression* (CCPR/C/GC/34), para 46, 12 September 2011 *[Комитет по правам человека ООН, Замечание общего порядка № 34, статья 19 «Свобода мнений и их выражения»,* CCPR/C/GC/34), п. 46, 12 сентября 2011 г.]

[15] UN Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* (A/HRC/29/32), para 57, 22 May 2015 [Совет по правам человека ООН, *Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение* (A/HRC/29/32), п. 57, 22 мая 2015 г.]

[16] UN Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* (A/HRC/38/35), para 47, 6 April 2018 [Совет по правам человека ООН, *Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение* (A/HRC/38/35), п. 47, 6 апреля 2018 г.]

[17] Там же, п. 47.

здоровья или нравственности населения. Ограничения, установленные пунктом 3 статьи 19, следует истолковывать ограничительно. Например, умаление и ограничение права на свободу выражения мнения со ссылкой на интересы национальной безопасности допускается только для защиты существования государства, его территориальной целостности или политической независимости от применения силы или угрозы ее применения».[18] Обоснования со ссылкой на интересы национальной безопасности не следует использовать «в качестве предлога для введения неопределенных или произвольных ограничений».[19] Обоснование со ссылкой на защиту общественного порядка может использоваться лишь в том случае, когда необходимо сохранить жизнедеятельность общества или его основополагающие принципы.[20]

Право на неприкосновенность частной жизни

Право на неприкосновенность частной жизни необходимо защищать в процессе мониторинга интернет-контента в поисках лиц, симпатизирующих террористам и насильственным экстремистам, вербовщиков и террористических заговоров. Мониторинг интернет-контента, например, посредством наблюдения, перехвата, сбора и хранения данных, является дополнительным средством борьбы с насильственный экстремизмом и терроризмом в Интернете.

Статья 17 МПГПП устанавливает, что, хотя неприкосновенность частной жизни и не является абсолютным правом, ее необходимо защищать от незаконного или произвольного вмешательства. В частности, незаконное вмешательство происходит в том случае, когда такое вмешательство находится за предусмотренными законом пределами. Произвольного вмешательства также следует избегать; поэтому, даже если закон предусматривает основания для вмешательства, оно должно быть обоснованным, необходимым и соразмерным в конкретных обстоятельствах. Любое хранение информации какого-либо лица, будь то государственными органами или частными лицами, должно регулироваться законом. В своем Замечании общего порядка № 16 Комитет по правам человека ООН рекомендует государствам обеспечить, чтобы «информация, касающаяся личной жизни какого либо лица, не попадала в руки лиц, которые не имеют разрешения на ее получение, обработку и использование, и к тому, чтобы такая информация никогда не использовалась в целях, не совместимых с целями Пакта».[21]

Руководящие принципы Совета Европы по правам человека и борьбе с терроризмом устанавливают, в отношении сбора и обработки персональных данных в контексте борьбы с терроризмом, что сбор и обработка персональных данных любыми органами, обладающими полномочиями в области государственной безопасности, могут предусматривать вмешательство в частную жизнь лиц только в случаях, если механизмы такого сбора и обработки данных:

(i) регулируются соответствующими положениями внутреннего права;
(ii) являются соразмерными цели, для которой такие сбор и обработка данных были предусмотрены;
(iii) подлежат контролю со стороны внешнего независимого уполномоченного органа.[22]

Международные инструменты необязательного характера

Помимо обязательств в рамках международного права, предусмотренных соглашениями о правах человека и

[18] UN Commission on Human Rights, *The Siracusa Principles*, para 29 [Комиссия по правам человека ООН, *Сиракузские принципы*, п. 29]

[19] Там же, п. 31.

[20] Там же

[21] UN Human Rights Committee, *CCPR General Comment No. 16: Article 17 (Right to Privacy). The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, para 10, 08 April 1988 [Комитет по правам человека ООН, *Замечание общего порядка № 16; статья 17 (Право на неприкосновенность частной жизни) Право на личную и семейную тайну, неприкосновенность жилища и тайну переписки, а также на защиту чести и репутации*, п. 10, 08 апреля 1988 г.]

[22] Council of Europe Guidelines on human rights and the fight against terrorism. 11 July 2002 [Руководящие принципы Совета Европы по правам человека и борьбе с терроризмом, 11 июля 2002 г.]

обычным международным правом, также существуют инструменты необязательного характера, которые могут быть полезными для лиц, ответственных за разработку политики, и прочих заинтересованных сторон в рамках законодательного процесса, направленного на предупреждение насильственного экстремизма и терроризма в сети Интернет и борьбу с ними. Сложность этого вопроса стала причиной возникновения ряда многосторонних инициатив, целью которых является разработка норм по модерации онлайн-контента. В связи с этим любой акт законодательной власти в сфере борьбы с контентом, пропагандирующим насильственный экстремизм и терроризм в сети Интернет, должен осуществляться с учетом указанных изменений.

Рабатский план действий по запрещению пропаганды национальной, расовой или религиозной ненависти, которая представляет собой подстрекательство к дискриминации, вражде и насилию[23], представленный в приложении к Докладу Верховного комиссара Организации Объединенных Наций по правам человека о соответствующих экспертных совещаниях, предлагает использовать тест из шести частей для определения высказываний, подлежащих преследованию в уголовном порядке. Необходимо учитывать следующие шесть факторов:

1. контекст, в котором имело место высказывание;
2. статус или положение субъекта высказывания в обществе;
3. намерение субъекта высказывания;
4. содержание и форма высказывания;
5. степень публичности и распространенности высказывания;
6. вероятность и степень неизбежности того, чтобы высказывание повлечет за собой преступное деяние.

В 2019 году государства ряда стран и некоторые ИКТ компании приняли «Крайстчерчский призыв» удалять террористические и экстремистские материалы в Интернете».[24] «Крайстчерский призыв» обязывает государства и ИКТ компании принять ряд мер по предупреждению насильственного экстремизма и терроризма в сети Интернет и борьбе с ними. Эти меры включают разработку инструментов по предотвращению загрузки террористического и экстремистского контента, борьбу с первопричинами насильственного экстремизма, увеличение прозрачности в области удаления и обнаружения контента, а также анализ того, как алгоритмы компаний приводят пользователей к контенту, пропагандирующему насильственный экстремизм.[25] На саммите «Группы двадцати» в Осаке в 2019 году главы всех 20 государств и государств приняли Заявление глав государств и государств «Группы двадцати» в Осаке о предотвращении использования Интернета для целей терроризма и насильственного экстремизма, ведущего к терроризму. Это Заявление содержит решительный призыв к онлайн-платформам проявить более ответственный подход и активизировать усилия по предотвращению трансляции, загрузки или повторной загрузки контента террористического характера, а также обязательство продолжать совместную работу по решению данной проблемы.[26]

Многосторонняя организация Глобальная сетевая инициатива разработала *Аналитическую записку об экстремистском контенте и секторе ИКТ*, в которой представлен ряд рекомендаций для государств и ИКТ компаний в части практики, которой следует избегать.[27] Например, не должны применяться ограничения по

---

[23] UN Human Rights Council, *Annual report of the United Nations High Commissioner for Human Rights – Report on the expert workshops on the prohibition of incitement to national, racial or religious hatred* (A/HRC/22/17/Add.4), 11 January 2013 [Совет по правам человека ООН, *Ежегодный доклад Верховного комиссара Организации Объединенных Наций по правам человека — Доклад об экспертных совещаниях по вопросам запрета на разжигание национальной, расовой или религиозной ненависти* (A/HRC/22/17/Add.4), 11 января 2013 г.]

[24] См. https://www.christchurchcall.com.

[25] Rt Hon Jacinda Ardern, *Christchurch Call to eliminate terrorist and violent extremist online content adopted*, 16 May 2019 [Достопочтенная Жасинда Ардерн, *«Крайстчерчский призыв» удалять террористические и экстремистские материалы в Интернете принят*, 16 мая 2019 г.]

[26] *G20 Osaka Leader's Statement on Preventing Exploitation of the Internet for Terrorism and Violent Extremism Conducive to Terrorism (VECT)*, 2019 [*Заявление глав государств и государств «Группы двадцати» в Осаке о предотвращении использования Интернета для целей терроризма и насильственного экстремизма, ведущего к терроризму (НЭВТ)*, 2019 г.]

[27] Global Network Initiative, *Extremist Content and the ICT Sector, A Global Network Initiative Policy Brief*, November 2016 [Глобальная сетевая инициатива, *Экстремистский контент и сектор ИКТ, аналитическая записка Глобальной сетевой инициативы*, ноябрь 2016 г.]

статьям или комментариям журналистов и различных СМИ в отношении террористических групп или террористических актов, при этом закон и политика должны проводить различие между высказываниями, направленными на подстрекательство к совершению террористических актов, и высказываниями, которые являются частью спора или обсуждения в отношении сообщений о таких актах.[28]

Камденские принципы по свободе выражения мнения и равенству («Камденские принципы»)[29], разработанные организацией Article 19, раскрывают взаимосвязь между аспектами свободы выражения мнения и равенства. Согласно Камденским принципам, свобода выражения мнения и равенство представляют собой взаимоподдерживающие и взаимоукрепляющие концепции; в Камденских принципах излагаются рекомендации относительно того, как снять напряжение между ними.

B. Разработка системы мер

В процессе разработки и принятия или обновления законодательства и системы мер в области решения проблем, связанных с наличием и доступностью контента с пропагандой насильственного экстремизма и терроризма в сети Интернет, следует учитывать описанные ниже элементы.

Гарантии соблюдения прав человека

Основной проблемой, присутствующей в законодательстве большинства стран, является отсутствие внимания (или незначительное внимание) к правам человека в целом и к праву на свободу выражения мнения — в частности. Законы, разрешающие блокировку или удаление контента с пропагандой насильственного экстремизма и терроризма в сети Интернет, должны приниматься в соответствии с международным правом в области прав человека. На практике этого можно достичь посредством принятия четких положений об удалении контента на основании условий пункта 3 статьи 19 МПГПП, обеспечивая при этом достаточную гибкость для того, чтобы указанные положения могли применяться с учетом технологического развития.

Принятие или обновление соответствующего законодательства

Существующее национальное законодательство в области насильственного экстремизма и терроризма зачастую не отражает текущих технологических реалий, поскольку оно было разработано до появления киберпространства. Предупреждение насильственного экстремизма и терроризма в сети Интернет и борьба с ними в отсутствие соответствующего законодательства могут привести к применению практики, нарушающей положения международного права в области прав человека, обеспечивая при этом лишь ограниченные результаты; и напротив, наличие конкретных правовых положений по этому вопросу позволит государственным учреждениям применять право более точно, ограничивая тем самым возможности для потенциального нарушения прав человека. Кроме того, широко распространена практика, когда правоохранительные органы требуют удалить контент, пропагандирующий насильственный экстремизм и терроризм в сети Интернет, основываясь исключительно на условиях оказания услуг конкретной онлайн-платформы. Это может привести к несоблюдению государственными ведомствами принципа законности, который требует, чтобы каждое действие государственного органа было основано на конкретном действующем правовом положении. Таким образом, желательно, чтобы государства приняли законы и прочие нормативные правовые акты в области решения проблем, связанных с наличием и доступностью контента с пропагандой насильственного экстремизма и терроризма в сети Интернет, или обновили соответствующее существующее законодательство с добавлением конкретных элементов, основанных на контенте.

---

[28] Там же, 4

[29] Article 19, *The Camden Principles on Freedom of Expression and Equality*, April 2009 [Article 19, *Камденские принципы по свободе выражения мнения и равенства*, апрель 2009 г.]

Разработка проектов правовых положений

Несуществующие, неопределенные или чрезмерно широкие определения контента с пропагандой насильственного экстремизма и терроризма в национальном законодательстве могут привести к чрезмерному удалению контента, исходя из политических, религиозных или идеологических причин. Этот риск можно снизить посредством принятия четких определений о контенте с пропагандой насильственного экстремизма и терроризма в сети Интернет, который подлежит блокировке или удалению. Кроме того, сотрудникам правоохранительных, судебных и прочих задействованных в этой сфере органов следует предоставить экспертное обучение в области характеристик и отличительных черт такого контента.

Процедуры независимого (судебного) контроля и подачи апелляций

Различные акты национального законодательства наделяют правоохранительные органы полномочиями указывать на контент, который они оценивают как незаконный, поставщикам интернет-услуг (ПИУ) или непосредственно онлайн-платформам (которые иногда именуются поставщиками услуг по передаче контента (ПКУ)), оставляя окончательное решение за соответствующими платформами или ПИУ. Такая практика представляет собой потенциальную угрозу для осуществления прав человека отдельными пользователями в полной мере в том случае, если за этой процедурой не обеспечивается независимый надзор. Это может привести к практике удаления контента, которая может нанести серьезный ущерб правам человека тех лиц, чей контент был заблокирован или удален. По этой причине законодательство всех стран по данному вопросу должно содержать правила, устанавливающие процедуры, которым должны следовать государственные органы, требующие заблокировать или удалить интернет-контент, а также права и обязанности ИКТ компаний как адресатов таких требований.

Более того, необходимо провести различие между решениями об удалении контента, принятыми государственными органами (в частности, правоохранительными и судебными органами) и ИКТ компаниями. Что касается первых, судебное решение может быть необходимо, поскольку государства являются основными гарантами прав человека и должны принять все необходимые предосторожности для того, чтобы предотвратить произвольное вмешательство в права человека, принадлежащие их гражданам. Если говорить о блокировке, которую ОБСЕ определяет как «деятельность, используемую для предотвращения доступа к интернет-контенту или веб-сайтам, включая платформы социальных сетей», Руководство ОБСЕ по вопросам свободы СМИ в Интернете рекомендует лицам, ответственным за разработку политики, «полагаться на блокировку только при наличии строго определенной законодательной базы в отношении контента, признанного судом незаконным».[30]

Также должна быть предусмотрена возможность обжалования решений государства в том случае, если пользователи сочтут свои права человека ограниченными незаконным образом. С другой стороны, ИКТ компании должны применять подход комплексной проверки посредством внедрения механизмов независимого контроля, чтобы пользователи имели возможность оспорить решения, касающиеся удаления контента, на основе положений национального законодательства или условий оказания услуг.

Механизмы правоприменения

Действия правоохранительных органов, связанные с предупреждением насильственного экстремизма и терроризма в сети Интернет и борьбой с ними, должны, в первую очередь, использовать меры, предусматривающие минимальное вмешательство, такие как сигнализация ИКТ компаниям об определенном контенте как о пропагандирующем насилие или экстремизм. Такие меры, как блокировка всего веб-сайта или всей платформы, следует использовать в самом крайнем случае; как указано в вышеозначенном руководстве

[30] Organization for Security and Co-operation in Europe (OSCE), Media Freedom on the Internet: *An OSCE Guidebook*, 09 March 2016 [Организация по безопасности и сотрудничеству в Европе (ОБСЕ), Свобода СМИ в Интернете: *руководство ОБСЕ*, 09 марта 2016 г.]

ОБСЕ, «блокировка не является эффективным методом решения проблем, связанных с интернет-контентом, и может иметь серьезные побочные эффекты, в том числе избыточную блокировку».[31]

В целом, для успешного применения законодательства и обеспечения его соблюдения может потребоваться ввести штрафы. Однако, если говорить о регулировании контента, потенциально высокие штрафы, в особенности в сочетании с нечетко определенными обязательствами, могут восприниматься ИКТ компаниями как стимул к блокировке или удалению законного контента для минимизации или избежания риска наложения штрафа, что в результате приведет к произвольному и сверхусердному ограничению свободы выражения мнения. Кроме того, высокие штрафы ставят под угрозу само существование небольших ИКТ компаний на рынке. В этой связи, штрафы во всех случаях должны быть соразмерными и должны налагаться в связи с четко определенными обязательствами.

Практический пример: Закон Германии о мерах в отношении социальных сетей

Закон Германии о мерах в отношении социальных сетей (Netzwerkdurchsetzungsgesetz – NetzDG) вступил в силу в октябре 2017 года (с переходным периодом до 01 января 2018 г.). Он обязывает социальные сети удалять или блокировать контент, который является явно незаконным, в течение 24 часов после получения соответствующей жалобы или в течение 7 дней, если контент не является явно незаконным (при этом в законе не определяются признаки очевидно незаконного контента). Сеть должна сохранить незаконный контент в качестве доказательства и обеспечивать его хранение в течение 10 недель. Постоянное или систематическое несоответствие требованиям закона может повлечь за собой штрафы в размере до 50 миллионов евро.

Законом установлен ряд механизмов обеспечения прозрачности, а именно: обязательство предоставлять пользователям легко опознаваемую, непосредственно доступную и постоянно действующую процедуру для подачи жалоб на незаконный контент; обязательство уведомлять лицо, подающее жалобу, а также соответствующего пользователя о любом решении с предоставлением обратившемуся лицу и автору контента мотивировки для принятия такого окончательного решения; и обязательство составлять отчеты об обработке жалоб раз в полгода для социальных сетей, получающих более 100 жалоб в год.

Помимо этого, механизмы надзора включают обязательство осуществлять мониторинг обработки жалоб посредством проведения руководством социальной сети ежемесячных проверок, а также надзор за этой процедурой со стороны ведомства, которому выполнение этой задачи поручено Федеральным министерством юстиции Германии. Кроме того, закон предоставляет пользователю возможность ответить на поступившую жалобу до вынесения решения социальной сетью в случае, если незаконность контента зависит от ложности фактического заявления или фактических обстоятельств. Наконец, закон требует, чтобы административный орган, желающий вынести решение (в частности, решение о наложении штрафа) на основании того факта, что контент, который не был удален или заблокирован, является незаконным, вначале получил решение суда, устанавливающее такую незаконность.

Закон NetzDG вызвал неоднозначную реакцию. Несмотря на то, что, в соответствии с некоторыми исследованиями, этот закон не привел к чрезмерному удалению контента, Специальный докладчик ООН по вопросу о праве на свободу мнений и их выражения выразил обеспокоенность в связи с тем, что жесткие сроки удаления контента и высокие штрафы могут быть несоразмерными и могут потенциально привести к удалению законного контента, а также в связи с тем, что отсутствует судебный контроль за удалением и стиранием контента компаниями социальных сетей.[32] Аналогичные опасения были выражены восемью из десяти экспертов, приглашенных на слушания по законопроекту.

В настоящий момент, все крупные социальные сети (Facebook, Twitter и YouTube) вначале рассматривают

[31] Там же

[32] Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression Letter reference OL DEU 01/2017, 01 June 2017. [Специальный докладчик по вопросу о поощрении и защите права на свободу мнений и их свободное выражение, письмо OL DEU 01/2017, 01 июня 2017 г.]

жалобы, поданные в соответствии с Законом NetzDG, в соответствии с собственными стандартами сообщества. В случае нарушения контент блокируется по всему миру. Если нарушение не обнаружено, жалоба оценивается с точки зрения Закона NetzDG; в случае если контент оказывается незаконным согласно положениям этого закона, доступ к нему блокируется только на территории Германии.

Меры реагирования по контенту:

2. Разработка механизмов обеспечения прозрачности и подотчетности

Настоящий раздел нацелен на оказание поддержки лицам, ответственным за разработку политики, и практикующим специалистам в разработке механизмов обеспечения прозрачности и подотчетности в рамках предупреждения насильственного экстремизма и терроризма в сети Интернет и борьбы с ними. Указанные механизмы касаются: a) организации надлежащего процесса, дающего физическому лицу возможность обжаловать решение об удалении контента, и b) информирования широкой общественности о практике и методах обращения по поводу незаконного контента и его удаления частными компаниями и государствами.

Настоящий раздел также рассказывает о важности внедрения систем мониторинга и оценки для содействия эффективной практике обращений по поводу незаконного контента и его удаления, а также для предотвращения незапланированных последствий. Данный раздел содержит три подраздела: «Механизмы обеспечения прозрачности и подотчетности», «Мониторинг и оценка мер реагирования по контенту» и «Автоматизированные процессы».

Соответствующие примеры передовой практики из Цюрихско-Лондонских рекомендаций

Передовая практика 4. *Разработка, в сотрудничестве с другими заинтересованными сторонами, общей системы мониторинга и оценки, способствующей повышению прозрачности и более глубокому пониманию воздействия мер реагирования.*

Передовая практика 7. *Принятие законов, положений и программ, направленных на противодействие наличию и доступности террористического и сопряженного с насилием контента в Интернете.*

Передовая практика 8. *Принятие во внимание соответствующих применимых и действующих международных стандартов и (или) принципов для решения проблем, связанных с наличием и доступностью террористического и сопряженного с насилием контента в Интернете и на платформах социальных сетей.*

Передовая практика 10. *Предоставление ссылок на соответствующие законы и прочие нормативные правовые акты, поощряющие направление обращений по поводу незаконного контента в ИКТ компании.*

Передовая практика 11. *Признание роли отрасли ИКТ в эффективном решении проблем, связанных с наличием и доступностью контента с пропагандой насильственного экстремизма и терроризма в сети Интернет и на платформах социальных сетей.*

Передовая практика 12. *Мониторинг и оценка применения автоматизированных процессов, используемых для ограничения повторного распространения уже существующего и (или) уже выявленного контента с пропагандой насильственного экстремизма и терроризма в сети Интернет*

ВВЕДЕНИЕ

В то время как раздел 1 рассказывает о разработке и принятии связанных с контентом законодательства и политики, настоящий раздел посвящен прозрачности и подотчетности в реализации таковых.

В некоторых странах лица, ответственные за разработку законодательных актов и политики, существенно увеличили объем правовых, кадровых и финансовых ресурсов, имеющихся в распоряжении государства для целей анализа контента, обращений по поводу незаконного контента и его удаления. Кроме того, возрастает общественное, экономическое и политическое давление на компании социальных сетей в части недопущения того, чтобы группировки насильственных экстремистов и террористов использовали их сервисы и платформы; в ответ на такое давление они начали сотрудничать с государствами и гражданским обществом в области модерации и удаления контента с пропагандой насильственного экстремизма и терроризма. Наконец, частные компании все чаще получают от государств в некоторых странах требования удалить незаконный контент в течение ограниченного срока.[33] Эти различные элементы могут привести к возрастанию уровня рисков, таких как случайное или ненамеренное подавление свободы слова в Интернете (так называемый «демотивирующий эффект» для свободы выражения мнения). В связи с этим прозрачность и подотчетность при модерации контента, направлении обращений по поводу незаконного контента и его удалении приобретают первоочередное значение с точки зрения защиты прав человека законопослушных пользователей Интернета.

Несмотря на то, что любой вид удаления контента— будь то посредством фильтров на этапе загрузки, средств автоматизированного принятия решений или сигнализирования— представляет собой ограничение свободы выражения мнения, некоторые виды ограничений касательно выражения мнений могут быть ограничены государствами в том случае, если выполнены требования, указанные в разделе 1. Но даже и в этих случаях, чрезвычайно важна прозрачность процесса для обеспечения того, чтобы соблюдалось право на свободу выражения мнения. Несмотря на то, что ведущую роль в повышении прозрачности и подотчетности в рамках мер реагирования по контенту играют государства, ИКТ компании также способны внести существенный вклад в повышение прозрачности.

A. Механизмы обеспечения прозрачности и подотчетности

Мониторинг контента

Мониторинг интернет-контента представляет собой дополнительное средство по борьбе с насильственным экстремизмом и терроризмом в сети Интернет: это может включать наблюдение, перехват, сбор и хранение данных. Несмотря на то, что мониторинг интернет-контента может помочь в обнаружении лиц, сочувствующих террористам и насильственным экстремистам, вербовщиков и террористических заговоров, те права, которые имеет человек в реальной жизни, должны также защищаться и в онлайн сфере, включая также и право на неприкосновенность частной жизни и свободу выражения мнения.[34] Как указано в разделе 1, государства не должны принимать законы и системы мер, которые запрещают шифрование и анонимность или ослабляют действие существующих инструментов цифровой безопасности.

Мониторинг интернет-контента со стороны государства может принимать различные формы. Например, в

[33] См. Раздел 1, практический пример о Netzwerkdurchsetzungsgesetz; Национальное собрание Франции; *Draft Law to Fight Hate on the Internet*, N° 1785, 20 March 2019; and European Commission, *Proposal for a Regulation of the European Parliament and the Council on Preventing the Dissemination of Terrorist Content Online* (COM(2018) 640 final), 12 September 2018 [*Законопроект о борьбе с ненавистью в Интернете*, N°1785, 20 марта 2019 г.; и Европейская комиссия, *Предложение о Регламенте Европейского Парламента и Совета по предотвращению распространения террористического контента в сети Интернет* (COM(2018) 640 окончательная версия), 12 сентября 2018 г.]

[34] См. UN Human Rights Council Resolutions on *The Promotion, Protection and Enjoyment of Human Rights on the Internet*: 20/8 (A/HRC/20/L.13), 05 July 2012, and 26/13 (A/HRC/26/L.2), 26 June 2014 [Резолюции Совета по правам человека ООН в области *Поощрения, защиты и осуществления прав человека в Интернете* 20/8 (A/HRC/20/L.13), 05 июля 2012 г. и 26/13 (A/HRC/26/L.2), 26 июня 2014 г.]

Швеции *Служба государственной безопасности Швеции* (Säkerhetspolisen[35]) осуществляет регулярный мониторинг веб-сайтов, которые могут содержать сообщения террористического характера. Деятельность Службы безопасности регулируется Законом о секторе безопасности (Förordning (2002:1050) med instruktion för Säkerhetspolisen). Однако этот закон не содержит никаких положений, которые непосредственно касаются мониторинга веб-сайтов. В случае если Служба безопасности обнаруживает контент, который она считает незаконным, она имеет право сообщить о таком контенте ИКТ компании, на чьих сервисах такой контент присутствует, и инициировать предварительное расследование, но не уполномочена принимать меры к удалению какого-либо контента.[36]

В Австралии Уполномоченный по вопросам электронной безопасности и находящееся в его ведении Группа за наблюдением киберпространства[37] проводят расследования по полученным жалобам на запрещенные материалы, которые, например, поощряют совершение преступлений или актов насилия, предоставляют инструкции о том, как это сделать, подстрекают к таким действиям, или оправдывают совершение террористического акта. Группа за наблюдением киберпространства оценивает интернет-контент, в отношении которого поступило обращение, согласно Национальной схеме классификации («Схема») и другим применимым законам, выделяя в приоритетном порядке серьезные материалы, которые, например, могут быть сочтены контентом, пропагандирующим терроризм, и «вызывающими отвращение материалами со сценами насилия». Последние представляют собой контент, демонстрирующий убийства, террористические акты, приводящие к смерти или серьезным травмам, а также прочие жестокие преступления, записанные лицом, совершившим такое преступление, или его пособниками. Такие виды контента с большой вероятностью будут отнесены к группе отклоненных материалов в соответствии со Схемой и будут считаться запрещенными в случае их размещения на территории Австралии. После проведения оценки материалов Группа за наблюдением киберпространства может уведомить о ее результатах соответствующего поставщика услуг хостинга в целях устранения. Уведомление об устранении, направляемое Группой за наблюдением киберпространства хостинговому сервису, имеет соответствующую санкцию, и за его невыполнение предусмотрены серьезные штрафы.

В Швейцарии, находящаяся в структуре Федерального департамента полиции, Координационная группа по вопросам киберпреступности Швейцарии (CYCO) активно проводит поиск незаконного контента в Интернете и получает соответствующие сообщения. После проведения оценки соответствующего контента и получения необходимых данных, CYCO передает дело на рассмотрение в соответствующие правоохранительные органы.[38]

Повышение уровня прозрачности и подотчетности

Прозрачность и подотчетность имеют определяющее значение для прогнозирования и минимизации потенциальных отрицательных последствий принимаемых мер реагирования по контенту в рамках предупреждения насильственного экстремизма и терроризма в сети Интернет и борьбы с ними, в том числе в контексте мониторинга контента в Интернете, а также его потенциального воздействия на осуществление прав человека.

Государствам рекомендуется ссылаться на соответствующее национальное законодательство, которое составляет основу для обращения при направлении требования об удалении незаконного контента ИКТ компаниям. Такая прозрачность процессов принятия решений укрепляет доверие к соответствующим заинтересованным сторонам и между ними. В этом отношении Государствам рекомендуется обеспечить доступ

---

[35] https://www.sakerhetspolisen.se/

[36] Swiss Institute of Comparative Law, *Comparative Study on Blocking, Filtering and Take-Down of Illegal Internet Content*, p. 671, 20 December 2015 [Швейцарский институт сравнительного права, *Сравнительное исследование в области блокировки, фильтрации и устранения незаконного интернет-контента*, стр. 671, 20 декабря 2015 г.]

[37] См. https://www.esafety.gov.au

[38] См. https://www.cybersecurityintelligence.com/cybercrime-coordination-unit-switzerland-cyco-2085.html

к соответствующим законам и прочим нормативным правовым актам.

Надежные механизмы обеспечения прозрачности и подотчетности также должны предоставлять физическим лицам доступ к средствам правовой защиты в случае неправомерного удаления их контента, в особенности если государственными и негосударственными участниками при этом были нарушены права на свободу выражения мнения или на неприкосновенность частной жизни. Руководящие принципы ООН по предпринимательской деятельности в аспекте прав человека представляют новую итерацию принципа доступа к средствам правовой защиты в рамках обязанности государства «посредством судебных, административных, законодательных или иных соответствующих средств... принимать надлежащие меры для обеспечения того, чтобы в случаях, когда такие нарушения происходят на их территории и (или) в пределах их юрисдикции, затрагиваемые стороны получали доступ к эффективным средствам правовой защиты.[39] Такие механизмы правовой защиты могут включать обязательства по предоставлению доступа к «средствам правовой защиты и механизмам подачи и рассмотрения жалоб, чтобы обеспечить возможность для пользователей оспорить удаление их контента», как предлагается Европейской комиссией.[40]

Европейская комиссия поручила Институту по правам человека и предпринимательской деятельности и организации гражданского общества Shift разработать пособие для отрасли ИКТ в отношении корпоративного обязательства соблюдать права человека на основе Руководящих принципов ООН по предпринимательской деятельности в аспекте прав человека. Цель пособия состоит в том, чтобы оказать поддержку ИКТ компаниям в адаптации принципов, указанных в Руководящих принципах ООН, к собственным системам и культурам таких ИКТ компаний.[41] Пособие включает конкретные указания относительно того, каким образом компании могут разработать систематические внутренние процессы, чтобы быть лучше подготовленными к надлежащей и оперативной обработке требований государства об удалении данных и (или) контента с соблюдением прав человека. Кроме того, в руководстве приводятся рекомендации и указания относительно того, каким образом ИКТ компании могут сообщить о проведении этой работы эффективным и прозрачным способом.

Сантакларские принципы прозрачности и подотчетности при модерации контента, разработанные рядом ученых и некоммерческих организаций, включая Фонд противодействия нарушениям конфиденциальности и гражданских свобод с применением электронных технологий, Американский союз защиты гражданских свобод и Центр демократии и технологий, рекомендуют компаниям публиковать количество удаленных постов и временно или постоянно заблокированных аккаунтов, уведомлять каждого пользователя о причине удаления или блокировки его аккаунта, а также предоставлять реальную возможность для своевременного обжалования таких действий.[42]

Практический пример: Ranking Digital Rights

Ranking Digital Rights (RDR) («Рейтинг цифровых прав») — это некоммерческий исследовательский проект, реализуемый в рамках Института открытых технологий Фонда New America. RDR публикует ежегодный индекс воздействия обязательств и политики ИКТ компаний на свободу выражения мнения и неприкосновенность частной жизни пользователей, основываясь на положениях международного права в области прав человека. Таким образом, индекс RDR предлагает четкие стандарты для компаний, приверженных обязательству соблюдать права человека на свободу выражения мнения и неприкосновенность частной жизни, а также

[39] *UN Guiding Principles on Business and Human Rights*, 2011 [*Руководящие принципы предпринимательской деятельности в аспекте прав человека ООН*, 2011 г.]

[40] European Commission, *Proposal for a Regulation on Preventing the Dissemination of Terrorist Content Online*, 2018 [Европейская комиссия, *Предложение о Регламенте по предотвращению распространения террористического контента в сети Интернет,* 2018 г.]

[41] Shift and Institute for Human Rights and Business, *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights*, European Comission, June 2013 [Организация Shift и Институт по правам человека и предпринимательской деятельности, *Руководство для отрасли ИКТ по реализации Руководящих принципов предпринимательской деятельности в аспекте прав человека ООН*, Европейская комиссия, июнь 2013 г.]

[42] *The Santa Clara Principles On Transparency and Accountability in Content Moderation*, 02 February 2018 [*Сантакларские принципы прозрачности и подотчетности в практике модерации контента*, 02 февраля 2018 г.]

способствует повышению уровня прозрачности и подотчетности компаний, публикуя свои общедоступные оценки.

В 2019 году в рамках Индекса ответственности корпораций RDR[43] была проведена оценка 24 компаний на основе 35 показателей, анализирующих «механизмы корпоративного управления компаний, чтобы определить потенциальные угрозы для пользователей, с позиции соблюдения прав человека, и предотвратить их наступление, а также раскрытые положения их политики, влияющие на свободу выражения мнения и неприкосновенность частной жизни пользователей».[44] Несмотря на улучшения, наблюдающиеся у компаний, которые оценивались ранее, в отчете отмечаются продолжающиеся проблемы с прозрачностью процедур по удалению контента. При расчетах индексов также было установлено, что компании все еще не обеспечили надлежащие механизмы подачи и рассмотрения жалоб и доступа к средствам правовой защиты, которые помогают сообщать о проблемах и устранять причиненный вред. При этом следует отметить, что компании-участницы Глобальной сетевой инициативы (см. ниже) получили более высокие индексные оценки, чем компании, не участвующие в ней.

Кроме того, в конце отчета RDR представлены конкретные рекомендации для компаний и для государств.[45] Государства также могут ознакомиться с отчетами RDR, чтобы лучше понять, в какой степени компании выполняют положения международного права в области прав человека.

Практический пример: Глобальная сетевая инициатива

Глобальная сетевая инициатива (GNI) — это многосторонняя платформа, целью которой является защита и развитие свободы выражения мнения и неприкосновенности личной жизни в сфере ИКТ. Принципы GNI, которые все компании-участницы GNI обязались соблюдать, создают основу для постоянно развивающейся системы ответственного принятия компаниями решений, которые обеспечивают соблюдение прав на свободу выражения мнения и неприкосновенность частной жизни.[46] Поскольку все больше компаний присоединяются к GNI, ожидается, что эти принципы будут «внедрены как международный стандарт в области защиты прав человека в сфере ИКТ»,[47] способствуя тем самым соблюдению прав человека, а также повышению уровня прозрачности и подотчетности ИКТ компаний.

Каждые два года компании-участницы GNI проходят независимую оценку с точки зрения их прогресса в реализации принципов GNI. Целью оценки является понимание того, что компании «добросовестно работают над реализацией принципов GNI и обеспечивают улучшение с течением времени». С этой целью текущие результаты компании оцениваются по сравнению с их прошлыми результатами. В рамках оценки рассматриваются системы, политика и процедуры компании, а также оценивается ряд практических примеров того, как компания справилась с конкретными инцидентами, и как можно улучшить применяемые ею меры реагирования. Оценка проводится несколькими независимыми учреждениями,[48] аккредитованными многосторонним советом GNI согласно критериям их независимости и компетентности.[49]

---

[43] Ranking Digital Rights, *2019 Ranking Digital Rights Corporate Accountability Index* [Проект «Рейтинг цифровых прав», *Индекс ответственности корпораций — 2019 от проекта «Рейтинг цифровых прав»*]

[44] См. https://rankingdigitalrights.org/about/our-work.

[45] *Recommendations for governments*, in: Ranking Digital Rights, *2018 Corporate Accountability Index* [*Рекомендации для правительств*, в издании: *Индекс ответственности корпораций — 2018 от проекта «Рейтинг цифровых прав»*]

[46] Global Network Initiative, Principles on Freedom of Expression and Privacy [Глобальная сетевая инициатива, Принципы свободы выражения мнения и неприкосновенности частной жизни]

[47] См. https://globalnetworkinitiative.org/about-gni.

[48] См. https://globalnetworkinitiative.org/independent-assessors.

[49] Global Network Initiative, *GNI Independence and Competency Criteria*. Updated August 2018 [Глобальная сетевая инициатива, *Критерии независимости и компетентности GNI*. Обновлено в августе 2018 г.]

Отчеты в целях обеспечения прозрачности

В то время как ведущую роль в повышении прозрачности и подотчетности в рамках мер реагирования по контенту, направленных на предупреждение насильственного экстремизма и терроризма в сети Интернет и борьбы с ними, играют государства, например, посредством принятия соответствующих законов или статей уголовного кодекса касательно обращений к ИКТ компаниям по поводу определенного контента, чтобы они провели его оценку, ИКТ компании также могут внести свой важный вклад в повышение прозрачности и подотчетности в этом процессе.

Представление отчетов в целях обеспечения прозрачности, которые дают информацию о том, в каком порядке компании осуществляют удаление контента на своих сервисах, может быть важным шагом к тому, чтобы общественность начала лучше понимать, в каких случаях происходит удаление контента, а также контент какого типа удаляется. Один из такого рода примеров реализуемой государством практики является Закон Германии о мерах в отношении социальных сетей (Netzwerkdurchsetzungsgesetz от 01 сентября 2017 г. (BGBl. I S. 3352), который более подробно описывается в разделе 1; он требует, чтобы платформы социальных сетей, получающие более 100 жалоб в течение календарного кода, раз в полгода публиковали отчеты об обработке жалоб. Кроме того, данный закон обязывает компании уведомлять лицо, подающее жалобу, а также соответствующего пользователя о принятом решении, с предоставлением пользователю разъяснений причин принятия такого решения. Аналогичные положения предусматриваются также и предлагаемым Европейской комиссией Регламентом по предотвращению распространения террористического контента в сети Интернет. Такие требования предусматривают механизмы для обеспечения большей прозрачности в отношении того, каким образом компании осуществляют регулирование контента на платформах социальных сетей.

Практический пример: Twitter

Согласно правилам и политике Twitter, «прозрачность критически важна для защиты свободы выражения мнения».[50] В связи с этим Twitter публикует полугодовые отчеты в целях обеспечения прозрачности, в которых отражаются текущие тенденции и осуществляется открытый обмен информацией.[51]

Политика Twitter в целом состоит в том, чтобы в кратчайшие сроки уведомлять пользователей о запросе информации в отношении их аккаунтов Twitter или Periscope, что включает направление им копии поступившего запроса, за исключением случаев, когда компании Twitter запрещено это делать. В соответствии с политикой Twitter в отношении конфиденциальной информации, компания также может раскрыть данные аккаунта правоохранительным органам в ответ на допустимый срочный запрос о раскрытии информации (напр., согласно § 2702(b)(8) раздела 18 Свода законов США (U.S.C.) или разделу 8 Закона о защите данных Ирландии от 1988 г. и 2003 г.).

Кроме того, Twitter сотрудничает с рядом организаций, такими как Parle-moi d'islam (Франция), Imams Online (Великобритания) или True Islam (США) в области борьбы с насильственным экстремизмом на платформе Twitter. В соответствии с политикой Twitter в отношении поддержки правоохранительных органов, Twitter предоставляет ответ на действительные судебные приказы о представлении информации в соответствии с действующим законодательством;[52] при этом компания разработала для правоохранительных органов собственный веб-сайт для подачи юридических запросов.[53]

[50]. См. https://help.twitter.com/en/rules-and-policies/tweet-withheld-by-country.

[51] См. последнюю версию https://transparency.twitter.com/en/information-requests.html#information-requests- jul-dec-2018.

[52] См. https://help.twitter.com/en/rules-and-policies/tweet-withheld-by-country

[53] См. https://legalrequests.twitter.com/forms/landing_disclaimer.

Практический пример: Инструментарий для представления отчетов в целях обеспечения прозрачности Института открытых технологий

Институт открытых технологий в структуре Фонда New America, аналитический центр, базирующийся на территории Соединенных Штатов Америки, публикует инструментарии для представления отчетов в целях обеспечения прозрачности, в которых оцениваются примеры передовой практики в области представления компаниями отчетов в целях обеспечения прозрачности, а также проводится обзор показателей, по которым отчитываются наиболее известные ИКТ компании.[54]

Признавая, что общественное давление в части повышения прозрачности привело к тому, что ИКТ компании стали расширять применение мер по обеспечению прозрачности, Институт открытых технологий считает, что сохраняется потребность в большей стандартизации того, каким образом компании отчитываются об удалении контента, а также в большей детализации того, какие данные при этом передаются. Несогласованность показателей и стандартов при составлении отчетов создает препятствия для проведения сравнения по всей отрасли и между различными компаниями для оценки воздействия удаления контента на наличие материалов насильственных экстремистов и их поведение в части распространения таковых в Интернете. Несмотря на то, что некоторые показатели варьируются в зависимости от конкретной платформы по причине различия в видах размещенного на них контента, Институт открытых технологий говорит о том, что при этом единый набор показателей, который может использоваться надлежащим образом, остается полезным и необходимым для проведения сравнений между компаниями и оценки воздействия. Более того, представление отчетов об удалении контента компаниями в результате нарушения их собственных условий оказания услуг или руководств по регулированию контента происходит нечасто и непостоянно, несмотря на то, что Facebook, Google и Twitter (и в меньшей степени — Microsoft) начали отчитываться по этому показателю в 2018 году.

Чтобы обозначить важность этого вопроса, в мае 2019 года Фонд противодействия нарушениям конфиденциальности и гражданских свобод с применением электронных технологий запустил свой проект TOSsed out, который предусматривает сбор контента, который был удален по причине несоответствия условиям оказания услуг самих платформ, которые Фонд считает применяемыми произвольно и несправедливо, а также недостаточно прозрачными.[55]

B. Мониторинг и оценка мер реагирования по контенту

Системы мониторинга и оценки

Демонстрация результативности имеет определяющее значение для обоснования правомерности и эффективности принимаемых мер для предупреждения насильственного экстремизма и терроризма в сети Интернет и борьбы с ними. Непрерывный мониторинг и оценка мер реагирования по контенту позволяют создать информационную основу для разработки законов и формирования системы мер в области процедур обращения по поводу незаконного контента и его удаления, в том числе посредством совершенствования практики определения целевого контента и его обнаружения, а также посредством устранения рисков нарушения прав человека по мере их появления.

Тот факт, что в настоящее время практические исследования и данные в отношении мер реагирования по

[54] New America Open Technology Institute, The Transparency Reporting Toolkit: Content Takedown Reporting, last updated 25 October 25, 2018 [Институт открытых технологий Фонда New America, Инструментарий для представления отчетов в целях обеспечения прозрачности: отчета об устранении контента, последнее обновление: 25 октября 2018 г.]

[55] См. https://www.eff.org/tossedout

контенту и их эффективности отсутствуют, вызывает особую обеспокоенность, поскольку это означает, что государства и ИКТ компании могут использовать ценные финансовые и кадровые ресурсы и программы не по назначению, что может привести к незапланированным и даже губительным последствиям с точки зрения прав человека. В этой связи государствам рекомендуется использовать, там где это возможно, опыт применения систем мониторинга и оценки, существующих в других секторах, в том числе в сфере здравоохранения, а также коммерческой рекламы и маркетинга.

Организация систем мониторинга и оценки

Системы мониторинга и оценки являются основными элементами разработки эффективных и действенных мер реагирования по контенту в деле профилактики и борьбы с насильственным экстремизмом и терроризмом в сети Интернет, и должны быть интегрированы в соответствующие законы и системы мер, а также в их практическую реализацию с самого начала.[56]

Государствам рекомендуется разработать, совместно с соответствующими заинтересованными сторонами, включая также представителей отрасли ИКТ, гражданского общества, а также научных учреждений, реалистичные способы и средства измерения результативности мер, предпринятых законами, системами мер и программ. Это означает, что с самого начала следует установить четко определенные целевые показатели для конкретных мер реагирования по контенту в части воздействия (возможно, опираясь на теории изменений, описанные в соответствующих системах мер), а также базовые значения таких целевых показателей для оценки воздействия. Мониторинг и оценка должны основываться на данных, определениях, методологиях и показателях успеха, которые открыто публикуются, являются согласованными и сопоставимыми.

Количественные показатели и инструменты

Учитывая огромный объем имеющихся данных, особенно важно сфокусировать системы мониторинга и оценки на определенный набор данных, чтобы иметь возможность извлечь значимую информацию для лиц, занимающихся разработкой законодательных актов, и лиц, ответственных за формирование политики. Кроме того, процессы сбора данных и информации должны быть организованы таким образом, чтобы они обеспечивали защиту таких прав человека, как право на свободу выражения мнения и неприкосновенность частной жизни, а также защиту законом для всех, без какой-либо дискриминации, что может ограничить способность государства собирать определенные данные или, по крайней мере, использовать их.

Возможные основные элементы для проведения мониторинга и оценки мер реагирования по контенту (не все из которых могут быть доступны в конкретной стране) включают:

- количество обращений с требованием об удалении контента и конкретные основания для таких обращений;
- основание обращения (национальное законодательство и (или) условия оказания услуг ИКТ компаний);
- характер физических или юридических лиц, направляющих обращение, такие как государственные учреждения (с возможной разбивкой на подразделения по контролю интернет-пространства и прочие учреждения); судебные органы, гражданское общество, ИКТ компании и физические лица;
- каналы, используемые для обращения (обращения подразделений по контролю интернет-пространства, инструменты, доступные доверенным сигнализирующим лицам, общедоступные формы);
- общее количество обращений по каждой соответствующей ИКТ компании;

[56] См., например, European Commission's *Proposal for a Regulation on Preventing the Dissemination of Terrorist Content Online*, [*Предложение* Европейской комиссии *о Регламенте по предотвращению распространения террористического контента в сети Интернет*], в частности, статьи 21 и 23, посвященные мониторингу и оценке

- время, потребовавшееся соответствующей ИКТ компании для анализа контента, в отношении которого она получила обращение;
- количество и процент обращений, которые привели к удалению контента;
- в случаях, когда это возможно и целесообразно, количество раз, когда контент, который был впоследствии удален, просматривался и вызывал интерес, и на протяжении какого времени он был доступен в Интернете до момента удаления;
- общее количество удалений контента и конкретные основания удаления;
- количество удалений контента, которые были обжалованы, и конкретные использованные процедуры обжалования (судебная/административная/механизм подачи и рассмотрения жалоб компании);
- количество принятых и отклоненных обжалований;
- в соответствующих случаях — обзор санкций, в частности, финансовых и уголовных.

Инструменты и возможности для проведения мониторинга и оценки

Количественные показатели применения мер реагирования на основе контента можно отслеживать с помощью общих механизмов мониторинга государственных/судебных органов, а также посредством аналитических инструментов, в частности, инструментов ИКТ компаний.

Информация об обращениях по поводу незаконного контента и о его удалении на основе распоряжений суда должна присутствовать в информационных системах, которые обычно используются судебными органами, и государство должно иметь возможность доступа к таким сведениям, как и в случае с другими судебными разбирательствами. Государству следует определить подходящие способы для регулярного получения обновленных данных от ИКТ компаний по поступившим обращениям и удалениям контента, осуществленным в соответствии с их собственными условиями оказания услуг; при этом ИКТ компании должны выполнять такие запросы государства в той степени, в какой они соответствуют положениям международного права в области прав человека и национального законодательства. Подразделения по контролю интернет-пространства также будут иметь в своем распоряжении систему для регистрации своих обращений, и они должны также учитываться государством.

Однако, даже если ограничить объем данных, поступающих в систему мониторинга и оценки вышеописанным способом, он все равно останется существенным. Повышение потенциала государства в области обработки значительных объемов данных и визуализации наборов данных может создать существенную дополнительную ценность с точки зрения непрерывной адаптации мер реагирования на основе контента и соответствующих гарантий соблюдения прав человека. Кроме того, государства могут принять решение финансировать проекты, реализуемые научными учреждениями и гражданским обществом, чтобы создать возможность для разработки инновационных подходов к проведению мониторинга и оценки.

Качественные показатели и инструменты

Описанные выше количественные методы с большой вероятностью позволят получить значительный массив информации. Тем не менее, их сочетание с качественными элементами, вероятнее всего приведет к получению гораздо более впечатляющих результатов оценки. Вот один из примеров: сотрудники правоохранительных органов проводят качественную оценку в дни Совместной оценки с участием подразделений по контролю интернет-пространства, чтобы оценить предпочтительность конкретной платформы для насильственных экстремистов и террористов, а также модели ее использования ими.[57] Дополнительные методы могут включать, например, (полу)структурированные интервью с лицами, которые производят контент с пропагандой насильственного экстремизма и терроризма в сети Интернет, делятся им или ставят такому контенту отметки

[57] Europol, *Referral Action Day with six EU Member states and Telegram*, 05 October 2018 [Европол, *День контроля контента с участием шести государств-членов ЕС и Telegram*, 05 октября 2018 г

«нравится», а также понимание того (опять же, посредством личного взаимодействия), каким образом более широкие группы интернет-пользователей подвергаются воздействию контента такого типа и как они с ним взаимодействуют.

Качественная оценка не только позволяет создать логику зачастую непомерных массивов данных, но также повышает уровень прозрачности работы ее участников в отношении конкретной практики — сам процесс качественного анализа становится частью размышлений о мерах реагирования на основе контента и их оптимизации.

Дополнительная ценность прозрачности процессов мониторинга и оценки

Результаты мониторинга и оценки должны быть общедоступны во всех возможных случаях, чтобы заинтересованные стороны, не принадлежащие к государственному сектору, включая представителей отрасли ИКТ, организаций гражданского общества и научных учреждений, имели возможность изучить и проанализировать их, чтобы представить свои предложения относительно возможных изменений. Следующим шагом может стать предоставление даже самих данных в форме так называемых наборов открытых данных; изучение таких данных заинтересованными сторонами, не принадлежащими к государственному сектору, потенциально может обеспечить еще более глубокое понимание их значимости для укрепления систем мониторинга и оценки.

Поскольку даже успешно функционирующие учреждения сталкиваются с проблемой присущей субъективности при проведении анализа, во всех случаях, когда это возможно, мониторинг и оценку следует проводить с привлечением автономных государственных органов (например, национальных служб статистики) или, по крайней мере, полагаясь на их технический опыт в организации таких систем мониторинга и оценки. Кроме того, регулярная независимая оценка как самих систем, так и образцов собранных данных может помочь получить свежий взгляд, способствуя укреплению систем мониторинга и оценки в целом.

Проблемы мониторинга и оценки

При проведении мониторинга и оценки воздействия мер реагирования на основе контента возникает ряд присущих этим процессам проблем. Во-первых, необходимо (хотя и сложно) оценить, приводит ли удаление контента к перемещению контента с пропагандой насильственного экстремизма и терроризма на другие платформы, которые могут регулироваться в меньшей степени. Различный опыт, полученный платформами в области удаления контента, также указывает на необходимость следования всеотраслевому подходу, который предусматривает оценку общего уменьшения, а не «удачи» достигнутой на какой-либо отдельной платформе, которая может привести к возрастанию количества контента террористического характера на других платформах за счет его «выдавливания» на более мелкие и в меньшей степени регулируемые платформы или в более зашифрованные каналы.

Тщательная проработка структуры оценки может решить некоторые из этих проблем. Тем не менее, всесторонние системы мониторинга и оценки также должны быть прозрачными с точки зрения ограничений на используемые методы, данных, которые могут быть собраны (как с технической точки зрения, так и с точки зрения требований к конфиденциальности данных), а также результатов оценки, которые можно будет из них впоследствии получить.

C. Автоматизированные процессы

Минимизация рисков, связанных с автоматизированными процессами

Поскольку все больше компаний разрабатывают и используют автоматизированные процессы, ускоряющие выявление и удаление незаконного контента, роль ИКТ компаний в развитии эффективных механизмов обеспечения прозрачности и подотчетности становится более важной, в особенности с учетом риска для права

на свободу выражения мнения, который может быть связан с такими автоматизированными процессами. ИКТ компаниям надлежит обеспечить эффективный и действенный анализ автоматизированных процессов, а также внедрение надлежащих механизмов обжалования.

Автоматизированные процессы могут серьезно нарушить права человека затрагиваемых ими пользователей в случае блокировки или удаления контента. Например, после того, как YouTube внедрила новую технологию автоматической сигнализации о контенте, нарушающем ее условия оказания услуг, и удаления такого контента, группа активистов-правозащитников пожаловалась на то, что тысячи загруженных на YouTube видеороликов, запечатлевших предполагаемые военные преступления, были удалены, поскольку автоматизированные процессы оценили их как нарушающие положения руководства по регулированию контента.[58]

Примеры автоматизированных процессов для обнаружения и удаления контента с пропагандой насильственного экстремизма и терроризма

Автоматизированные процессы все чаще используются крупными социальными сетями для обнаружения незаконного контента на своих платформах, сигнализации о таком контенте и (или) его удаления; в частности, это касается Facebook, Twitter и YouTube. Каждая платформа использует свои виды автоматизированных процессов.[59]

Facebook. Facebook использует машинное обучение для оценки постов на Facebook, которые могут сигнализировать о поддержке ДАИШ/ИГИЛ или «Аль-Каиды». Этот инструмент генерирует определенный балл, указывающий на вероятность того, что тот или иной пост нарушает политику Facebook в области борьбы с терроризмом, что помогает группе ответственных за проверку в компании. Кроме того, Facebook начала применять искусственный интеллект (ИИ).[60] В частности, ИИ используется для направления нового загруженного контента к проверяющему-человеку, для определения кластеров страниц, постов, групп или профилей, содержащих террористический контент, а также для проверки фотографий и видеороликов по имеющейся базе данных. По словам руководителя отдела политики в области борьбы с терроризмом Facebook, компания находится на начальном этапе разработки использования искусственного интеллекта по анализу текста. Кроме того, Facebook использует ИИ для сокращения периода, в течение которого аккаунты террористов-рецидивистов остаются доступными на Facebook.[61]

Twitter. Twitter все в большей степени сосредотачивается на превентивном выявлении проблемных аккаунтов на своей платформе.[62] В своем отчете компания отметила, что ее собственные, внутренние инструменты в упреждающем порядке просигнализировали о 91 % от всех 205 156 заблокированных аккаунтов. Вследствие этого на сообщения от государственных органов за отчетный период пришлось лишь 0,1 % от общего числа блокировок.

YouTube В 2018 году в своей публикации в блоге YouTube подчеркнула, что «машины позволяют нам отмечать контент, который требуется проанализировать, на должном уровне, помогая нам удалять миллионы видеороликов с нарушениями, прежде чем они будут просмотрены». Согласно представленным статистическим данным, за период с октября по декабрь 2017 года компания YouTube удалила 8 миллионов видеороликов, о 6.7 миллионах из которых вначале просигнализировали машины, при этом 76 % из них были

[58] Submission by AccessNow to David Kaye, Special Rapporteur on the promotion and protection for the right to freedom of opinion and expression in response to questions for the “Study on Content Regulation in the Digital Age”, January 2018 [Документы, представленные организацией AccessNow Дэвиду Кэю, Специальному докладчику по вопросу о поощрении и защите права на свободу мнений и их свободное выражение, в ответ на вопросы для «Исследования в области регулирования контента в цифровую эпоху», январь 2018 г.]

[59] Перечень таких компаний взят из публикации: Nikita Malik, *The Fight Against Terrorism Online: Here’s The Verdict*, Forbes, 20 September 2018

[60] *A View from the CT Foxhole: An Interview with Brian Fishman, Counterterrorism Policy Manager, Facebook*. Combating Terrorism Centre, US Military Academy. September 2017, Volume 10, Issue 8

[61] Facebook, *Hard Questions: How We Counter Terrorism*, 15 June 2017

[62] Twitter, *How Twitter is fighting spam and malicious automation*, 26 June 2018.

удалены прежде, чем были просмотрены хоть один раз.[63]

Права человека и искусственный интеллект: роль государства

ИКТ компании все чаще используют искусственный интеллект (ИИ) для модерации контента, в частности, в рамках автоматизированных процессов. Системы ИИ применяются для контроля контента, размещаемого пользователями в Интернете, на предмет обнаружения потенциальных нарушений условий обслуживания. Несмотря на то, что системы ИИ могут быть весьма эффективными с точки зрения выявления контента с пропагандой терроризма или насильственного экстремизма, их алгоритмы могут ошибочно отмечать контент как незаконный, что может привести к серьезным нарушениям прав человека и прочих прав соответствующих пользователей в случае блокировки или удаления контента. Таким образом, требуется законодательство, регулирующее использование и параметры инструментов для модерации контента на базе ИИ; это включает требования в отношении инструментов обратной связи/сигнализации для физических лиц, которые считают, что их контент был удален незаконно.[64]

Специальный докладчик ООН по вопросам свободы выражения мнений рекомендует, чтобы «государства обеспечивали центральное положение прав человека для частного сектора при разработке, развертывании и внедрении систем ИИ».[65] Специальный докладчик также отметил, что государства могут выполнять свои обязательства в области защиты прав человека «посредством принятия правовых мер по ограничению разработки и внедрения приложений ИИ или оказанию влияния на эти процессы посредством разработки системы мер в отношении закупки приложений ИИ у частных компаний представителями государственного сектора, посредством программ саморегулирования и совместного регулирования, а также посредством наращивания потенциала компаний частного сектора в области признания и приоритезации прав на свободу мнений и свободу их выражения в своей корпоративной деятельности».[66]

Наконец, автоматизированные процессы при принятии решения об удалении контента на том основании, что он пропагандирует насильственный экстремизм или терроризм, должны применяться наряду с мерами по контролю, осуществляемому человеком, а также при принятии решений в процессе обжалования. Соответствующие положения об этом могут быть прописаны в национальном законодательстве.

---

[63] См. https://youtube.googleblog.com/2018/04/more-information-faster-removals-more.html

[64] См., например, European Commission's *Proposal on Preventing the Dissemination of Terrorist Content Online*, [*Предложение* Европейской комиссии *о Регламенте по предотвращению распространения террористического контента в сети Интернет*], в частности, статьи 9 и 10, посвященные конкретным гарантиям, связанным с использованием автоматизированных инструментов.

[65] UN General Assembly, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression on Artificial Intelligence technologies and implications for the information environment*, (A/73/348), para 63, 29 August 2018 [Генеральная Ассамблея ООН, *Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение о технологиях искусственного интеллекта и их последствиях для информационной среды* (A/73/348), п. 63, 29 августа 2018 г.]

[66] Там же, п. 22

Меры реагирования по контенту:

3. Реализация мер реагирования по контенту посредством многостороннего сотрудничества

Данный раздел предназначен для лиц, ответственных за разработку политики, и практикующих специалистов и содержит конкретные практические примеры сотрудничества между государствами, ИКТ компаниями и гражданским обществом. В частности, примеры сотрудничества между государствами, ИКТ компаниями и гражданским обществом; между ИКТ компаниями; а также между ИКТ компаниями и гражданским обществом. Данный раздел содержит два подраздела: «Многостороннее сотрудничество» и «Дальнейшие инициативы».

Соответствующие примеры передовой практики из Цюрихско-Лондонских рекомендаций:

Передовая практика 3. *Выработка четкой стратегии борьбы с насильственным экстремизмом и терроризмом в сети Интернет на основе подхода объединяющего участие соответствующих государственных учреждений и всего общества, координирующего меры реагирования как на основе контента, так и на основе коммуникаций, а также оффлайн- мероприятия, включая, при необходимости, обучение и вовлечение организаций гражданского общества.*

Передовая практика 6. *Принятие многостороннего подхода для взаимодействия между государствами, представителями отрасли ИКТ и организациями гражданского общества в работе по предупреждению насильственного экстремизма и терроризма в сети Интернет и борьбе с ними.*

Передовая практика 9. *Организация эффективного сотрудничества и поощрение, в необходимых случаях, более активного участия отрасли ИКТ, а также сотрудничество с организациями гражданского общества в борьбе с контентом, пропагандирующим насильственный экстремизм и терроризм в сети Интернет и на платформах социальных сетей.*

Передовая практика 11. *Признание роли отрасли ИКТ в эффективном решении проблем, связанных с наличием и доступностью контента с пропагандой насильственного экстремизма и терроризма в сети Интернет и на платформах социальных сетей.*

Введение

Программные заявления крупнейших ИКТ компаний четко говорят о том, что эта отрасль, включая компании социальных сетей, стала основным инструментом общества для доступа к информации, обмена информацией и ее обсуждения. Генеральный директор Facebook описал миссию своей компании в «оказании помощи людям во всем мире объединиться в глобальное сообщество и стать ближе друг к другу».[67] Компания «ВКонтакте» видит свою миссию в том, чтобы «соединять людей, сервисы и компании через простые и удобные инструменты коммуникации».[68] Цель Google — «удобно организовать всю информацию в мире и сделать ее доступной и полезной каждому».[69] Tencent стремится к тому, чтобы «повысить качество жизни посредством преимуществ интернет-услуг».[70]

Учитывая то, что значительная часть инфраструктуры, лежащей в основе Интернета, принадлежит частным ИКТ компаниям, в цифровую эру все более возрастает их роль при принятии мер по предупреждению насильственного экстремизма и терроризма и борьбе с ними. Принимая во внимание огромное значение частых ИКТ компаний, а также транснациональные характеристики цифрового пространства, эффективное сотрудничество между всеми заинтересованными сторонами — государствами, отраслью ИКТ и гражданским обществом — является необходимым условием для предупреждения насильственного экстремизма и терроризма в сети Интернет и борьбы с ними. Тем не менее, эти частные компании зачастую сталкиваются с рядом проблем в рамках совместного и самостоятельного регулирования своих платформ, в особенности в той сфере, которая затрагивает вопросы прав человека.[71]

Наращивание усилий по предупреждению насильственного экстремизма и терроризма в сети Интернет и борьбе с ними, которые сочетают в себе государственные, государственно-частные и частные механизмы, говорит о более фундаментальном сдвиге в способе ведения бизнеса в глобальном масштабе. С учетом этой тенденции, сотрудничество между различными заинтересованными сторонами — государствами, бизнесом и гражданским обществом — может рассматриваться как прагматичный ответ, направленный на заполнение некоторых пробелов в традиционных подходах к регулированию, установленных государствами. Фактически такие инициативы направлены на оказание поддержки эффективному государственному управлению посредством обеспечения того, чтобы коммерческие участники действовали в рамках принципа верховенства закона и соблюдали права человека. Действуя совместно, группы различных заинтересованных сторон могут разрабатывать более эффективные подходы и решения, чем те, которые могут получиться в результате работы только одной группы заинтересованных сторон.

A. Многостороннее сотрудничество

Ключевая роль государственных учреждений в многостороннем сотрудничестве

Государства несут основную ответственность за борьбу с насильственным экстремизмом и терроризмом. Как

---

[67] Mark Zuckerberg, Building Global Community, 16 February 2017.

[68] См. https://vk.com/about

[69] См. https://www.google.com/about/

[70] См. https://www.tencent.com/en-us/abouttencent.html

[71] Danish Institute for Human Rights, Submission to Special Rapporteur on Freedom of Expression, 28 January 2016 [Институт Дании по правам человека, Документы, представленные Специальному докладчику по вопросу о праве на свободу мнений и их свободное выражение, 28 января 2016 г.]

указано в разделе 1, законодатели и лица, ответственные за разработку политики, несут ответственность за разработку соответствующих норм в соответствии с обязательствами государства в рамках международного права, а также согласно своего национального законодательства. Государства вовлекают в эту работу ИКТ компании, чтобы обеспечить соответствие практики совместного регулирования и саморегулирования международному праву в области прав человека и национальному законодательству.

Помимо такого подхода, который основан только на законодательных мерах, государства также могут играть важную роль в координации и работе с отраслью ИКТ и гражданским обществом, создавая и поддерживая площадки для сотрудничества. Они имеют особое значение для национальных учреждений, занимающихся вопросами контроля и поиска террористического контента в Интернете, сигнализируют о нем и направляют запросы о его удалении посредством процедур обращения в ИКТ компании. Площадки для сотрудничества могут внести ценный вклад в работу государств и способствовать внедрению более инклюзивного процесса принятия решений в отношении мер реагирования по контенту. Открытые каналы коммуникаций между соответствующими заинтересованными сторонами также помогают выявлять и заполнять критические пробелы для обеспечения эффективности мер по предупреждению насильственного экстремизма и терроризма в сети Интернет и борьбы с ними, а также сглаживать возможные конфликты интересов. Кроме того, институционализированные и скоординированные усилия могут способствовать принятию дополнительных мер различными заинтересованными сторонами, а также эффективному распределению кадровых и финансовых ресурсов между ними.

Практический пример: Подразделения по контролю интернет-пространства на уровне ЕС и на национальном уровне

Подразделение по контролю интернет-пространства (IRU) Европейского союза (ЕС) является подразделением Европейского контртеррористического центра Европола и состоит из команды экспертов в области борьбы с терроризмом мотивированного религией, языковедения, аппаратно-программных разработчиков, а также представителей правоохранительных органов, специализирующихся в сфере борьбы с терроризмом.[72] Подразделение начало свою работу в 2015 году и обладает следующими полномочиями:

- оказывать поддержку компетентным органам ЕС посредством проведения стратегического и оперативного анализа;
- отмечать контент, пропагандирующий терроризм и насильственный экстремизм, и сообщать о нем соответствующим партнерам;
- выявлять интернет-контент, используемый сетями торговцев людьми для привлечения мигрантов и беженцев, и требовать его удаления;
- оперативно осуществлять и поддерживать процедуру обращения по поводу контента в тестом сотрудничестве с представителями отрасли.[73]

IRU занимается оценкой интернет-контента и направлением запросов по удалению незаконного контента в адрес соответствующих ИКТ компаний. Согласно докладу об обеспечении прозрачности IRU ЕС, представленному в 2017 году, «сотрудничество с частным сектором является основополагающим элементом профилактической деятельности».[74] С момента создания этого подразделения в июле 2015 года и до декабря 2017 года IRU ЕС провела оценку 46 392 документов, в результате которых было принято 44 807 решений о

[72] См. https://www.europol.europa.eu/about-europol/eu-internet-referal-unit-eu-iru

[73] Там же

[74] EU Internet Referral Unit, *Transparency Report 2017* [Подразделение по контролю интернет-пространства ЕС, *Доклад об обеспечении прозрачности, 2017 г.*]

направлении запросов об удалении; и доля удаления контента на основании этих обращений составила 92 %.[75] Директива ЕС о противодействии терроризму предусматривает гарантии в отношении удаления контента, которые описаны в статье 21(3): *«Меры по удалению и блокировке должны быть приняты на основании полностью прозрачных процедур и должны предоставлять надлежащие гарантии, в частности, для обеспечения того, чтобы такие меры были действительно необходимы и пропорциональны, а также чтобы пользователи были проинформированы о причине принятия таких мер. Гарантии, связанные с удалением и блокировкой, должны также включать возможность судебного обжалования».*[76] В случае если оцениваемый контент нарушает требования, определенные полномочиями Европола, обращение по поводу такого контента направляется ИКТ компании, на чьей платформе он был обнаружен. Тем не менее, в конечном итоге, решение об удалении такого отмеченного контента остается на усмотрение компании, после проведения оценки с учетом ее соответствующих условий оказания услуг. У IRU ЕС отсутствуют законные полномочия требовать от компаний удаления контента.

Аналогичные подразделения по контролю существуют в Великобритании, Франции и Нидерландах, и в соответствии с отчетами Европола, аналогичные механизмы были созданы в Бельгии, Германии и Италии.[77]

Для содействия в координации совместной работы государств и ИКТ компаний IRU ЕС организует так называемые «дни контроля контента», собирая вместе представителей специализированных подразделений правоохранительных органов из различных национальных IRU, а также IRU ЕС и ИКТ компаний.[78]

Возрастающая степень использования подразделениями IRU обращений по удалению контента вызывает критику со сторону организаций гражданского общества, таких как Глобальная сетевая инициатива (GNI) в связи с тем, что такие обращения не сопровождаются предоставлением соответствующего доступа к средствам правовой защиты, обеспечением подотчетности или прозрачности для пользователей и широкой общественности.[79] GNI также опубликовала заявление о своей обеспокоенности тем фактом, что некоторые IRU могут сигнализировать о том, что контент, возможно, нарушает условия ИКТ компании, не указывая, нарушает ли такой контент национальное законодательство.[80]

Многостороннее сотрудничество: использование преимуществ соответствующих заинтересованных сторон

Многосторонний подход с большей вероятностью окажется эффективным и устойчивым в том случае, если вовлеченные в его реализацию заинтересованные стороны обладают общим пониманием своих соответствующих функций и обязанностей, а также знают свои преимущества и предел возможностей. Такой подход способен объединить политические, правовые, общественные и технические ноу-хау и опыт, необходимые для эффективного решения проблем, связанных с наличием и доступностью террористического контента в Интернете.

---

[75] Там же

[76] Там же

[77] Europol, *Referral Action Day*, 2018 [Европол, *День контроля контента*, 2018 г.]

[78] Europol, *EU Law Enforcement and Google Take on Terrorist Propaganda in Latest Europol Referral Action Days*, 16 July 2018 [Европол, *Правоохранительные органы ЕС и Google сражаются с террористической пропагандой в ходе последних дней контроля контента, организованных Европолом* 16 июля 2018 г.] Europol, *Referral Action Day*, 2018 [Европол, *День контроля контента*, 2018 г.]

[79] См. Global Network Initiative, *Extremist Content and the ICT Sector*, 2016, and Jason Pielemeier and Chris Sheehy, *Understanding the Human Rights Risks Associated with Internet Referral Units*, Global Network Initiative, 25 February 2019 [Глобальная сетевая инициатива, *Экстремистский контент и сектор ИКТ*, 2016 г., и Джейсон Пилемейер и Крис Шихи, *Понимание рисков для прав человека, связанных с подразделениями по контролю интернет-пространства*, Глобальная сетевая инициатива, 25 февраля 2019 г.]

[80] Global Network Initiative, *Understanding the Human Rights Risks Associated with Internet Referral Units*. 25 February 2019 [Глобальная сетевая инициатива, *Понимание рисков для прав человека, связанных с подразделениями по контролю интернет-пространства*, 25 февраля 2019 г.]

Практический пример: программа «Наблюдатель YouTube»

В 2012 году YouTube разработала программу «Наблюдатель Youtube»,[81] которая предоставляет волонтерам-физическим лицам, государственным органам и неправительственным организациям, помогающим выявлять контент с нарушениями принципов сообщества YouTube, возможность доступа к инструментам, которые позволят им направлять жалобы на видеоматериалы с нарушениями более эффективно (программа «Наблюдатель» не предусматривает немедленного закрытия опубликовавшего контент с нарушением аккаунта, в соответствии с национальным законодательством). Как только YouTube получает жалобу об определенном контенте, специалисты Youtube, прошедшие специальное обучение, анализируют такой контент, чтобы определить, нужно ли удалить отмеченные видеоролики или нет. Поскольку ожидается, что наблюдатели будут направлять свои сигналы с высокой степенью точности, контент, о котором они сообщают, анализируется в приоритетном порядке. Кроме того, они получают доступ к инструменту, который позволяет отправлять жалобы сразу на несколько видео, в которых есть нарушения; просматривать окончательные решения о роликах, на которые отправлены жалобы; получать результат проверки своих жалоб в ускоренном порядке; обсуждать со специалистами YouTube особенности разных видов контента; изучать тематические онлайн-курсы (только для представителей некоммерческих организаций).

Как указано в отчете YouTube по обеспечению прозрачности, в период между январем и мартом 2019 года наблюдатели отметили наибольшее число из обнаруженных людьми видеороликов, которые были впоследствии удалены (всего удалено 1 396 945 видеороликов, по сравнению с 4022, о которых сообщили НПО и 16, о которых сообщили государственные органы), что составляет приблизительно одну шестую часть контента, который был удален автоматизированными методами обнаружения (в количестве 6 372 936 видеоматериалов).[82]

B. Дальнейшие инициативы

Инициативы отрасли ИКТ и гражданского общества

Платформы социальных сетей стали основным инструментом общества для доступа к информации, обмена информацией и ее обсуждения. ИКТ компании весьма часто сталкиваются с проблемами в рамках совместного и самостоятельного регулирования в отношении своих платформ, в особенности в том, что касается защиты прав человека, таких как свобода слова и право на неприкосновенность частной жизни. Ответом на это могут стать эффективные механизмы предупреждения распространения контента с пропагандой насильственного экстремизма и терроризма в сети Интернет и борьбы с ним — инициативы ИКТ отрасли, такие как обмен знаниями и технологиями между компаниями, создание платформ для интерактивных инструментов и ресурсов по модерированию контента, а также проведение со стороны крупных компаний курсов обучения для небольших компаний по вопросам подхода к удалению контента.

ИКТ компании могут рассмотреть возможность введения, на добровольной основе, своих собственных практик по борьбе с насильственным экстремизмом и терроризмом в Интернете, например, путем разработки кодексов поведения или этических правил, касающихся распространения изображений, видеороликов и другого рода визуальной информации, при этом такая практика также может быть отражена в договоре о предоставлении услуг. Это позволит повысить их собственный уровень осведомленности и ответственности, а также поможет дополнить национальное законодательство.

[81] См. https://support.google.com/youtube/answer/7554338?hl=en&ref_topic=2803138

[82] См. https://transparencyreport.google.com/youtube-policy/removals?hl=en

Практический пример: Глобальный интернет-форум по противодействию терроризму (GIFCT)

В 2017 году YouTube, Facebook, Microsoft и Twitter основали *Глобальный интернет-форум по противодействию терроризму* (GIFCT), миссия которого состоит в том, чтобы «существенно уменьшить возможности террористов по продвижению терроризма, распространению пропаганды насильственного экстремизма, а также использованию в своих целях или прославлению актов насилия посредством наших платформ».[83] В 2019 году к GIFCT присоединилась Dropbox.

Цель GIFCT состоит в обмене технологиями и инструментами, а также в проведении обучения для более малых компаний в области борьбы с террористическим контентом, что делается в партнерстве с аффилированной с ООН инициативой «Технологии против терроризма» (Tech Against Terrorism). Например, GIFCT создал базу данных, которая позволяет компаниям создавать «цифровые отпечатки пальцев» любого размещенного контента террористической направленности (так называемая «база данных по обмену хэшем»). В июне 2019 года эта база содержала уже свыше 200 000 образцов хэша.[84]

После принятия «Крайстчерчского призыва» по удалению террористических материалов в Интернете в мае 2019 года, GIFCT взял на себя обязательство сосредоточиться на реагировании на кризисные ситуации посредством «внедрения совместных протоколов работы с контентом на случай инцидентов для реагирования на происходящие события, такие как ужасная террористическая атака в Крайстчерче, чтобы обеспечить быстрый и эффективный обмен соответствующей информацией, ее обработку и принятие мер в отношении нее всеми компаниями-участницами».[85]

Фонд New America выразил сомнения относительно инициатив GIFCT по обмену знаниями; они не имеют возможности четко оценить и отслеживать свой успех, что может привести к вытеснению из сферы разработки инновационной практики небольших компаний, которые способны работать более эффективно. Поскольку участники GIFCT по сути создают передовую практику, которой они обмениваются с более малыми платформами без проведения тщательной стратегической оценки, деятельность таких платформ по разработке и внедрению новых и инновационных стратегий является ограниченной.[86]

Практический пример: «Технологии против терроризма» (Tech Against Terrorism)

«Технологии против терроризма» — это инициатива, санкционированная ООН, и государственно-частное партнерство.[87] В рамках этой инициативы, начиная с 2016 года, осуществляется мониторинг использования террористами Интернета, и его результаты показывают, что среди 50 наиболее активно используемых террористическими и насильственными экстремистскими группировками платформ более половины составляют небольшие платформы и микроплатформы. Инициатива «Технологии против терроризма» направлена, в частности, на работу с малыми компаниями, у которых зачастую не имеется финансовых, кадровых и технических ресурсов для эффективного предупреждения неправомерного использования их платформ для целей насильственного экстремизма и терроризма и противодействия таковым.

Компании, которые присоединяются к инициативе «Технологии против терроризма», соглашаются с обязательствами в рамках данной инициативы,[88] которые содержат шесть простых и понятных руководящих

[83] См. https://www.gifct.org/about/

[84] Там же

[85] См. Facebook, *Global Internet Forum To Counter Terrorism: An Update on Our Progress Two Years on*. 24 July 2019, и Microsoft, *The Christchurch Call and Steps to Tackle Terrorist and Violent Extremist Content*, 15 May 2019.

[86] Spandana Singh, *Taking Down Terrorism: Strategies for Evaluating the Moderation and Removal of Extremist Contents and Accounts*. New America.

[87] См. https://www.techagainstterrorism.org/

[88] Tech Against Terrorism, *The Pledge for Smaller Tech Companies*. См. http://88.208.218.79/gns/home.aspx

принципов передовой практики: уважение свободы выражения мнения, уважение права пользователей выражать различные взгляды и мнения; защита права пользователей на неприкосновенность частной жизни; обеспечение прозрачности в части касающейся процедуры удаления контента; определение того, какой контент является допустимым, наряду с предоставлением доступа к механизмам обжалования; и желанием дальнейшего сотрудничества. Цель этих обязательств — стать «исходной точкой, при помощи которой компании смогут выстроить собственные соответствующие системы и политику ». Они основываются на инструментах международного права, таких как принципы Глобальной сетевой инициативы.

В целях оказания поддержки небольшим компаниям в рамках инициативы «Технологии против терроризма» в 2017 году была запущена Платформа обмена знаниями, на которой небольшие ИКТ компании могут получить доступ к специальным инструментам и инструментариям, таким как образец договора на предоставление услуг и типовое руководство по составлению отчетов в целях обеспечения прозрачности. Эта платформа снабдит их инструментами, необходимыми для более эффективного предупреждения использования террористами и насильственными экстремистами их сервисов и борьбы с такого рода использованием.

Практический пример: INHOPE — практический опыт регулирования контента с пропагандой насильственного экстремизма и терроризма в Интернете

Международная ассоциация «горячих линий» сети Интернет работает в 43 странах по всему миру и стремится внести свой вклад в обеспечение того, чтобы Интернет был «свободен от сексуального насилия над детьми и их сексуальной эксплуатации».[89] Миссия ассоциации — «укрепить международные усилия по борьбе с материалами, содержащими сцены сексуального насилия над детьми».[90] INHOPE сотрудничает с различными заинтересованными сторонами, включая Интерпол, Европол, Twitter, Crisp Thinking, Microsoft, Google, Facebook и Trend MICRO.

В состав INHOPE входят 48 «горячих линий», которые предоставляют широкой общественности механизм для сообщения о контенте или деятельности в Интернете, которые потенциально являются незаконными. Основное внимание INHOPE уделяет материалам, содержащим сцены сексуального насилия над детьми, но также в сферу деятельности ассоциации входят разжигающие ненависть высказывания и ксенофобский интернет-контент. Несмотря на то, что INHOPE дает определение термину «разжигающие ненависть высказывания», ассоциация признает, что это чрезвычайно сложный вопрос, который зачастую не предусматривает ответственности в соответствии с уголовным правом. В связи с этим каждое сообщение о ненавистнических высказываниях, поступающее на «горячую линию», оценивается в соответствии с национальным законодательством, т.е. по месту размещения соответствующего контента.[91]

Еще один урок, извлеченный из деятельности INHOPE — это важность хорошего самочувствия сотрудников, а именно модераторов контента, а также признание того, что проверка контента на предмет наличия контента с пропагандой насильственного экстремизма и терроризма оказывает серьезное психологическое давление на лиц, проводящих такую проверку. Официальный документ, разработанный и опубликованный французской «горячей линией» Point de Contact, направлен на разработку общего набора примеров передовой практики в области операционной обработки вредного и потенциально незаконного контента, который может поставить под угрозу физическую безопасность и психологическое самочувствие специалистов по проверке контента.[92]

[89] См. http://88.208.218.79/gns/home.aspx

[90] См. http://88.208.218.79/gns/who-we-are/our-mission.aspx

[91] См. http://88.208.218.79/gns/internet-concerns/overview-of-the-problem/hate-speech.aspx

[92] Point de Contact of the Guide d'Usage pour la Lutte contre la Pédopornographie, *Child sexual abuse material and online terrorist propaganda Tackling illegal content and ensuring staff welfare*, 2014

Меры реагирования на основе коммуникаций:

4. Разработка, принятие и оценка системы мер

Данный раздел предназначен для лиц, ответственных за разработку политики, и практикующих специалистов и содержит практические примеры передовой практики в области разработки, принятия и оценки действенных систем мер и программ, касающихся мер реагирования на основе коммуникаций, являющихся частью соответствующих стратегий и национальных планов действий. Раздел состоит из трёх подразделов: «Разработка системы мер», «Мониторинг и оценка» и «Этические риски и риски с точки зрения безопасности».

Соответствующие примеры передовой практики из Цюрихско-Лондонских рекомендаций:

Передовая практика 1. *Принятие и внедрение законодательной базы и политических механизмов на национальном уровне в целях предупреждения насильственного экстремизма и терроризма в сети Интернет и борьбы с ними.*

Передовая практика 2. *Обеспечение всестороннего понимания существующих и потенциальных онлайн-угроз, исходящих от насильственного экстремизма и терроризма в рамках каждого национального и местного контекста.*

Передовая практика 3. *Выработка четкой стратегии борьбы с насильственным экстремизмом и терроризмом в сети Интернет на основе подхода, объединяющего вовлечение соответствующих государственных учреждений и всего общества, координирующего меры реагирования как на основе контента, так и на основе коммуникаций, а также оффлайн-мероприятия, включая обучение и привлечение организаций гражданского общества в соответствующих случаях.*

Передовая практика 4. *Разработка, в сотрудничестве с другими заинтересованными сторонами, общей системы мониторинга и оценки, способствующей повышению прозрачности и более глубокому пониманию воздействия мер реагирования.*

Передовая практика 5. *Укрепление международного сотрудничества в качестве ключевого компонента для эффективного предупреждения насильственного экстремизма и терроризма в сети Интернет и борьбы с ними.*

Передовая практика 16. *Обеспечение сосредоточенности всех кампаний на общей цели, которая может быть простой, как, например, содействие диалогу и участию; на реалистичном пакете измеримых целей;*

на надежной методологии оценки воздействия, оказываемого на целевую аудиторию.

Передовая практика 17. *Понимание и принятие мер для уменьшения возможных рисков, связанных со стратегией и проведением коммуникационных кампаний.*

ВВЕДЕНИЕ

Политика профилактики на основе коммуникаций должна быть сбалансирована с учетом мер реагирования на основе контента в рамках всестороннего подхода к предупреждению насильственного экстремизма и терроризма и борьбе с ними — как в Интернете, так и в реальной жизни — и должна принимать во внимание основополагающие внутренние и внешние движущие силы насильственного экстремизма, ведущего к терроризму.[93] В соответствии с Резолюцией Совета Безопасности ООН 2354 по борьбе с пропагандой терроризма, любая политика, разрабатываемая и принимаемая в целях противодействия терроризму и насильственному экстремизму, должна соответствовать международным правовым обязательствам государств, включая международное право в области прав человека, а также соблюдать принцип верховенства закона и право на неприкосновенность частной жизни и на свободу выражения мнения, объединений, мирных собраний, вероисповедания и убеждений.[94]

Разработка и принятие четких правовых или официальных определений основных терминов, таких как «насильственный экстремизм» и «терроризм» («противодействие насильственном экстремизму и терроризму») в национальном законодательстве, стратегии или плане действий будут способствовать повышению эффективности реализации стратегии мер по коммуникации.[95] Определения могут сыграть важную роль при формировании понимания государствами проблемы, эффективно разграничить и адресно сфокусировать меры реагирования, а также помочь в достижении скоординированного подхода вовлеченных сторон в решении проблем. Чрезвычайно важно, чтобы государства эффективно оповещали о своих намерениях и содержании своей политики в области предупреждения насильственного экстремизма и терроризма в сети Интернет и борьбы с ними. Меры реагирования на основе коммуникаций в Интернете должны дополнять аналогичные меры, предпринимаемые в реальной «оффлайн» жизни; в противном случае существует опасность того, что доверие как к самим государствам, так и к их политике будет подорвано.

A. Разработка системы мер

Борьба со всеми формами насильственного экстремизма и терроризма

Система мер реагирования на основе коммуникаций должна быть направлена на предупреждение и борьбу с насильственным экстремизмом и терроризмом во всех их проявлениях и должна подчеркивать, что насильственный экстремизм и терроризм не имеют связи с какой-либо религией, убеждениями и не имеют этнической принадлежности или гражданства. Группировки насильственных экстремистов и террористов

[93] UN Global Counter-Terrorism Strategy Review (A/RES/70/291), para 39, 19 July 2016 [Обзор Глобальной контртеррористической стратегии ООН (A/RES/70/291), пункт 39, 19 июля 2016 г.]

[94] UN Security Council Resolution 2354 (2017) [Резолюция Совета Безопасности ООН 2354 (2017 г.)]

[95] Без ограничения прочих определений или терминов из других источников, в том числе из национального законодательства, общепризнанным ориентиром для определения термина «террористические акты»» можно считать определение, представленное в Резолюции Совета Безопасности ООН 1566 (2004 г.), п. 3: «[...] преступные акты, в том числе против гражданских лиц, совершаемые с намерением причинить смерть или серьезный ущерб здоровью или захватить заложников с целью вызвать состояние ужаса у широкой общественности, или группы людей, или отдельных лиц, запугать население или заставить правительство или международную организацию совершить какое-либо действие или воздержаться от его совершения и представляющие собой преступления по смыслу международных конвенций и протоколов, касающихся терроризма, и в соответствии с содержащимися в них определениями, ни при каких обстоятельствах не могут быть оправданы никакими соображениями политического, философского, идеологического, расового, этнического, религиозного или другого подобного характера [...]».

используют целый спектр различных тактик и видов контента для различных аудиторий, включая широкую общественность, находящиеся в группе риска и уязвимые аудитории, а также преданных сторонников. Кроме того, группировки насильственных экстремистов и террористов все чаще разрабатывают специализированный контент для радикализации и вербовки, а также стратегии вовлечения, направленные на женщин и девочек. Соответственно, всесторонние меры реагирования на основе коммуникаций должны принимать во внимание этот фактор, а стратегии и политика должны разрабатываться с учетом предупреждения таких тактик и противодействия им.

Чтобы полностью охватить весь спектр контента с пропагандой насильственного экстремизма и терроризма в Интернете, требуется использовать различные меры реагирования на основе коммуникаций. Для целей настоящего инструментария, меры реагирования на основе коммуникаций можно разделить на две широкие категории: «восходящие» и «нисходящие» методы (см. также раздел 5, рис. 1).

➔ **«Восходящие» методы** являются упреждающими и направлены на широкую аудиторию. Их цель состоит в формировании устойчивости к пропаганде насильственного экстремизма и терроризма, в повышении осведомленности общественности о политике государства и оказываемых им услугах поддержки, или в опровержении дезинформации посредством повышения осведомленности и образовательных подходов, либо распространения положительных или альтернативных идей.

➔ **«Нисходящие» методы,** напротив, сфокусированы на опровержении, доказательстве ложности аргументов в пропагандистских материалах, распространяемых группировками насильственных экстремистов или террористов, или попыток обоснования террористических актов, подстрекательства к таковым или прославления («*оправдания*») таковых, а также на борьбу с такими действиями. Такие методы предназначены для конкретных аудиторий, включая уже радикализированных лиц, лиц, симпатизирующих пропаганде насильственного экстремизма или терроризма, или лиц, которые считаются особенно уязвимыми или подверженными риску радикализации или вербовки. Нисходящие методы включают контрпропагандистские кампании, направленные на более конкретные аудитории, подверженные риску, а также персонализированные онлайн-мероприятия в отношении лиц, состоящих в насильственных экстремистских и террористических сообществах в Интернете.

Подход, основанный на участии всего общества

Разработка системы мер реагирования на основе коммуникаций должна быть направлена на ограничение воздействия коммуникаций со стороны насильственных экстремистов и террористов, а также на работу по устранению лежащих в основе внутренних и внешних движущих сил насильственного экстремизма и терроризма. В этой связи предупреждение насильственного экстремизма и терроризма и борьба с ними посредством мер реагирования на основе коммуникаций не должны считаться чисто вопросом безопасности, а, напротив, рассматриваться как многоаспектная проблема, для решения которой требуется междисциплинарный, мультиинституциональный подход, основанный на участии всего общества. Государства должны играть ведущую роль в поддержке подхода, основанного на участии всего общества. Соответственно, их политика и стратегии должны поощрять соответствующие заинтересованные стороны, включая ИКТ компании и организации гражданского общества в соответствующих случаях, к координации и сотрудничеству в области реализации методов на основе коммуникаций.

Такие методы должны разрабатываться и утверждаться в соответствии с более масштабными национальными стратегиями и политическими механизмами, направленными на предупреждение насильственного экстремизма и терроризма и борьбу с ними, чтобы обеспечить согласованности мероприятий, проводимых онлайн и оффлайн. Оффлайн-мероприятия могут включать инициативы по формированию критического мышления, цифровой грамотности и устойчивости посредством повышения осведомленности и обучения широкой общественности, вовлечения рядовых членов сообщества, а также иные методы, направленные на устранение внутренних и внешних движущих сил, которые могут привести к тому, что отдельные лица начнут поддерживать насильственный экстремизм и терроризм.

Исследователи, учетные и практикующие специалисты также могут представить свое видение по вопросу коммуникаций со стороны насильственных экстремистов и террористов, которое ляжет в основу потенциальных мер реагирования. Успешные методы основываются на опыте, полученном в широком спектре взаимосвязанных секторов и областей, включая, помимо прочего, технологии, маркетинг, рекламу, производство контента, исследования в области коммуникаций, психологию, социологию, политологию, образование и государственную политику. Помимо профессионального опыта, также следует учитывать взгляды и ценности основных целевых аудиторий; кроме того, при наличии возможности, к разработке и реализации мер реагирования следует привлекать конкретные аудитории (например, молодежь, женщин).

Государствам следует рассмотреть возможность повышения эффективности и действенности всесторонних подходов к предупреждению насильственного экстремизма и терроризма в сети Интернет и борьбе с ними посредством создания национального органа межведомственной координации для организации работы и интеграции онлайн- и оффлайн-инициатив и программ в рамках подхода, основанного на вовлечении соответствующих государственных учреждений, совершенствования стратегий и политики, а также обмена результатами исследований, мониторинга и оценки.

Практический пример: Канадский центр по взаимодействию с общественностью и предотвращению насилия[96]

Канадский центр был основан в 2017 году и несет ответственность за реализацию инициатив Государства Канады в области противодействия переходу от радикализации к насилию. В обязанности Центра входит разработка соответствующей системы мер, содействие многостороннему сотрудничеству и координации, разработка целевых программ и финансирование, планирование и координация исследований. Центр уделяет особое внимание содействию в работе, проводимой с сообществом, включая создание Национального экспертного комитета для содействия в разработке соответствующей системы мер. Фонд по формированию устойчивости сообщества Канадского центра оказывает поддержку в проведении профилактической работы и на сегодняшний день профинансировал двадцать четыре проекта на общую сумму свыше 16 миллионов канадских долларов.[97]

В 2018 году Канадский центр разработал Национальную стратегию по противодействию переходу от радикализации к насилию, в которой обозначены три приоритета государства в области предупреждения радикализации и противодействию таковой:

1. формирование, обмен и использование знаний;
2. противодействие переходу от радикализации к насилию, происходящей в результате воздействия Интернета;
3. соответствующие вспомогательные мероприятия.

Стратегия предусматривает четкие и подробные определения понятий радикализации, перехода от радикализации к насилию и насильственного экстремизма, признавая, что этот процесс подвергается воздействию множества факторов, включая подверженность пропаганде терроризма или насильственного экстремизма как в Интернете, так и в реальной жизни. В *Национальной стратегии* четко изложено обязательство Государства Канады обеспечить «защиту прав человека и основных свобод, включая права на свободу выражения мнения и неприкосновенность частной жизни, находящиеся под защитой Устава ООН», а также обеспечить «многообразие и политическое участие для всех канадцев».[98]

Национальная стратегия предусматривает проведение работы по предупреждению радикализации и

[96] См. https://www.publicsafety.gc.ca/cnt/bt/cc/index-en.aspx.

[97] См. https://www.canada.ca/en/public-safety-canada/news/2018/12/launch-of-national-strategy-on-countering-radicalization-to-violence-and-update-on-terrorist-threat-to-canada-terrorism-threat-level-unchanged.html.

[98] См. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-strtg-cntrng-rdclztn-vlnc/index-en.aspx.

противодействию таковой, которые разделены на три потока, направленные на каждый из этапов процесса радикализации, начиная с ранней профилактики до мероприятий по предупреждению в группах риска и освобождению от влияния. Радикализации в сети Интернет придается особое значение как одному из трех ключевых приоритетов; при этом подчеркивается необходимость способствовать развитию коммуникаций между государством, гражданским обществом, технологическими компаниями и международными участниками, а также оказанию поддержки исследованиям в целях формирования доказательной базы в отношении того, каким образом группировки насильственных экстремистов и террористов могут действовать в Интернете.

Фонд по формированию устойчивости сообщества имеет целью оказание поддержки инициативам гражданского общества, которые способствуют повышению цифровой грамотности и распространению альтернативной идеологии, и предоставил финансирование нескольким программам, включая следующие:

- *Canada Redirect («Перенаправление в Канаде»* (компания Moonshot CVE) — направление уязвимым лицам, которые активно ищут в Интернете насильственные экстремистские материалы, положительный, альтернативный контент посредством онлайн-рекламы и видеоконтента;
- *Pushing Back Against Hate in Online Communities («Противодействие ненависти в интернет-сообществах»)* (компания Media Smarts) — исследование уровня понимания разжигания ненависти и радикализации в Интернете среди учеников средних школ, чтобы проинформировать об этом школы и родителей в целях принятия мер;
- Мультимедиа-портал *SOMEONE («Обучение в социальных сетях каждый день»)* (Университет Конкордия) — формирование устойчивости к разжиганию ненависти и радикализации, ведущей к насилию, у молодых людей посредством серии основанных на фактах ресурсов для преподавателей, СМИ, государства и широкой общественности в целях совершенствования мер реагирования на эти проблемы на различных уровнях образования, от начального до высшего.[99]

Практический пример: Руководящие принципы национальной системы мер по противодействию экстремизму — Национальный антитеррористический орган (NATCA) Пакистана

Подход, объединяющий вовлечение соответствующих государственных учреждений и всего общества

Руководящие принципы национальной системы мер по противодействию экстремизму (NCEPG), разработанные правительством Пакистана, стали результатом проведения 34 раундов различных встреч с участием 305 заинтересованных сторон и основываются на подходе, предусматривающем вовлечение соответствующих государственных учреждений и всего общества.[100] В число заинтересованных сторон, с которыми были проведены консультации, вошли представители областных госучреждений, представители научного сообщества, СМИ, богословы и организации гражданского общества. В соответствии с Конституцией Республики Пакистан, все встречи проходили с вовлечением заинтересованных сторон, для обеспечения соблюдения прав человека, учета интересов меньшинств, маргинализованных сообществ и женщин.

В стратегии отмечается ключевая роль выживших жертв терроризма и бывших последователей насильственного экстремизма в борьбе с пропагандой насильственного экстремизма и терроризма, а ее цель состоит в поддержке создания платформы, на которой можно было бы собрать соответствующие истории этих выживших жертв и бывших последователей. В Руководящих принципах национальной системы мер признается проблема с нахождением «надежных и убедительных» посредников для донесения соответствующих установок, поэтому основное внимание для этих целей уделяется лицам, имеющим аналогичный с целевой

[99] См. https://www.publicsafety.gc.ca/cnt/bt/cc/fpd-en.aspx.

[100] National Counter Terrorism Authority – Pakistan, National Counter Extremism Policy Guidelines January 2018 [Национальный антитеррористический орган Пакистана, Национальные руководящие указания политики по противодействию экстремизму, январь 2018 г.]

аудиторией опыт.

Меры реагирования на основе коммуникаций как часть национальной стратегии

Руководящие принципы национальной системы мер признают важность привлечения онлайн- и оффлайн-СМИ не только как средств распространения информации, но и как активного инструмента для проведения работы по противодействию экстремизму на основе коммуникаций. Это включает использование СМИ, чтобы помочь придать историям жертв насильственного экстремизма человеческое лицо, а также помочь в развенчании информационной составляющей сути пропаганды насильственного экстремизма.

Руководящие принципы национальной системы мер также включают рекомендации в отношении создания медиа-группы по противодействию насильственному экстремизму со стороны Министерства информации и вещания в партнерстве с Национальным антитеррористическим органом в целях обеспечения «синхронизации предпринимаемых мер по реализации коммуникационной стратегии по предупреждению насильственного экстремизма в обществе». Данная группа предназначена для работы совместно с областными информационными департаментами с целью доведения до местного населения реализуемых в их регионе программ по противодействию насильственному экстремизму.

Примеры коммуникационных кампаний реализуемых в рамках NCEPG

PurAzm Pakistan — один из примеров программ, которые реализуются в рамках NCEPG. PurAzm представляет собой медиакампанию, в которой демонстрируются истории из повседневной жизни простых пакистанцев, а также полицейских, специалистов по борьбе с полиомиелитом, докторов и государственных должностных лиц, а ее цель состоит в том, чтобы распространить идею о том, что пакистанцы «отвергают идею зла насильственного экстремизма и сохраняют стойкость и надежду, несмотря на неблагоприятные последствия».[101]

Начиная с 2014 года, в рамках инициативы было снято 30 коротких фильмов. Программа PurAzm предусматривает вручение премии PurAzm, которая направлена на поддержание устойчивости программы посредством оказания помощи студентам вузов и молодым специалистам в создании «оригинального, самобытного аудиовизуального и текстового контента на темы Purazm Pakistan».

Роль СМИ

Комплексные коммуникационные стратегии и системы мер также могут учитывать потенциальную роль и воздействие СМИ в части «расширения диалога и углубления взаимопонимания», а также «в утверждении принципов терпимости и сосуществования, в содействии созданию обстановки, не способствующей подстрекательству к терроризму, и в противодействии распространению террористических идей».[102] Предпринимаемые со стороны государств меры не должны нарушать свободу, плюрализм или равенство точек зрения в СМИ. Подходы, используемые в этой области, не должны предусматривать стремления к регулированию СМИ, при этом любые попытки сотрудничества со СМИ должны происходить на добровольной или независимой основе. Государства также могут сыграть важную роль в поддержании многообразия источников и облегчении доступа к СМИ.[103]

В своей *Декларации о свободе выражения мнений и информации в СМИ в контексте борьбы с терроризмом* Совет Европы рекомендует журналистам и СМИ учитывать свою роль и не способствовать террористам достигать своих целей. Это включает отказ от непреднамеренного создания атмосферы страха того, что терроризм может разрастись, а также отказ от предоставления террористам платформы посредством непропорционального освещения их деятельности. Совет Европы рекомендует СМИ рассмотреть возможность принятия и введения в действие соответствующей передовой практики, если это еще не было сделано, или

[101] См. http://purazm.gov.pk/about/.

[102] UN Security Council Resolution 2354 (2017), preamble para. 13 [Резолюция Совета Безопасности ООН 2354, пункт преамбулы 13].

[103] Article 19, 'Hate Speech' Explained A Toolkit, 2015 [Статья 19, Разжигание ненависти: разъяснение инструментария, 2015 г.]

адаптировать существующие подходы с учетом потенциальных вопросов этики, возникающих при публикации СМИ сообщений, касающихся насильственного экстремизма и терроризма.[104] Одним из таких примеров является добровольное принятие СМИ в России кодекса поведения («*правила поведения СМИ в случаях террористического акта и контртеррористической операции*») в 2003 году.[105] Кодекс преимущественно сосредоточен на передовой практике поведения для СМИ в период, когда происходят террористические инциденты, во избежание негативного влияния на оперативную безопасность или создания дополнительного риска для жизни людей, но при этом подчеркивает важность права на свободу выражения мнения и предоставляет возможность публичного обсуждения таких вопросов, как терроризм. В качестве примера финансируемой государством программы, учитывающей возможную роль СМИ в борьбе с пропагандой насильственного экстремизма и терроризма, можно привести один из проектов в рамках текущей Программы обучения лидерству для иностранных кадров (IVLP) Государственного департамента США, который сосредоточен на следующем направлении: «Противодействие насильственному экстремизму — сообщения и стратегии СМИ». В рамках этого проекта проводилась работа с журналистами, экспертами и государственными чиновниками по всему миру, чтобы обозначить положительную роль и обязанности СМИ (как онлайн, так и печатных) в поддержании демократии, а также в предупреждении насильственного экстремизма и терроризма и борьбе с ними.[106] В ходе проекта также была изучена роль государств в соблюдении принципа верховенства закона и свободы прессы.

Международное сотрудничество является неотъемлемой частью работы по предупреждению насильственного экстремизма и терроризма в сети Интернет и борьбе с ними с учетом транснационального характера как самой угрозы, так и природы Интернета. Международное сотрудничество способствует наращиванию потенциала посредством обмена передовой практикой, которая позволяет обеспечить, чтобы национальные меры реагирования по ограничению влияния пропаганды насильственного экстремизма и терроризма, (как в Интернете, так и в реальной жизни), а также по распространению контрпропаганды были взаимодополняющими и устойчивыми.

Международные форумы могут помочь получить синергию в рамках международного сообщества для максимизации коллективных усилий и накопления опыта в области предупреждения насильственного экстремизма и терроризма в сети Интернет и борьбы с ними. Кроме того, такие форумы могут создать среду взаимного доверия, способствовать построению платформ для улучшенных коммуникаций, а также обеспечить эффективное и действенное использование ресурсов. В связи с этим Государствам рекомендуется наладить непрерывный обмен передовой практикой и информацией о национальных программах и принципах оценки, а также стремиться к формированию общих систем и показателей мониторинга и оценки для успешного выполнения поставленных задач (*см. B. Мониторинг и оценка мер реагирования на основе контента*).

Практический пример: Национальные практические семинары по противодействию использованию сети Интернет в террористических целях Организации по безопасности и сотрудничеству в Европе (ОБСЕ)[107]

В январе 2019 года Координатор проектов ОБСЕ в Узбекистане и Антитеррористическое подразделение ОБСЕ провели трехдневный национальный практический семинар (“Table Top Exercise” - TTX) по противодействию

---

[104] Ср. *Declaration on freedom of expression and information in the media in the context of the fight against terrorism*, adopted by the Committee of Ministers, 02 March 2005 [*Декларация о свободе выражения мнений и информации в СМИ в контексте борьбы с терроризмом*, принятая Комитетом министров 02 марта 2005 г.]

[105] Антитеррористическая конвенция (правила поведения СМИ в случаях террористического акта и контртеррористической операции), 11 апреля 2003 г

[106] Chiemelie Ezeobi, *Nigeria: Countering Violent Extremism*, allAfrica, 13 June 2018.

[107] См. https://polis.osce.org/national-tabletop-exercise-countering-use-internet-terrorist-purposes.

использованию сети Интернет в террористических целях на основе *Цюрихско-Лондонских рекомендаций* ГКТФ. Мероприятие основывалось на результатах предыдущих мероприятий, проведенных ОБСЕ ранее, и вовлекло в эту работу представителей гражданского общества, уделяя при этом особое внимание соблюдению прав человека и учету гендерных аспектов. Данный семинар был направлен на применение подхода, основанного на участии всего общества, и в нем приняли участие 45 представителей госсектора, правоохранительных органов, СМИ, научного сообщества, молодежных организаций и отрасли ИКТ.

Организаторы провели семинар с использованием интерактивного сценария, содержащего вымышленную историю, которая использует реалистичные примеры основанные на реально происходящих в мире событиях и возникающих угрозах безопасности, имеющих отношение к Центральной Азии. В ходе мероприятия международные эксперты и представители ОБСЕ сделали ряд презентаций по соответствующим передовым практикам для содействия обсуждениям между участниками. Мероприятие охватило различные аспекты (меры реагирования, профилактика, выработка системы мер), и было направлено на выработку самими национальными участниками реально исполнимых в данном контексте конкретных мер, на основе специально разработанных инструкций для модераторов мероприятия, которые обеспечивали проведение обсуждение в соответствующем ключе для получения реально достижимых результатов.

Четкие цели:

Мероприятие было направлено на разработку документа «*Практические меры по повышению эффективности системы мер*» *(APRP)* и национального плана действий в целях повышения эффективности работы по устранению угроз, создаваемых использованием Интернета в террористических целях. В APRP приводится последовательный краткий обзор тем и вопросов, которые обсуждались в ходе мероприятия, а также изложены четкие «практические меры по повышению эффективности системы мер». Основополагающие цели мероприятия состояли в том, чтобы продемонстрировать участникам потенциальные пути взаимодействия и сотрудничества между заинтересованными сторонами, а также обеспечить соответствие реализуемых на практике мер международному законодательству и обязательствам, в частности в сфере обеспечения прав человека.

Подход, основанный на участии всего общества:

Данное мероприятие было разработано для продвижения подхода, основанного на участии всего общества, с включением в работу госорганов Узбекистана, представителей гражданского общества и отрасли ИКТ, а также международных экспертов. Успешное проведение мероприятия стало возможным в результате обеспечения структурированного общения между различными участниками, и выбранного для этого формата мероприятия, при котором удалось обеспечить взаимопонимание. Модераторы обсуждений имели заранее подготовленный список «наводящих вопросов» и ключевых тем для обсуждения. Такая структура позволила не только обеспечить успешный диалог, но и дать возможность участникам предложить необходимые ответные меры для решения существующих проблем. Например, изначально в тематику мероприятия не планировалось включать меры реагирования на основе коммуникаций, однако, когда стало очевидно, что есть определенная потребность по разъяснению таких методов как «контр и альтернативные нарративы», организаторы учли это в соответствующих рекомендациях APRR, которые стали основным документом, определяющим будущие сферы и направления работы по данной проблематике в местных условиях.

Постоянные и эффективные коммуникации также являются важным компонентом трех разделов, включенных в APRR, при этом во втором и третьем разделах четко определяются термины «сотрудничество» и «стратегические коммуникации» соответственно. Что касается правовых вопросов (первый раздел APRR), выводы по результатам обсуждения указывают на то, что национальное и международное законодательство, касающееся использования насильственными экстремистами и террористами Интернета «должно быть достаточно подробным» для того, чтобы снабдить население необходимой информацией и помочь гражданам защититься от произвольного или незаконного вмешательства в их частную жизнь. Аналогичным образом, за

счет привлечения участников из числа СМИ, организаторы обеспечили включение в APRP предложений по будущему обучению журналистов в области «эффективного освещения со стороны СМИ террористических угрозы и атак».

Практическая направленность:

Разработка APRP и национального плана действий обеспечивает постоянное сотрудничество между гражданским обществом, государством и отраслью ИКТ посредством определения стратегических целей и будущих проектов, предусматривающих участие представителей каждой из этих групп. В ARPR рассматриваются три основные направления: нормативно-правовая база по преступлениям, связанным с использованием Интернета насильственными экстремистами и террористами; государственно-частное партнерство и сотрудничество с международными ИКТ компаниями; стратегические коммуникации, СМИ, образование и исследования. Рекомендации по каждой теме включают сроки, общие сведения об участниках, ответственных за реализацию, а также перечень измеримых показателей для оценки их эффективности.

Прозрачность и признание рисков:

При проведении семинара особое внимание было обращено на вопросы, связанные с обеспечением прав человека, и при разработке рекомендаций по выработке системы мер были учтены соответствующие риски, связанные с противодействием использованию Интернета насильственными экстремистами и террористами. Модераторы соответствующих сессий мероприятия разъяснили участникам, каким образом плохо организованные кампании могут, помимо прочего, увеличить риск радикализации или непреднамеренно влиять на однобокое или ограничительное толкование религиозных аспектов.

Учитывая техническую сложность сети Интернет, а также ее постоянную и быструю эволюцию, национальные стратегии и соответствующие системы мер должны разрабатываться с четким пониманием как возможностей, предоставляемых мерам реагирования на основе коммуникаций онлайн, так и уязвимостей, которые могут быть использованы насильственными экстремистами и террористами. В связи с этим государствам следует обеспечить, чтобы политика и стратегии разрабатывались с учетом гибкости, на основе результатов последних исследований, а также предусмотреть их оценку, пересмотр и итерационное обновление на непрерывной основе, чтобы не отставать от изменений в интернет-пространстве и цифровой тактики, применяемой насильственными экстремистами и террористами.

Национальные планы действий или стратегии могут обновляться ежегодно, при этом тенденции в сети Интернет зачастую меняются быстрее. Анализ тенденций в соответствующих интернет-аудиториях, платформах и популярном контенте, а также понимание инфраструктуры и архитектуры Интернета (например, онлайн «эхо-камеры» и алгоритмические «пузыри фильтров»), на базе которых разрабатывается система мер на основе коммуникаций, также подлежат регулярному пересмотру и итерационному обновлению, чтобы обеспечить сохранение эффективности указанной системы мер.[108]

Насильственные экстремисты и террористы, использующие Интернет-общение для радикализации и вербовки отдельных лиц, а также для внесения раскола в сообщества, как правило, легко адаптируются и быстро начинают использовать изменения в интернет-пространстве и культурной среде в своих интересах. В этой связи государствам также следует инвестировать в исследования и аналитические инструменты для обеспечения всестороннего понимания изменяющихся намерений и воздействий средств общения насильственных экстремистов и террористов в Интернете и в реальной жизни, а также более масштабных

[108] Онлайн «эхо-камеры» описывают явление, когда люди подвергаются влиянию согласующихся идей и мнений в ущерб альтернативным или особым взглядам. «Пузыри фильтров» с большой вероятностью возникают в тех случаях, когда поисковые системы или социальные сети персонализируют результаты поиска или содержание новостной ленты посредством моделей и алгоритмов машинного обучения, которые рекомендуют контент, исходя из местонахождения соответствующих лиц, демографической информации или их прошлого поведения в сети Интернет, который в этой связи с большей вероятностью будет положительно воспринят

онлайн-тенденций с точки зрения соответствующих аудиторий, платформ и влиятельных лиц.

B. Мониторинг и оценка

Оценка воздействия должна являться центральным элементом всех подходов к коммуникациям, принимаемых в целях борьбы с коммуникациями насильственных экстремистов и террористов в Интернете. Механизмы, посредством которых государства могут оценить последствия своих коммуникаций, будь то положительные или отрицательные, имеют определяющее значение при разработке любых методов коммуникаций, а также конкретных кампаний. Такой подход к мониторингу и оценке позволит улучшить понимание долгосрочного воздействия мер реагирования на основе коммуникаций, а также даст возможность вносить поправки в меры, предпринимаемые в будущем, как на национальном, так и на международном уровнях.

Постоянное и долгосрочное финансирование расходов по проведению мониторинга и оценки, в том числе, в соответствующих случаях, посредством сотрудничества с отраслью ИКТ, научным сообществом и гражданским обществом, позволяют обеспечить ресурсы, которые должны быть эффективно распределены между наиболее действенными программами. Всесторонняя интегрированная и непрерывная оценка воздействия также способствует повышению прозрачности и подотчености, помогая определять как запланированные, так и незапланированные результаты применения мер реагирования.

Системы мониторинга и оценки

Учитывая сложность и широкий спектр потенциального воздействия мер реагирования на основе коммуникаций, государствам следует разработать общую систему всестороннего мониторинга и оценки, которая предусматривает четкие показатели по различным используемым ею методам. Демонстрация воздействия имеет определяющее значение с точки зрения обеспечения правомерности и эффективности мероприятий, предпринимаемых для предупреждения насильственного экстремизма и терроризма в сети Интернет и борьбы с ними.

Системы мониторинга и оценки также должны разрабатываться с учетом возможности отслеживать и фиксировать воздействие принимаемых мер реагирования на определенные аудитории, чтобы обеспечить их недискриминационный характер, так же как и для достижения запланированных результатов по отношению к целевой аудитории. С учетом того, что основанные на коммуникациях меры реагирования на проявления насильственного экстремизма и терроризма в сети Интернет пока остаются развивающейся сферой деятельности, государствам рекомендуется использовать опыт применения систем мониторинга и оценки, существующих в других секторах, в том числе в сфере здравоохранения, а также коммерческой рекламы и маркетинга в соответствующих случаях.

Теории изменений, цели и задачи

Политика государства должна быть основана на четко определенной теории изменений, которая объясняет, как и почему те или иные используемые меры реагирования на основе коммуникаций способствуют достижению целей и решению задач более общего Национального плана или стратегии. Теория изменений должна являться неотъемлемой частью разработки и реализации любых мер реагирования на основе коммуникаций и создавать структуру для проведения оценки их воздействия.

Начиная с желаемого воздействия на поведение и отношение запланированной целевой аудитории, теория изменений должна определять шаги, которые требуется предпринять для того, чтобы меры реагирования на основе коммуникаций привели к желаемым результатам и воздействиям, а также порядок оценки таковых. В основе эффективной и реалистичной теории изменений лежат четко определенные основные концепции. Требуется устранить любое отклонение в части понимания определений чтобы обеспечить необходимое участие основных заинтересованных сторон и точно оценить воздействие.

До начала этапов разработки и распространения в рамках кампании следует установить общую долгосрочную цель и серию связанных с ней непосредственных задач. В результате будет составлен набор базисных показателей, по сравнению с которыми будет производиться оценка воздействия на запланированную целевую аудиторию. Задачи должны быть поставлены в форме четко определенных количественно измеримых показателей желаемого результата. Они должны поддаваться оценке, чтобы предоставить возможность сравнить достигнутый ими успех с имеющимися показателями, и реалистичными, с учетом имеющихся ресурсов и выполнения соответствующих работ в прошлом.

Так называемые «призывы к действию», когда в рамках кампании целевую аудиторию просят предпринять конкретные действия в ответ, могут быть эффективным способом мобилизации поддержки, поощрения и укрепления изменений в отношении и поведении, а также значимым показателем для помощи в оценке воздействия. Призывы к действию также могут стать эффективными средствами мобилизации поддержки — как в Интернете, так и в реальной жизни — и не допустить того, чтобы коммуникационные кампании рассматривались целевыми аудиториями как поверхностные или недостаточно глубокие. Такие методы необходимо поддерживать в действии во избежание того, что первоначальный энтузиазм со временем угаснет, и участники станут относиться к ценностям кампании скептически, что сократит возможности для будущей мобилизации.

Практический пример: Центр глобального взаимодействия, Государственный департамент США

Центр глобального взаимодействия (GEC) отвечает за работу в области борьбы с коммуникациями со стороны международных террористических организаций и иностранных государств в США. GEC был создан решением государственного секретаря в 2016 году, а его миссия состоит в том, чтобы осуществлять «руководство, синхронизацию и координацию усилий Федерального государства в области распознавания, понимания, выявления пропаганды и дезинформации из государственных и негосударственных зарубежных источников, направленной на подрыв интересов государственной безопасности Соединенных Штатов Америки, и борьбы с таковой».[109] GEC был создан посредством расширения более ранней межведомственной инициативы США, Центра стратегических антитеррористических коммуникаций (CSCC), который также входил в структуру Государственного департамента.

Четкая стратегия:

Межведомственный подход позволяет GEC координировать работу с коммуникациями без дублирования по всем госструктурам США. Координация с департаментами государственной безопасности помогает создавать информационную основу для постановки задач в рамках деятельности GEC с учетом свежей аналитической и разведывательной информации. Такие межведомственные коммуникации позволяют синхронизировать работу GEC с реализацией прочих антитеррористических мероприятий и мер реагирования госучреждений США.

Производство контента:

GEC и его партнеры сформировали систему разработки программ на основе многочисленных платформ, включая социальные сети, спутниковое телевидение, радио, кино и печать, на различных языках.

Измерение и оценка:

GEC был создан с целью принятия адаптивных мер для реагирования на воздействие средств общения террористов за счет совмещения опыта, полученного в области теории анализа и обработки данных и в сфере борьбы с терроризмом. Согласно официальному сайту GEC, Центр «подходит к решению задачи по развенчанию террористической идеологии с пониманием того, что люди и группы людей, наиболее близкие к сфере противостояния нарративов, способны обеспечить наиболее впечатляющие результаты в борьбе с

[109] См. https://www.state.gov/about-us-global-engagement-center/.

ними». В связи с этим GEC ведет работу по четырем основным направлениям: наука и технологии, межведомственное сотрудничество, привлечение партнеров и производство контента. Использование имеющегося опыта в части теории и технологий анализа и обработки данных позволило разработать передовую практику в области измерения и оценки коммуникационных кампаний, а также применить «эвристически управляемый экспериментальный» подход, который предусматривает использование структуры «создание–оценка–накопление опыта» в отношении реализуемых на практике мероприятий в целях обеспечения их максимальной эффективности, в том числе посредством методов A/B тестирования и многомерного анализа.[110] Кроме того, в докладе «Национальные рамки стратегической коммуникации» от 2010 г. отмечается, что при разработке любой программы стратегических коммуникаций правительства США «должны также предусматриваться особый бюджет и ресурсы на проведение оценочных мероприятий, необходимых для измерения успеха».[111]

Прозрачность, признание рисков и проблем:

В докладе «Национальные рамки стратегической коммуникации» от 2010 г. также подробно описываются сложности, возникающие в процессе оценки того, насколько успешными оказались реализованные меры реагирования на основе коммуникаций с точки зрения изменений в позиции аудитории: «Во-первых, такая работа зачастую имеет целью воздействие на восприятие целевой аудиторией, за которым не так легко наблюдать и, соответственно, которое непросто измерить... Во-вторых, сложно отделить воздействие коммуникаций и вовлечения от влияния прочих факторов, в том числе других стратегических решений. Наконец, воздействие коммуникаций и вовлечения является долгосрочным и требует постоянного измерения».[112] С учетом указанных проблем, наилучшим вариантом является разработка поэтапных, многоуровневых планов оценки успеха, предназначенных для анализа конкретного плана действий или конкретной программы.

Показатели

Госучреждениям рекомендуется разработать, совместно с другими заинтересованными сторонами, включая представителей отрасли ИКТ, организаций гражданского общества, а также научных учреждения, реалистичные показатели для оценки успешности системы мер и программ, направленных на предупреждение насильственного экстремизма в сети Интернет и борьбу с ним. Такие показатели следует разрабатывать с учетом соблюдения прав человека, таких как право на свободу выражения мнений, свободу вероисповедания или убеждений, а также запрет на произвольное или незаконное вмешательство в частную жизнь, закрепленных во Всеобщей декларации прав человека и Международном пакте о гражданских и политических правах.[113]

Показатели для оценки мер реагирования на основе коммуникаций должны согласовываться с содержанием целей и теории изменений, определенными в самом начале процесса разработки. Для оценки изменений (положительных или отрицательных) в основных показателях, а также для установления границ возможного воздействия кампании на целевую аудиторию во всех возможных случаях следует использовать базовые показатели и контрольные группы. Такие показатели в широком смысле можно разделить на три категории: показатели осведомленности, вовлеченности и воздействия. Для создания полной картины эффективности и

---

110 *Там же*.

111 The White House, *National framework for strategic communication*, 2010, p. 13 [Белый дом, *Национальные рамки стратегической коммуникации*, 2010 г., стр. 13]

112 *Там же*, стр. 13.

113 Резолюция Совета Безопасности ООН 2354 (2017 г.) напоминает о праве на свободу выражения мнения, отраженном в статье 19 Всеобщей декларации прав человека, принятой Генеральной Ассамблеей в 1948 году («Всеобщая декларация»), и в статье 19 Международного пакта о гражданских и политических правах, принятого Генеральной Ассамблеей в 1966 году («МПГПП»), и подчеркивает, что любые ограничения этих прав должны быть установлены законом и основания для их введения должны соответствовать пункту 3 статьи 19 МПГПП.

воздействия кампании можно проводить совместный анализ этих показателей.

Осведомленность, вовлеченность и воздействие

Показатели осведомленности демонстрируют охват кампании или количество людей, на которых она оказывает воздействие, а также характеристики такой аудитории. Общие показатели осведомленности для интернет-контента включают показы (количество экранов, на которых появляется контент) и просмотры (количество людей, активно потребляющих контент). Кроме того, показатели осведомленности могут включать демографическую информацию, в том числе возраст, пол и приблизительное местонахождение аудиторий, а также информацию, связанную с интересами аудиторий.

Показатели вовлеченности демонстрируют объем и виды взаимодействия между членами аудитории, участниками кампании и контентом кампании. Показатели вовлеченности могут включать взаимодействие с социальными сетями в форме отметок «нравится», реакций, комментариев и нажатий кнопки «поделиться» и при этом могут быть положительными или отрицательными. Знание количества и природы таких действий способно помочь участникам кампании понять характер взаимодействия их аудитории с кампанией или ее контентом, а также реакцию аудитории на кампанию или такой контент.

Показатели воздействия демонстрируют поддающиеся измерению изменения в знаниях, позициях или поведении целевой аудитории, которые можно отнести к результатам воздействия контента кампании или взаимодействия с таким контентом. Можно совместить надлежащим образом проанализированные показатели осведомленности и вовлеченности, чтобы лицам, проводящим оценку, было проще понять степень воздействия, оказанного их кампанией. Для содействия в проведении общей оценки воздействия можно использовать дополнительные показатели, такие как свидетельства совершения определенных действий оффлайн, реакции на призывы к действию или качественная оценка комментариев в Интернете.

Инструменты мониторинга и оценки

Отслеживать практическую реализацию мер реагирования на основе коммуникаций в Интернете можно посредством различных аналитических онлайн-инструментов, включая «серверный» (back-end) анализ, проводящийся на многих платформах социальных сетей. Такие инструменты могут стать источниками целого спектра показателей и аналитической информации о степени, в которой меры реагирования на основе коммуникаций достигают целевых аудиторий, и о том, как такие аудитории взаимодействуют с контентом кампаний. Они способны создать возможность для внедрения итеративного процесса, который позволит оптимизировать и адаптировать кампанию для достижения ее целей и решения поставленных задач.

Основанные на коммуникациях меры реагирования на проявления насильственного экстремизма и терроризма в сети Интернет, в особенности те из них, которые реализуются силами гражданского общества, проходят лишь начальный этап развития, а организации гражданского общества зачастую не знакомы с передовой практикой в области мониторинга и оценки в Интернете. В этой связи государства могут поощрять использование более сложных подходов посредством предоставления финансирования и поддержки при разработке инновационных методов сбора информации, анализа и исследований, чтобы выйти за пределы базовой аналитики и стандартных показателей, предусмотренных платформами социальных сетей.

Существует огромный спектр доступных и применимых аналитических инструментов — от бесплатных общедоступных вариантов до более прогрессивных коммерческих инструментов:

➔ **Инструменты анализа общественного мнения в социальных сетях** помогут в разработке и оценке эффективных мер реагирования на основе коммуникаций в Интернете. Такие инструменты способны выявлять интересующий контент общедоступных социальных сетей по крупным платформам социальных сетей, таким как Twitter, или форумам и блогам, таким как Reddit или 4Chan. Соответствующий контент можно сортировать по теме, датам или языку. Показатели, получаемые благодаря таким инструментам, помогают отследить тенденции в области распространения нарративов, раскрыть взаимосвязи между отдельными темами, а также

выявить контент, платформы, влиятельных лиц и язык, используемые как насильственными экстремистами или террористами в Интернете, так и целевой аудиторией.

➔ **Инструменты картирования сетей** помогут визуализировать онлайн-сети групп насильственных экстремистов и террористов, а также связи этих групп с различными аудиториями. Инструменты картирования также полезны для определения аудиторий, подвергающихся воздействию мер реагирования на основе коммуникаций, а также способа, которым контент кампании достигает определенных аудиторий. Кроме того, анализ сетей способствует выявлению влиятельных лиц в Интернете, которые могли бы представить соответствующие кампании целевым аудиториям.

➔ **Анализ эмоциональной окраски высказываний** представляет собой совместное использование технологий интеллектуального анализа данных и обработки естественного языка (NLP) для автоматизированного сбора образцов текста и анализа их значения. Программное обеспечение для обработки естественного языка можно применять к образцам онлайн-текста для целей классификации, анализа и определения значения больших объемов слов, фраз или предложений. Метод такого типа может помочь в обработке данных, объем которых слишком велик для проведения анализа вручную, в целях получения более глубокой количественной информации из данных, которые были собраны в рамках кампании, чтобы определить степень воздействия.

Качественные методы

Наряду с возможностями, предоставляемыми онлайн-инструментами и аналитическими данными, существует ряд онлайн- и оффлайн-методов качественного характера, которые могут сыграть важную роль в проведении мониторинга и оценки мер реагирования на основе коммуникаций. Спектр таких методов широк: от качественной оценки онлайн-взаимодействий (например, комментариев) до оффлайн-опросов, фокус-групп и интервью с представителями соответствующей целевой аудитории. Качественные методы могут быть более дорогими или требовать больше времени, чем количественные, однако при этом они могут выступать источниками ценной информации на протяжении всей кампании. Такие методы повсеместно используются в других областях, для понимания того, какой отклик получают различные способы коммуникаций — от социологических или политических исследований до психологии. Примеры передовой практики из этих областей следует применять во всех возможных случаях.

Государства должны понимать, что использование таких методов в отношении определенных типов целевой аудитории может быть невозможным; в частности, это касается аудиторий, недовольных действиями государства, или аудиторий, выражающих симпатию группировкам насильственных экстремистов или террористов либо их идеям. При использовании персонализированных качественных методов государствам во всех случаях следует действовать прозрачно, с учетом подбора наиболее подходящей кандидатуры на роль медиатора или посредника, а также позволять участникам вносить свой вклад анонимно в тех случаях, когда требуется создать условия для подлинной открытости и честности.

Проблемы, связанные с мониторингом и оценкой

Эффективное осуществление мониторинга и оценки основанных на коммуникациях мер реагирования на проявления насильственного экстремизма и терроризма в сети Интернет сопряжено с рядом характерных проблем. Если говорить о мерах реагирования, направленных на нисходящие аудитории, небольшие размеры выборки могут ограничить статистическую значимость полученных выводов. Препятствия для доступа к определенным аудиториям также могут привести к ограничениям с точки зрения получения требуемых показателей, а в результате — к неполной оценке воздействия мер реагирования определенного вида. Результатом этого может стать необъективный выбор в пользу более доступных методов цифровой оценки, ведущий к недостатку качественных данных в заключительном отчете об оценке.

Даже в тех случаях, когда используются качественные методы, может возникнуть фактор «социальной желательности» — стимул для участников представить те результаты, которые, по их мнению, хотят получить

лица, проводящие оценку, или которые считаются социально приемлемыми. Тщательная разработка структуры оценки, а также эффективная реализация приемлемых методов оценки соответствующими участниками способны уменьшить некоторые из этих возможных последствий. В этой связи комплексные системы оценки должны быть прозрачными с точки зрения ограничений в отношении использования определенных методов; при этом любые неоспоримые ограничения должны быть упомянуты в заключительном отчете об оценке. В целях избежания предвзятости и проведения объективной внешней оценки, следует рассмотреть возможность привлечения независимых оценщиков во всех случаях, когда это целесообразно.

Риски, связанные с мониторингом и оценкой

Наряду с возможными проблемами, возникающими при оценке мер реагирования на основе коммуникаций, процессы мониторинга и оценки могут быть сопряжены с этическими рисками, наступающими, например, в результате неумышленного распространения или публикации данных, идентифицирующих личность пользователя сети Интернет. Поэтому важно учитывать правовой контекст, в котором проводится кампания, включая законодательство в области неприкосновенности частной жизни, а также обработки и хранения данных. Госучреждениям следует предоставить соответствующие гарантии в отношении любых инициированных на уровне государства мер реагирования, но при этом также убедиться в том, что в отношении мер реагирования, реализуемых другими участниками и получающих финансирование или поддержку от государства, действуют аналогичные обязательные процедуры.

В целях обеспечения прозрачности, результаты оценки мер реагирования на основе коммуникаций должны быть переданы соответствующим заинтересованным сторонам во всех случаях, когда это возможно, чтобы организовать обмен опытом, повысить эффективность мер реагирования, а также сформировать взаимное доверие. Однако необходимо убедиться в том, что неприкосновенность частной жизни лиц, реализующих соответствующую программу, а также аудиторий, которые она охватывает, защищена посредством анонимизации любой информации, позволяющей установить личность. Такая информация может включать имя пользователя или аккаунта, профиль, фотографии или данные геолокации. Любые выдержки из текста, предоставленного участниками целевых аудиторий, также следует изменить в степени, достаточной для того, чтобы предотвратить их идентификацию посредством функций поиска в социальных сетях или поисковых систем.

Практические примеры: Система оценки Государственной службы коммуникации Великобритании и Руководство по планированию государственных коммуникационных кампаний[114]

Общая и комплексная национальная система:

Система оценки Государственной службы коммуникации Великобритании (GCS) 2016 года представляет собой инструмент, доступный заинтересованным сторонам во всех госструктурах Великобритании. Цель создания этой системы — помочь лицам, осуществляющим коммуникации, оценить и продемонстрировать воздействие проведенной государством работы по осуществлению коммуникаций. Указанная система оценки предназначена не только для коммуникаций государственных учреждений, связанных с насильственным экстремизмом и терроризмом, но и для осуществления деятельности, направленной на достижение целого спектра целей государственной службы.

Использование опыта других секторов:

В основе этой системы оценки лежат самые последние отраслевые стандарты и практические методы, а также

[114] Government Communication Service (GCS), *GCS Evaluation Framework*, January 2016; GCS, *A guide to campaign planning* [Государственная служба коммуникации, *Система оценки Государственной службы коммуникации*, январь 2016 г.; Государственная служба коммуникации, *Руководство по планированию кампаний*]

опыт частного сектора в сфере оценки коммуникаций. Такая структура предусматривает интеграцию методов, отражающую разнообразие механизмов коммуникаций, включая СМИ и цифровые платформы, с учетом важности проведения измерения и оценки с самого начала любой работы по обмену информацией.

Показатели:

Система оценки GCS рекомендует использовать сочетание качественных и количественных методов (например, опросы, обратная связь по результатам интервью, фокус-группы, аналитические данные социальных сетей, а также отслеживание) для оценки результатов и воздействия коммуникационных кампаний. Руководство по системе оценки также предлагает использовать базисные показатели для обеспечения надежности при оценке изменений.[115]

Непрерывная оценка и оптимизация:

Система оценки GCS включает предложения в отношении внесения итеративных корректировок в коммуникационные кампании на основании результатов непрерывного измерения и оценки. Система предполагает, что пользователям следует: «Анализировать эффективность работы и обеспечивать использование результатов оценки в рамках текущей деятельности и будущего планирования».[116]

Оценка жизненного цикла:

Руководство по планированию государственных коммуникационных кампаний гражданской службы Великобритании представляет собой инструмент, помогающим всем сотрудникам государственных учреждений Великобритании принимать конкретные меры в рамках планирования и осуществления любых инициированных государством коммуникаций, даже на этапе до начала производства и распространения контента. Указанное руководство описывает шаги по определению целей соответствующих коммуникаций, целевых аудиторий, идей контента, механизмов практической реализации и процедур оценки: «основные шаги OASIS».[117] Кроме того, в нем представлены ссылки на инструменты, способные помочь повысить качество получаемой от аудитории информации, а также улучшить оценку эффективности коммуникационных кампаний: например, ссылки на аналитические инструменты и руководства социальных сетей.

C. Этические риски и риски с точки зрения безопасности

Подходы с участием различных заинтересованных сторон

Коммуникации со стороны государства могут не дойти до запланированных адресатов и попасть к другой аудитории. С учетом указанных рисков, наибольшей эффективности таких коммуникаций можно достичь при их использовании в восходящем направлении или в качестве средства профилактики для содействия социальному сплочению и формированию устойчивости. В рамках коммуникаций такого типа потенциальные последствия наступления вышеозначенных рисков будут менее серьезными, чем в случае нисходящих коммуникаций. Таким образом, государственные учреждения могут вести работу совместно с представителями отрасли ИКТ и организациями гражданского общества (на добровольной основе) в целях поддержки и наделения правами и полномочиями пользующихся доверием лиц для гарантии того, чтобы их голоса в Интернете были услышаны. Кроме того, целями такой совместной работы являются как направление положительных и альтернативных сообщений лицам, уязвимым к воздействию террористического и экстремистского контента, так и онлайн-взаимодействие с лицами, выражающими сопряженные с насилием

[115] GCS, *GCS Evaluation Framework*, p. 3 [Государственная служба коммуникации, *Система оценки Государственный службы коммуникации*, стр. 3]

[116] *Там же*, стр. 2

[117] GCS, *A guide to campaign planning*, pp. 1–2 [Государственная служба коммуникации, *Руководство по планированию кампаний*, стр. 1-2

экстремистские взгляды или поддерживающими терроризм в Интернете.

Прозрачность

В случае если государства реализуют меры реагирования на основе коммуникаций напрямую, важно обеспечить прозрачность кампаний такого типа в отношении их происхождения или источника финансирования во избежание нарастания недовольства, которое группировки насильственных экстремистов и террористов используют в своих интересах. Любые сообщения, будь то онлайн или оффлайн, должны дополнять более масштабную политику и деятельность государственных органов, чтобы не допустить подрыва доверия к государству.

Прозрачный подход поможет сформировать доверие между населением и государством, снижая тем самым риски, описанные ниже. В случае если государства поддерживают неправительственные организации и организации гражданского общества, прозрачность (в отношении как финансирования, так и оказания поддержки) имеет большое значение с точки зрения недопущения подрыва доверия и нарушения воздействия соответствующих мер реагирования; кроме того, прозрачность способствует обмену передовой практикой, а также формированию культуры накопления опыта и обмена информацией между всеми заинтересованными сторонами.

Незапланированные последствия

Инициированные государством меры реагирования на основе коммуникаций могут иметь целых спектр сложных последствий, не все из которых обязательно будут положительными. В процессе разработки любой меры реагирования на основе коммуникаций следует сопоставлять возможное положительное воздействие с возможным отрицательным или незапланированным воздействием, чтобы понять потенциальную ценность такого воздействия, а также принять меры к минимизации любых возможных отрицательных последствий.

Как результат, государственные учреждения могут обращаться за содействием к различным заинтересованным сторонам, чтобы определить, в какой области каждый участник способен оказать наиболее эффективное воздействие, интегрировать оффлайн- и онлайн-мероприятия, а также применять подход «не навреди» с соответствующими гарантиями для обеспечения того, чтобы меры реагирования на основе коммуникаций были соразмерными и не создавали излишних рисков или незапланированных последствий.

Такие незапланированные последствия могут включать:

- неверное понимание или тривиализацию недовольства целевых аудиторий;
- увеличение привлекательности идей насильственного экстремизма или терроризма;
- риск стигматизации определенных групп населения как «подверженных риску» либо дальнейшее отчуждение или исключение определенных групп, не доверяющих государству;
- признание кампаний незаконными или подрыв доверия к ним в части оспаривания идей насильственного экстремизма или терроризма из-за связей с брендами или посредниками для передачи сообщений, к которым их целевые аудитории могут не испытывать доверия.

Риски с точки зрения безопасности

Основанные на коммуникациях меры реагирования на террористический и сопряженный с насилием экстремистский контент могут подвергнуть риску как членов соответствующих аудиторий, так и самих участников соответствующей кампании: потенциально им угрожают оскорбления в Интернете, а в исключительных случаях — физический вред. Использование подхода «не навреди» и безопасность лиц, реализующих меры реагирования на основе коммуникаций, должны иметь первостепенное значение; при этом участникам должны быть предоставлены результаты всесторонней оценки потенциальных рисков, которым они подвергаются.

Такая оценка должна составлять основу системы безопасности и этики, включая меры по минимизации таких рисков. Указанную систему следует согласовать со всеми заинтересованными сторонами на этапе разработки любой меры реагирования, а на этапах реализации, мониторинга и оценки в отношении нее необходимо регулярно проводить консультации и вносить требуемые изменения.

В некоторых (очень редких) случаях государства принимают решение не раскрывать информацию об оказываемой ими поддержке в отношении определенных мер реагирования на основе коммуникаций в интересах безопасности; например, в случае нисходящей меры реагирования (*см. рис. 1, раздел 5*), когда аудитория кампании может обратиться против лиц, проводящих такую кампанию, или угрожать им. Такие опасения также могут создавать этический риск в форме подверженности заинтересованных сторон, не принадлежащих к государственному сектору, повышенному риску с точки зрения безопасности.

Конкретные риски с точки зрения безопасности и этики, которые следует принять во внимание, варьируются в зависимости от типа кампании, а также прочих факторов, таких как условия, в которых осуществляется кампания, и запланированные целевые аудитории. Однако такие риски можно эффективно снизить посредством тщательного планирования и осторожности при реализации, включая более детальную постановку целей и внимательный выбор контента.

Риски с точки зрения вовлечения

Наконец, хотя многие меры реагирования на основе коммуникаций не предусматривают непосредственного вовлечения лиц, находящихся в группе риска, уязвимых перед угрозой насильственного экстремизма или терроризма или являющихся в настоящее время членами насильственных экстремистских или террористических группировок, все меры реагирования должны включать заранее определенные рекомендации относительно любых взаимодействий с такими лицами. Соответствующие рекомендации должны быть даны в отношении как этапа реализации, так и этапа оценки программ (например, фокус-группы, опросы).

Принимать надлежащие меры при взаимодействии с потенциально уязвимыми лицами — не только этическое требование, но и потенциальная возможность обеспечить положительное воздействие определенных видов мер реагирования для борьбы с насильственным экстремизмом и терроризмом в Интернете. Необходимо учитывать следующие аспекты:

- как взаимодействовать с уязвимыми лицами таким образом, чтобы снизить персональный риск для них, а также ощутимо и эффективно удовлетворить их конкретные нужды;
- как избежать выхода за пределы компетенции и осуществления деятельности, которую отдельные участники кампании не имеют полномочий вести;
- какие существуют подходящие варианты поддержки со стороны органов власти, гражданского общества или сообщества для установления контактов с уязвимыми лицами в случае необходимости.

Привлечение организатора кампаний может помочь в выявлении потенциально негативных, опасных, неожиданных и контрпродуктивных реакций на коммуникационные кампании и в подготовке ответа на такие реакции. Организаторы кампаний зачастую участвуют в коммуникационных кампаниях, не связанных с террористическим и сопряженным с насилием экстремистским (таких как коммерческие рекламные кампании) и могут оказаться полезными как при выявлении комментариев, реакций или действий, связанных с контентом коммуникаций, так и при реагировании на них в соответствующих случаях.

Кроме того, большинство крупных платформ социальных сетей предоставляют рекламодателям или пользователям возможность просматривать комментарии к размещенному контенту и реакции на него, а также анализировать их и реагировать на них. Также существует огромное число доступных коммерческих инструментов, упрощающих управление кампаниями, для групп, которые одновременно осуществляют большое количество коммуникационные кампаний в Интернете или анализируют их воздействие.

Наконец, прозрачность является ключевым элементом методов модерации для участников различных платформ. Государственным органам следует рассмотреть возможность опубликовать содержание политики для социальных сетей в отношении любых страниц и сайтов с публичными коммуникациями с разъяснениями в отношении контента, который может быть подвергнут модерации со стороны организаторов кампании. В число таких видов контента может входить, например, контент, содержащий угрозы или насилие.

Меры реагирования на основе коммуникаций:

5. Сотрудничество с представителями отрасли ИКТ и работа с ОГО

Данный раздел предназначен для лиц, ответственных за разработку политики, и практикующих специалистов и содержит конкретные практические примеры в области развития эффективного сотрудничества между государствами, частным сектором и гражданским обществом, а также, в соответствующих случаях, в области разработки и реализации ряда эффективных мер реагирования на основе коммуникаций, охватывающих все аспекты угрозы насильственного экстремизма и терроризма в сети Интернет. Данный раздел содержит два подраздела: «Партнерства между государством, представителями отрасли ИКТ и гражданского общества» и «Партнерства в рамках спектра мер реагирования на основе коммуникаций».

Соответствующие примеры передовой практики из Цюрихско-Лондонских рекомендаций:

Передовая практика 6. *Применение подхода с участием различных заинтересованных сторон для взаимодействия между государствами, представителями отрасли ИКТ и организациями гражданского общества в работе по предупреждению насильственного экстремизма и терроризма в сети Интернет и борьбе с ними.*

Передовая практика 13. *Противодействие всем аспектам насильственного экстремизма и терроризма путем адаптации онлайн-мероприятий с учетом спектра мер реагирования на основе коммуникаций, включая программы профилактической направленности и контрпропагандистские кампании.*

Передовая практика 14. *Поощрение добровольного сотрудничества для создания аутентичных и инновационных основанных на коммуникациях подходов к решению проблемы террористического и сопряженного с насилием экстремистского контента в сети Интернет путем объединения усилий ИКТ компаний, организаций гражданского общества и других субъектов.*

Передовая практика 15. *Обеспечение наличия определенной целевой аудитории (или аудиторий) для кампаний, конкретной цели (например, снижение риска перехода от радикализации к насилию или содействие в распространении мирных альтернатив пропаганде насилия) и производство четко сфокусированных, точных и контекстно-зависимых сообщений. Анализ конкретной(ых) аудитории(й) может способствовать выявлению подходящих посредников для передачи сообщений, пользующихся доверием у соответствующей(их) целевой(ых) аудитории(й).*

ВВЕДЕНИЕ

Учитывая транснациональный характер Интернета, поддержку в предупреждении насильственного экстремизма и терроризма в сети Интернет и борьбе с ними может оказать эффективное сотрудничество между государствами и различными заинтересованными сторонами, включая ИКТ компании и соответствующие организации гражданского общества. Цюрихско-Лондонские рекомендации подчеркивают, что «государства несут основную ответственность за борьбу с насильственным экстремизмом и терроризмом. Прерогатива государства заключается в принятии решения относительно выбора наиболее эффективного подхода, в соответствии с его обязательствами согласно международному праву, а также согласно его национальному законодательству».[118]

Подход с участием различных заинтересованных сторон, сочетающий в себе политический, технический и контекстуальный опыт и основанный на новейших глубоких исследованиях, которые посвящены характеру движущих сил, лежащих в основе поддержки идей насильственного экстремизма или терроризма, может сыграть важную роль в реализации эффективных мер реагирования на основе коммуникаций. Такое сотрудничество помогает эффективно использовать необходимые креативность, опыт и ресурсы, а также способствует разработке инновационных и устойчивых мер реагирования, предусматривающие четкие стратегии, а также эффективные планирование, разработку, реализацию и оценку.

A. Партнерства между государством, представителями отрасли ИКТ и гражданского общества

Подходы с участием различных заинтересованных сторон: гражданское общество

Государства, рассматривающие возможность реализации коммуникационных стратегий в целях борьбы против террористического и сопряженного с насилием экстремистского контента, должны понимать какой вклад способны внести гражданское общество и прочие гражданские организации в качестве ответственных за реализацию, организаторов или создателей кампаний, а не только как партнеры или дружественные структуры, вовлеченные в их распространение. Организации гражданского общества, которые, как правило, тесно взаимодействуют с местными сообществами, будут с большей вероятностью пользоваться доверием основных аудиторий и могут стать эффективными партнерами в построении системы обладающих большой силой воздействия и устойчивых мер реагирования на уровне местного сообщества.

Организации гражданского общества способны оказать действенную поддержку мерам реагирования на основе коммуникаций для ряда целевых аудиторий, в том числе с учетом определенного пола или возраста, либо для определенных групп сообщества, таких как религиозные организации или образовательные учреждения. В этой связи в случае создания партнерства с организациями гражданского общества при разработке мер реагирования на основе коммуникаций будут учитываться важные аспекты с точки зрения факторов вербовки в экстремистские и террористические группировки (таких как пол), а также направленность таких мер на конкретные опасения и уязвимости соответствующих целевых аудиторий.

Подходы с участием различных заинтересованных сторон с большой вероятностью окажутся эффективными в том случае, если все участники имеют общее понимание соответствующих функций, обязанностей, сильных сторон и ограничений каждого из них с точки зрения реагирования на проявления насильственного экстремизма и терроризма в Интернете. Учитывая потенциальные ограничения с точки зрения участия государства в реагировании на эти проблемы (*см. раздел 4. С. Этические риски и риски с точки зрения безопасности при*

[118] GCTF, *Zurich-London Recommendations on Preventing and Countering Violent Extremism and Terrorism Online*, 2017, p. 4 [ГКТФ, *Цюрихско-Лондонские рекомендации по предупреждению насильственного экстремизма и терроризма в сети Интернет и борьбе с ними*, 2017 г., стр. 4].

принятии мер реагирования на основе коммуникаций), государства могут поощрять самые различные группы гражданского общества к участию в формировании доверия в сообществах, а также в противостоянии нарративам и тактике радикализации и вербовки, используемым экстремистскими и террористическими группировками.

Учитывая широкий выбор возможных подходов к разработке и реализации мер реагирования на основе коммуникаций, государства могут создавать партнерства с организациями гражданского общества за пределами сферы противодействия насильственному экстремизму и борьбы с ним (ПБНЭ). В их число могут входить организации, преимущественно сосредоточенные на защите прав человека, работе с молодежью, оказании социальных услуг и поддержки или осуществлении культурной деятельности. Такие организации могли ранее не рассматривать деятельность по ПБНЭ как часть своих полномочий или могли не знать о важной роли, которую такие методы могут сыграть в рамках более масштабного подхода к предупреждению насильственного экстремизма и терроризма в сети Интернет и борьбе с ними, основанного на участии всего общества.

Таким образом, государства могут обеспечить поддержку и наращивание потенциала представителей гражданского общества посредством проведения обучения, предоставления ресурсов (например, инструментария) и (или) финансирования, чтобы способствовать более активному участию в деятельности по ПБНЭ существующих организаций, работающих как в рамках этой сферы, так и за ее пределами. Такая работа должна быть долгосрочной и устойчивой, поскольку в случае гражданского общества ее результаты неизменно совершенствуются с течением времени. Развитие и демонстрация эффекта от первоначальных программ, в особенности разработанных организациями, которые не имеют опыта в ПБНЭ, могут потребовать времени. В этой связи государствам также следует финансировать проведение мониторинга и оценки в отношении как их собственной работы по наращиванию потенциала, так и программ гражданского общества, которые они поддерживают.

Формирование доверия

Открытый и честный диалог между всеми заинтересованными сторонами имеет определяющее значение для обеспечения эффективного и устойчивого сотрудничества в области предупреждения насильственного экстремизма и терроризма в сети Интернет и борьбы с ними. Государствам следует знать о любых существующих уязвимостях и не допускать избыточного страхования от рисков в части отношений с участием различных заинтересованных сторон, особенно в случаях, когда гражданское общество может быть обеспокоено стигматизацией определенных сообществ.

В связи с этим участие организаций гражданского общества в контрпропагандистской деятельности совместно с государственными учреждениями должно быть добровольным и должно основываться на принципах доверия, конфиденциальности, поэтапного включения в работу и приверженности целям такой работы. При создании любых новых партнерств обсуждения потенциального ответного удара по организациям гражданского общества, которые получают финансирование и выполняют поручения в области коммуникационной работы от государства, должны быть открытыми и прозрачными. Это позволит организациям гражданского общества принимать обоснованные решения о сотрудничестве с госучреждениями в области мер реагирования на проблемы, связанные с присутствием насильственного экстремизма и терроризма в Интернете.

Практический пример: Программа Building a Stronger Britain Together

Программа Building a Stronger Britain Together («Построим сильную Британию вместе») (BSBT) оказывает поддержку британским организациям гражданского общества и местных сообществ, целью которых является создание положительных альтернатив вербовке в экстремистские организации. Программа, финансируемая Министерством внутренних дел Великобритании и находящаяся под управлением Фондов местных сообществ Великобритании, а также частного коммуникационного агентства M&C

Saatchi, позволяет организациям местных сообществ подавать заявки на получение поддержки в натуральной форме или грантового финансирования для программ, направленных на достижение целей, которые являются актуальными с точки зрения целей CONTEST правительства Великобритании, в местных сообществах.[119] Таким образом, программа составляет часть национальной стратегии по предупреждению насильственного экстремизма и терроризма и борьбе с ними согласно рекомендациям раздела 4. По состоянию на февраль 2019 года, 233 организации местных сообществ успешно получили гранты или поддержку в натуральной форме через программы BSBT.[120] По состоянию на лето 2017 года были достигнуты следующие результаты: 20 пакетов коммуникационных стратегий, 15 новых веб-сайтов, 33 пакета обучения и 5 кампаний в социальных сетях.[121]

Подход, основанный на участии всего общества:

В широком смысле программа BSBT направлена на противодействие «экстремизму в любых его формах» и получает поддержку со стороны широкого круга организаций местных сообществ, «независимо от расы, веры, сексуальной ориентации, возраста и пола».[122] В число организаций-партнеров программы BSBT входят центры местных сообществ, религиозные, культурные и молодежные группы, а также спортивные программы. Программа BSBT также признает, что тенденция к использованию сети Интернет в целях насильственного экстремизма и терроризма сохраняется, и потому поощряет заявки по проектам, направленным на «продвижение положительных альтернативных нарративов в целях противодействия экстремистскому контенту в Интернете и (или) для борьбы с экстремистской деятельностью онлайн».[123]

В основе поддержки со стороны такого широкого круга организаций местных сообществ лежит признание того факта, что местные организации и представители гражданского общества «отлично понимают местные нужды и проблемы и лучше всего подходят для предоставления грантов на местном уровне».[124] Проекты имеют различные целевые аудитории и предусматривают оказание поддержки со стороны сообщества уязвимым и изолированным женщинам в сообществах этнических меньшинств, а также проведение семинаров, посвященных британским ценностям и экстремизму в местных условиях.[125] Такой инклюзивный подход помогает обеспечить охват соответствующими проектами подвергающихся риску и маргинализованных групп населения с помощью заслуживающих доверия посредников, не работающих в госструктурах Великобритании.

Кроме того, программа BSBT направлена на укрепление взаимоотношений между организациями-участницами и способствует обмену «передовой практикой» посредством проведения мероприятий на местах, которые также включают обучение в таких областях, как использование социальных сетей и эффективные связи с общественностью.[126] Фондом программы BSBT управляет частная коммуникационная компания M&C Saatchi, которая привносит опыт коммерческого сектора, в дополнение к работе государственных органов и поддержке со стороны гражданского общества.

Четкая стратегия:

Программа BSBT оказывает поддержку широкому спектру организаций, работающих над сохранением

---

[119] Home Office, *Guidance Building a Stronger Britain Together*, 16 September 2016 [Министерство внутренних дел Великобритании, *Руководство по программе Building a Stronger Britain Together*, 16 сентября 2016 г.]

[120] См. ttps://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/777653/Building_a_Stronger_Britain_Together_partners.pdf.

[121] Home Office, *Partnership Support Programme Summer 2017 Update* [Министерство внутренних дел Великобритании, *Программа партнерской поддержки, лето 2017 г., обновление*]

[122] Home Office, *Building a Stronger Britain Together*, [Министерство внутренних дел Великобритании, *Программа Building a Stronger Britain Together*]

[123] См. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/ file/759649/bsbt-inkind-guidance-applicants.pdf, стр. 1.

[124] https://www.efc.be/news/new-programmeme-building-stronger-britain-together-deliver-800000-grants/.

[125] Home Office, Partnership Support Programme Summer 2017 Update [Министерство внутренних дел Великобритании, Программа партнерской поддержки, лето 2017 г., обновление]

[126] *Там же*.

британских ценностей «демократии, свободы слова, взаимоуважения и возможностей для всех». В рамках реализации этой задачи процедура подачи заявок по программе BSBT предусматривает, чтобы успешные заявители предоставляли гарантии непосредственного соблюдения и поддержки существующей антитеррористической стратегии правительства Великобритании.[127] Потенциальные организации-участницы программы BSBT должны оценить актуальность своих проектов с точки достижения четырех желаемых результатов:

1. сокращение числа людей, позиции, взгляды и чувства которых противоречат общим ценностям;
2. возросшее чувство причастности и гражданского участия на местном уровне;
3. более устойчивые сообщества;
4. целенаправленные мероприятия по противодействию известной экстремистской деятельности на местном уровне.[128]

Чтобы предложение было рассмотрено на предмет предоставления гранта или поддержки в натуральной форме, оно должно соответствовать результату 4 и как минимум одному из трех других результатов.[129]

Измерение и оценка:

Заявки на получение поддержки в рамках программы BSBT также должны предусматривать разработку проектов с учетом определенной целевой аудитории и измеримых результатов, включая процедуры подтверждения и оценки таких результатов посредством использования ключевых показателей эффективности (КПЭ).[130] Соответствующие организации должны указать свои общие цели и задачи, а также цели и задачи конкретного проекта, для достижения которых они хотели бы получить поддержку в рамках программы BSBT, а также пояснить, каким образом такие цели и задачи связаны с четырьмя результатами BSBT.

Прозрачность:

Успешные заявители должны открыто сообщить о том, что они получают государственное финансирование, на своем веб-сайте или иным способом; в противном случае их финансирование будет отозвано.[131] Кроме того, перечень финансируемых организаций ежегодно публикуется и делается доступным для всеобщего сведения.

Добровольное сотрудничество с ИКТ компаниями в целях профилактики

Добровольное и прозрачное сотрудничество между госучреждениями и ИКТ компаниями поможет обеспечить более глубокое понимание угрозы, которую создают распространяемые насильственными экстремистами и террористами коммуникации в Интернете, а также усилить воздействие мер реагирования на основе коммуникаций в борьбе с такими угрозами. Как и в рамках партнерств с организациями гражданского общества, партнерства государств и ИКТ компаний в части мер реагирования на основе коммуникаций должны основываться на принципах прозрачности и доверия в соответствии с национальным законодательством.

Государства могут поощрять ИКТ компании к ведению профилактической деятельности в рамках предупреждения проявлений насильственного экстремизма и терроризма на платформах таких компаний и борьбы с ними, а также к более эффективной защите своих пользователей посредством поддержки основанных на коммуникациях инновационных методов, используемых гражданским обществом. Такое сотрудничество с крупными ИКТ компаниями позволит увеличить степень охвата и воздействия, требуемых для эффективного и устойчивого противостояния угрозе, которую создают распространяемые насильственными экстремистами и террористами коммуникации в Интернете.

---

[127] Home Office, *Applying for grant support Guidance for applicants*, 2019 [Министерство внутренних дел Великобритании, *Подача заявок на получение грантовой поддержки. Руководство для заявителей*, 2019 г.]

[128] *Там же*, стр. 13-15.

[129] *Там же*, стр. 13.

[130] *Там же*, стр. 16.

[131] *Там же*, стр. 7.

Примером такого сотрудничества может служить партнерство между ПРООН и программой YouTube *Creators for Change* («*Авторы за изменения*»), которая поддерживает ОГО в Малайзии, Индонезии, Таиланде и Филиппинах посредством предоставления небольших грантов, проведения кураторской работы, а также развития сети единомышленников в целях поощрения влиятельных лиц из представителей молодежи к созданию контента для противодействия сообщениям террористов и насильственных экстремистов и создания положительной альтернативы таким сообщениям в Интернете.[132] ПРООН также создала аналогичное партнерство с компанией Facebook в этом регионе для демонстрации серии онлайн-видеороликов с участием бывших насильственных экстремистов.[133] Ели говорить о примерах на национальном уровне, правительство Австралии сформировало партнерства с широким кругом частных технологических компаний, в том числе с компаниями Facebook, Google, Microsoft (включая Xbox), Oath, Twitter, Instagram, Periscope и Yahoo для проведения конференции DIGI Engage 2018 совместно со Специальным саммитом АСЕАН-Австралия.[134] В мероприятии приняло участие 80 лидеров молодежных движений из указанного региона в целях развития своих навыков и получения инструментов, которые помогут им внести свой вклад в противодействие насильственному экстремизму в Интернете. Эта инициатива проводится ежегодно, начиная с 2017 года, и продолжает привлекать молодых людей из Азиатско-Тихоокеанского региона.[135]

Государствам также следует стремиться привлечь, помимо крупных платформ социальных сетей, таких как Facebook, YouTube или Twitter, многочисленные малые ИКТ компании, которые также могут сыграть важную роль в создании соответствующей онлайн-экосистемы для защиты от насильственных экстремистов и террористов. Платформы, используемые насильственными экстремистами и террористами, как правило, различаются в зависимости от географического положения и языка, однако могут включать и небольшие платформы социальных сетей, форумы, мессенджеры, аудио- или видеоплатформы. Государствам следует понимать, что, несмотря на желание небольших платформ участвовать в предупреждении насильственного экстремизма и терроризма в сети Интернет и борьбе с ними, у них может не быть таких же ресурсов и опыта, как у крупных компаний, и в этой связи им может потребоваться дополнительная поддержка от других участников сектора ИКТ.

Международная координация

Государства могут использовать существующие государственные или отраслевые площадки для обмена передовой практикой и ресурсами (при наличии такой возможности), например, Исполнительный директорат Контртеррористического комитета Организации Объединенных Наций (ИДКТК ООН), Глобальный интернет-форум по противодействию терроризму (GIFCT) или Интернет-форум ЕС. Такие площадки способствуют разработке общих целей и структур, открытию каналов для коммуникаций, наращиванию потенциала, сглаживанию конфликтов интересов и выявлению критически важных пробелов. Скоординированные усилия помогают упростить реализацию инициатив с участием различных заинтересованных сторон и обеспечить принятие взаимодополняющих мер.

Практический пример: Интернет-форум Европейского союза

Добровольное сотрудничество:

Интернет-форум ЕС был запущен в декабре 2015 года Комиссаром по вопросам миграции, внутренних дел и гражданства для решения проблемы, связанной с использованием Интернета террористическими группировками. Интернет-форум ЕС объединяет министров внутренних дел стран ЕС, представителей

[132] См. http://www.asia-pacific.undp.org/content/rbap/en/home/operations/projects/overview/creators-for-change0.html.

[133] См. http://www.asia-pacific.undp.org/content/rbap/en/home/programmes-and-initiatives/extremelives.html.

[134] См. https://digiengage2018.splashthat.com/.

[135] См. https://digiengage2019.splashthat.com/.

интернет-индустрии и прочие заинтересованные стороны (такие как Европол, Европейскую сеть стратегических коммуникаций и Сеть по повышению осведомленности о радикализации) для сотрудничества в рамках добровольного партнерства. Целью Форума является решение проблемы, связанной с использованием Интернета террористами и, соответственно, обеспечение более эффективной защиты граждан ЕС. В связи с этим Интернет-форум ЕС имеет две основные задачи: сократить наличие и доступность террористического интернет-контента, а также предоставить партнерам из числа представителей гражданского общества права и возможности для увеличения объема эффективных альтернативных нарративов в Интернете. Интернет-форум ЕС дает возможность представителям государств-членов ЕС обсуждать вопросы, касающиеся использования Интернета террористами и насильственными экстремистами, с участием широкого круга ИКТ компаний; по состоянию на декабрь 2018 года, в их число входили компании Baaz, Dropbox, Facebook, Google, Justpaste.it, Microsoft, Snap и Twitter.

Поддержка мер реагирования на основе коммуникаций, реализуемых гражданским обществом

В декабре 2016 года в рамках Интернет-форума ЕС была запущена Программа ЕС по предоставлению прав и возможностей гражданскому обществу для оказания содействия в разработке кампаний по распространению альтернативных нарративов и контраргументов в Интернете.[136] В настоящее время программа предоставляет финансирование ЕС в размере приблизительно 12 миллионов евро в целях борьбы с экстремизмом и терроризмом. Программа подтверждает тот факт, что многие организации гражданского общества уже предпринимают активные попытки по созданию и распространению альтернативных нарративов, противостоящих идеям насильственного экстремизма и терроризма, однако им зачастую не хватает возможностей и ресурсов для эффективного ведения такой деятельности в Интернете. Программа направлена на создание партнерств с экспертами и авторами в сфере маркетинга и коммуникаций для предоставления профильного обучения получателям грантов из числа представителей гражданского общества, а также на поддержание существующих партнерств с крупными компаниями социальных сетей, которые также проводят соответствующее обучение и рассказывают о передовой практике в области онлайн-маркетинга и создания контента по всему миру. Обучающие материалы в рамках Программы по предоставлению прав и возможностей гражданскому обществу доступны онлайн на нескольких языках.[137]

Прозрачность:

Организации гражданского общества, получающие финансирование и поддержку в рамках Программы по предоставлению прав и возможностей гражданскому обществу, перечислены в открытой онлайн-базе данных с указанием названий проектов и сумм предоставленного финансирования.[138]

Опыт частного сектора

ИКТ компании обладают значительным техническим опытом, возможностями для обучения и ресурсами — как для госсектора, так и для гражданского общества — для содействия в успешной реализации мер реагирования на основе коммуникаций. Это включает консультации по вопросам обеспечения наилучшего охвата и вовлечения конкретных аудиторий на определенных ИКТ платформах (в том числе посредством адресной рекламы), а также эффективной оценки воздействия онлайн-коммуникаций. ИКТ компании также могут сыграть важную роль в финансировании и поддержке исследований в области использования их платформ группировками насильственных экстремистов и террористов. Результаты таких исследований могут впоследствии использоваться партнерами в различных отраслях при разработке мер реагирования коммуникационного характера, адаптированных для соответствующей онлайн-экосистемы.

---

[136] См. https://ec.europa.eu/home-affairs/what-we-do/networks/radicalisation_awareness_network/civil-society-empowerment-programme_en

[137] *Там же.*

[138] См. https://ec.europa.eu/home-affairs/sites/homeaffairs/files/financing/fundings/security-and-safeguarding-liberties/internal-security-fund-police/union-actions/docs/isfp-list-proposals-selected-for- funding-during-2018_en.pdf

При работе с частным сектором в области борьбы с коммуникациями, распространяемыми насильственными экстремистами и террористами в Интернете государствам следует также обратиться к опыту различных экспертов из других областей, включая анализ данных, онлайн-коммуникации, рекламу, маркетинг и производство контента, а также активно сотрудничать с такими экспертами. Опыт работы в этих областях поможет вывести меры по ПБНЭ за пределы базовых методов маркетинга контента для создания более сложных онлайн-кампаний с использованием самых передовых методов, применяемых в коммерческом секторе.

Например, многие коммерческие бренды стремятся отойти от нацеленности на конкретные продукты и использовать кампании, в большей степени ориентированные на ценности, чтобы учесть интересы более молодых аудиторий. Другие создают иммерсивные кампании, предусматривающие многочисленные версии контента, чтобы различные аудитории могли найти в них близкие для себя сообщения. В качестве альтернативы, поскольку ценность крупных кампаний постепенно снижается, многие компании все чаще используют адресные микрокампании с участием «влиятельных лиц» для продвижения своих продуктов в узкоспециализированных аудиториях. Такие методы были разработаны по результатам глубоких исследований рынка и с применением онлайн-анализа для формирования четкого понимания того, какие именно аудитории они должны охватить. В некоторых случаях разработка и подготовка новых итераций кампаний и контента начинается с использования искусственного интеллекта.

Коммуникации со стороны государства и гражданского общества зачастую опаздывают с применением таких более современных методов, отдавая вместо этого предпочтение масштабным кампаниям для массовых аудиторий. Поскольку приобретение опыта в этих областях может оказаться чрезмерно дорогим для организаций гражданского общества, государства также могут внести здесь свой вклад посредством поощрения безвозмездной поддержки или поддержки в натуральной форме со стороны частного сектора в рамках программ корпоративной социальной ответственности (КСР) для решения проблем, связанных с насильственным экстремизмом и терроризмом в сети Интернет.

B. Партнерства в рамках спектра мер реагирования на основе коммуникаций

Зачастую отсутствует концептуальная ясность в отношении спектра возможных основанных на коммуникациях мер реагирования на проявления насильственного экстремизма и терроризма в сети Интернет. В некоторых случаях в качестве универсального термина для описания ряда методов направления сообщений в рамках практики ПБНЭ используется слово «контрпропаганда» или «контраргументы». В этой связи чрезвычайно важно четко и последовательно провести различия между различными мерами реагирования на основе коммуникаций, чтобы обеспечить их правильное применение и не допустить использования таких мер в неподходящих аудиториях во избежание незапланированных последствий. Для целей настоящего инструментария, меры реагирования на основе коммуникаций можно разделить на две широкие категории: восходящие и нисходящие методы (*см. раздел 4 «Борьба со всеми формами насильственного экстремизма и терроризма»*).

Следует отметить, что, несмотря на это разделение на категории, меры реагирования на основе коммуникаций не являются обособленными и могут использоваться как часть более масштабного спектра мер, поэтому некоторые кампании или программы могут включать элементы одного или нескольких видов реагирования. Кроме того, меры реагирования на основе коммуникаций: во многом зависят от контекста, поэтому сравнение таких мер, реализуемых в разных условиях на национальном или местном уровне, может оказаться невозможным. В таблице ниже (таблица 1) показаны различия между восходящими и нисходящими методами проведения коммуникационных кампаний, включая разницу в задачах, в видах необходимых посредников для передачи сообщений, а также в видах целевой аудитории.

Таблица 1. Восходящие и нисходящие методы принятия мер реагирования на основе коммуникаций

	Восходящие методы		**Нисходящие методы**	
Вид меры реагирования	Повышение осведомленности	Положительные или альтернативные нарративы	Контраргументы	Онлайн-вовлечение и мероприятия
Цели	Профилактика и формирование устойчивости		Удержание от увлечения экстремистским или террористическим контентом или остановка радикализации на ранней стадии	Содействие дерадикализации или освобождению от влияния группировок насильственных экстремистов или террористов, либо их идеологий
Задачи	" «Информировать о государственной политике, стратегии или законодательстве " Повысить осведомленность об услугах по оказанию поддержки " Опровергать дезинформацию или неверную информацию " Устранить опасения, сформировать доверие со стороны общества и выстроить отношения с основными дружественными структурами " Сформировать сильное и инклюзивное ощущение идентичности и принадлежности " Повысить осведомленность граждан об их правах и обязанностях	" Популяризировать положительные ценности, например, права человека, демократию, толерантность, многообразие и плюрализм " Продвигать методы расширения гражданского участия на благо общества " Бороться с отрицательными стереотипами и предубеждениями	" Непосредственно оспаривать, разрушать, дискредитировать или развенчивать сообщения и идеологии насильственного экстремизма или терроризма посредством эмоционально заряженного контента, раскрытия лицемерия, лжи, дезинформации или неверной информации	" Непосредственно вовлекать участников насильственных экстремистских или террористических группировок, или онлайн-сообществ

	Восходящие методы		Нисходящие методы	
Посредники для передачи сообщений	" «Государство " Государственные служащие " Политики	" Гражданское общество " Местные сообщества " Молодежь " «Влиятельные лица», например, представители спорта или индустрии развлечений " Частный сектор " Религиозные деятели или учреждения " Бывшие экстремисты / террористы и (или) выжившие после применения насилия экстремистами или террористами		" Прошедшие специальное обучение практикующие специалисты по вмешательству и (или) бывшие экстремисты / террористы
Целевые аудитории	Более массовые аудитории, например, широкая общественность, родители и семьи, государственные служащие, практикующие специалисты, ученики средней школы		Подверженные риску или уязвимые лица, т.е. лица, активно просматривающие или ищущие экстремистский или террористический контент в Интернете	Участники насильственных экстремистских или террористических группировок, или онлайн-сообществ

Государства должны знать о возможности того, что доверие к кампании у определенных целевых аудиторий может быть подорвано в том случае, если госучреждения будут непосредственно реализовывать нисходящие меры реагирования на основе коммуникаций, участвовать в их реализации или оказывать им открытую поддержку. Вместо этого государства могут помочь в наращивании потенциала организаций, работающих в этих сферах, а также поощрять другие лица (например, фонды частного сектора и гражданского общества) к оказанию непосредственной поддержки таким мерам.

Практический пример: Проект ЮНЕСКО «Предупреждение экстремизма благодаря расширению прав и возможностей молодежи»

1 февраля 2018 г. ЮНЕСКО запустила двухлетний проект стоимостью 2 миллиона долл. США, направленный на вовлечение молодежи в Тунисе, Марокко, Ливии и Иордании в работу по предупреждению насильственного экстремизма. ЮНЕСКО и Контртеррористический центр Организации Объединенных Наций (КТЦ ООН) запустили проект «Предупреждение насильственного экстремизма благодаря расширению прав и возможностей молодежи в Иордании, Ливии, Марокко и Тунисе» в рамках проведения соответствующего мероприятия в штаб-квартире ЮНЕСКО в Париже в апреле 2018 года; софинансирование по проекту предоставляет правительство Канады. Проект направлен на расширение прав и возможностей молодежи для развития устойчивости к идеям насильственного экстремизма в качестве альтернативы прямой контрпропаганде в связи с конкретными экстремистскими идеями или контентом.

Расширение прав и возможностей молодых людей как пользующихся доверием посредников для донесения альтернативных идей

Проект ЮНЕСКО сосредоточен на роли молодежи в реагировании на проявления насильственного экстремизма в указанном регионе. В запуске проекта приняли участие шесть молодых людей, тем или иным образом подвергшихся воздействию насильственного экстремизма на территории региона, которые выступили со своими комментариями. Проект поддерживает молодежные инициативы в области образования, науки, культуры и СМИ в целях предупреждения насильственного экстремизма. В этом многостороннем проекте участвуют молодежные организации, заинтересованные стороны из числа образовательных учреждений и работники СМИ, ведущие совместную работу в различных областях, включающих диалоги с молодежью,

обучение в сфере освещения событий с учетом возможности конфликта и лаборатории критического мышления.[139]

Проект предусматривает проведение обучения в области «противодействия разжиганию ненависти в Интернете» и направлен, помимо прочего, на разработку «новых медиапространств для распространения альтернативных нарративов молодыми людьми и для них». В связи с этим проект предусматривает вовлечение работников СМИ и молодежных онлайн-сообществ посредством проведения обучения и разработки национальных и региональных онлайн-кампаний.[140] Своей целью в рамках проекта ЮНЕСКО называет «создание для молодых женщин и мужчин возможностей для деятельности в качестве проводников перемен и миростроителей непосредственно в своих общинах и в обществе в целом, а также поощрение конструктивного представления о молодых людях как о лидерах, решающих проблемы, связанные с ненавистническими настроениями».[141] В соответствии с Резолюцией Совета Безопасности ООН 2250 и Повесткой дня ООН в целях устойчивого развития проект направлен на формирование навыков, которые могут быть использованы как в Интернете, так и в реальной жизни.

Сотрудничество с различными заинтересованными сторонами

ЮНЕСКО тесно сотрудничает с такими партнерами, как министерства молодежи, образования, труда, ИКТ компаниями, а также с организациями гражданского общества, в структура и деятельности которых охватывают молодежь, сети образовательных и культурных учреждений, местные религиозные лидеры и вузы. В рамках всех этих партнерств ЮНЕСКО закрепляет принципы соблюдения прав человека и прозрачности.

В ходе мероприятия, проходившего в Канаде в ноябре 2018 года, в рамках указанной программы ЕС и ЮНЕСКО провели семинар для молодежи, посвященный СМИ, журналистике и культуре с учетом соблюдения прав человека. В число участников вошли организации гражданского общества студенты факультетов журналистики и представители СМИ. Три сессии были посвящены темам медиаграмотности, освещению событий с учетом соблюдения прав человека, а также мультипликации как культурному инструменту для формирования толерантности и открытости.[142]

Сообщения, аудитории и посредники для передачи сообщений

Сообщения в рамках мер реагирования на основе коммуникаций должны быть четко сфокусированными, ясными, а также должны учитывать контекст, с особым вниманием к созданию убедительных нарративов и контента. Кампании, предназначенные для формирования устойчивости к террористическому и сопряженному с насилием экстремистскому контенту, требуют использования сообщений и посредников для их передачи, отличных от сообщений и посредников, которые задействуются в рамках кампаний по освобождению от влияния или дерадикализации сторонников насильственного экстремизма и терроризма, а также лиц, симпатизирующих таким идеям.

В случае если кампании будут разрабатываться не согласованно, существует возможность наступления незапланированных последствий, включая неумышленное содействие в распространении или поддержке идей насильственного экстремизма и терроризма в рамках нисходящих кампаний.[143] При разработке таких сообщений ключевой момент состоит в том, чтобы вместо попыток развенчать или опровергнуть

---

[139] UNESCO, *Launch of Project to Tackle Violent Extremism in Jordan, Libya, Morocco and Tunisia*, 19 April 2018 [ЮНЕСКО, *Запуск проекта по борьбе с насильственным экстремизмом в Иордании, Ливии, Марокко и Тунисе*, 19 апреля 2018 г.]

[140] UNESCO, *New project to tackle violent extremism in Jordan, Libya, Morocco and Tunisia*, 05 February 2018 [ЮНЕСКО, *Новый проект по борьбе с насильственным экстремизмом в Иордании, Ливии, Марокко и Тунисе*, 5 февраля 2018 г.]

[141] См. https://en.unesco.org/preventing-violent-extremism/youth/project.

[142] UNESCO, *Canada, EU and UNESCO host media, journalism and culture for human rights youth seminar*, 18 November 2018 [ЮНЕСКО, *Канада, ЕС и ЮНЕСКО проводят семинар для молодежи, посвященный СМИ, журналистике и культуре с учетом соблюдения прав человека*, 18 ноября 2018 г.]

[143] Nicholas J. Cull, *Counter Propaganda: Cases from US Public Diplomacy and beyond*, Legatum Institute Transitions Forum, July 2015.

экстремистские или террористические идеи сообщения содержали нарративы, находящие более глубокий отклик у целевой аудитории.[144] Воздействие информации, которая оспаривает взгляды отдельных лиц, может лишь закрепить такие взгляды.[145] В этой связи сообщение следует составлять с учетом конкретной аудитории и для нее, а также принимая во внимание возможные последствия для лиц, находящихся за пределами целевой аудитории, которые при этом могут подвергнуться воздействию кампании.

Чтобы сообщение нашло эффективный отклик, посредники для передачи сообщений должны быть реальными людьми и должны пользоваться доверием у целевой аудитории. Таким посредником может стать один из участников соответствующей целевой аудитории. Пол также является важным аспектом, поскольку кампании могут находить различный отклик у мужчин и у женщин, или у мальчиков и у девочек.

Некоторые из наиболее эффективных кампаний предусматривают непосредственное вовлечение или участие аудиторий посредством создания фокус-групп или проведения опросов на этапе их разработки в целях создания, проверки и совершенствования сообщений, контента или планов по их распространению, поскольку зачастую участники таких аудиторий обладают непосредственным опытом, знанием местных особенностей и пониманием того, каким образом можно наиболее эффективно вовлечь других участников и оказать на них влияние. Вопросы этики, безопасности и рисков, связанные с таким вовлечением аудиторий, необходимо проанализировать заблаговременно, включая такие их аспекты, как стимулы для соответствующих аудиторий, анонимность, а также порядок получения и фиксирования результатов. Требуется принять необходимые меры для защиты персональных данных и личностей всех участников.

Практический пример: Afrika Moja — Центр передового опыта в области предупреждения насильственного экстремизма и борьбы с ним Межправительственной организации по развитию (IGAD)

В сентябре 2017 года Межправительственная организация по развитию (IGAD) собрала молодых людей со всего региона Африканского Рога и Восточной Африки, включая Сомали, Джибути, Кению, Танзанию и Уганду, для разработки и запуска платформы гражданского общества в целях содействия в проведении серии кампаний по популяризации альтернативных нарративов и контраргументов на основе историй, произошедших в этом регионе.[146]

В основе двухдневного семинара лежали результаты проведенного ранее мероприятия по обучению молодых активистов навыкам, которые требуются для разработки инновационных и эффективных кампаний на базе видеороликов и изображений с использованием подхода «равный равному», что обеспечило участие в создании контента целевой аудитории. В результате была создана платформа Afrika Moja, целью которой является борьба с экстремистскими сообщениями в указанном регионе посредством распространения историй местных жителей, имеющих положительный характер, и раскрытия лицемерия со стороны группировок насильственных экстремистов. Первая кампания платформы, Strength in Diversity («Сила в многообразии»), была также создана в ходе указанного мероприятия, а ее целью стало определение общих ценностей для всего населения континента. После семинара кампания получила распространение в социальных сетях (Facebook,

---

144 C.R. Sunstein, *On Rumors: How Falsehoods Spread, Why We Believe Them, and What Can Be Done* (Princeton: Princeton University Press, 2014), pp. 47-53. По результатам еще одного недавнего исследования был сделан вывод о том, что в ходе кампании по выборам президента США в 2012 году «(...) Twitter помог сплетникам распространить ложную информацию в гей-сетях и лишь в редких случаях функционировал в качестве самокорректирующегося рынка идей». Ср. J. Shin, L. Jian, K. Driscoll, F. Bar, *Political rumoring on Twitter during the 2012 US presidential election: Rumor diffusion and correction*, New Media & Society, 08 March 2016, p. 2, doi: 10.1177/1461444816634054 (2016-10-23).

145 Amanda Ripley, *Complicating the Narratives – The Whole Story*, The Whole Story, 27 June 2018. Загружено18 сентября 2018 г. с https://thewholestory.solutionsjournalism.org/complicating-the-narratives- b91ea06ddf63.

146 IGAD Center of Excellence in Preventing and Countering Violent Extremism (ICEPCVE), *IGAD Launches Afrika Moja, An Umbrella Platform For Civil Society Campaigns To Counter Violent Extremism*, 20 September 2017 [Центр передового опыта в области предупреждения насильственного экстремизма и борьбы с ним (ICEPCVE) Межправительственной организации по развитию (IGAD), *IGAD запускает Afrika Moja, зонтичную платформу для кампаний гражданского общества по борьбе с насильственным экстремизмом*, 20 сентября 2017 г.]

Twitter и Instagram). Центр продолжил оказывать поддержку ОГО и молодежи региона в целях создания эффективных контрпропагандистских кампаний, в том числе посредством проведения дополнительных семинаров в Уганде, Кении, Эфиопии и Джибути, посвященных распространению мнений лидеров молодежных движений, созданию контрпропагандистских иллюстраций и инфографики, построению эффективных стратегических партнерств в области коммуникаций, а также эффективному использованию видеоматериалов соответственно.[147]

В качестве альтернативы, к участию в кампаниях могут привлекаться «влиятельные лица» — люди, способные обеспечить эффективный контакт с определенными аудиториями и получить от них отклик, как в ходе разработки кампаний, так и в ходе их реализации. Например, в зависимости от аудитории, это могут быть представители местного сообщества или деятели культуры (например, музыканты или спортсмены).

Таким образом, кампании должны разрабатываться на основе результатов анализа целевой аудитории, понимания желаемой аудитории «оффлайн», а также A/B тестирования сообщений в целях определения эффективных и творческих методов создания и распространения контента. Эту информационную основу следует использовать на этапах творческого планирования, разработки контента и тестирования, а также включить в подробные планы создания и распространения контента, чтобы обеспечить эффективную разработку и реализацию кампаний, а также достижение их целей и решение поставленных задач.

Коммуникационные среды

Для обеспечения эффективности коммуникационных кампаний носитель коммуникации так же важен, как контент и способ передачи сообщения. Это включает вид контента (например, текст, аудио- или видеоматериалы и т. д.) и коммуникационный канал или платформу, посредством которых такой контент распространяется (например, социальные сети, игровые платформы, трансляции, печать и т. д.).

Кампании следует разрабатывать на основе четкого понимания соответствующих тенденций, в том числе того, что является популярным в соответствующей целевой аудитории и почему. В некоторых случаях это может оказаться не онлайн-платформа и не определенный вид контента. Напротив, оффлайн-подходы и существующий контент (например, популярные телевизионные или радиопрограммы или печатные издания) могут оказывать более сильное влияние. Эти аспекты должны лечь в основу подробных планов распространения для каждой кампании.

Практический пример: Duta Damai — «Посланники мира»

Pusat Media Damai (Медиацентр мира) был учрежден Заместителем по вопросам предупреждения, защиты и дерадикализации Национального агентства Индонезии по борьбе с терроризмом (BNPT) в целях поддержания национальных усилий по борьбе с использованием сети Интернет насильственными экстремистами и террористами и противостоянию такому использованию. В рамках более масштабной стратегии BNPT впоследствии создало Duta Dumai — Инициативу «Посланники мира» — в 2016 году.[148]

Работа с молодежью:

Duta Damai — это сообщество молодых блогеров, создателей веб-сайтов и разработчиков, которые работают

[147] ICEPCVE, *Yali Workshop – 13th To 16th November 2018: Amplifying The Voices Of Young African Leaders*, 02 October 2018 [Центр передового опыта в области предупреждения насильственного экстремизма и борьбы с ним (ICEPCVE), *Семинар Yali — 13–16 ноября 2018 г. Распространение мнений молодых африканских лидеров*, 02 октября 2018 г]; ICEPCVE, *Using Illustrations And Infographics To Communicate Violent Extremism*, 07 July 2019 [ICEPCVE, *Использование иллюстраций и инфографики для рассказа о насильственном экстремизме*, 07 июля 2019 г.]; ICEPCVE, *Partnerships To Strenghten Strategic Communications*, 30 May 2019 [ICEPCVE, *Партнерства для укрепления стратегических коммуникаций*, 30 мая 2019 г.]; ICEPCV *Tell Me A Story Video Messages To Challenge And Undermine Violent Extremist Ideologies*, 21 May 2019 [ICEPCV *Расскажи мне историю: видеосообщения в целях оспаривания и подрыва идеологий насильственного экстремизма*, 21 мая 2019 г.]

[148] Asmak Abdurrahman, *ASEAN Youth Ambassador for Peace 2019 Resmi dibuka*, Duta Damai NTB, 2019.

в рамках общей стратегии Национального агентства по борьбе с терроризмом, способствуя достижению контртеррористических целей государств, а также распространению цифровой грамотности, демократии и мира.[149]

Программа «Посланники мира» учит своих молодых участников создавать и распространять собственные контраргументы и положительные нарративы, как в Интернете, так и в реальной жизни. Эти «посланники» из числа молодежи делятся своим контентом друг с другом и с общественностью через Интернет посредством целого спектра различных источников. С момента своего создания программа «Посланники мира» распространилась на 13 провинций, а число ее участников-молодых людей достигло 780.[150]

Указанная программа учитывает аспекты устойчивости и масштаба, давая молодым «посланникам» возможности самим стать тренерами и помогать другим людям в своих сообществах овладеть аналогичными навыками.

Международное сотрудничество:

Инициатива «Посланники мира» распространяется на новые провинции и области каждый год, и в этом году она вышла на международный уровень и теперь включает представителей молодежи из Малайзии, Сингапура, Камбоджи, Лаоса, Филиппин, Брунея-Даруссалама, Мьянмы и Таиланда.[151] В рамках реализации инициативы на международном уровне была проведена трехдневная конференция, темой которой стало «Распространение мира в киберпространстве». Конференцию посетили 116 молодых людей в возрасте от 20 до 30 лет из Индонезии и других стран АСЕАН.

Первой целью конференции было проведение обучения для участников в области опасностей, связанных с онлайн-радикализацией, а также способов распространения экстремистских и террористических идей в Интернете. Конечной целью стало расширение прав и возможностей молодежи в сфере использования киберпространства для оспаривания таких идей и борьбы с ними с помощью собственных положительных и мирных нарративов. Программа обеспечила развитие у ее участников как навыков письменной речи, так и технических навыков (разработка веб-сайтов/графики, монтаж видеоматериалов и т. д.).[152]

[149] См. https://dutadamainusatenggarabarat.id/tentang-kami-2/.

[150] Dyah Dwi Astuti, *Duta Damai Dunia Maya direncanakan diperluas hingga antarbenua*, ANTARANEWS. com, 24 April 2019.

[151] Asmak Abdurrahman, *ASEAN Youth Ambassador for Peace 2019 Resmi dibuka*.

[152] *Там же*.

Меры реагирования на основе коммуникаций:

6. Расширение прав и возможностей молодежи и формирование устойчивости посредством обучения молодежи в области противодействия насильственному экстремизму и борьбы с ним, обеспечения онлайн-безопасности и цифровой гражданственности

Данный раздел предназначен для лиц, ответственных за разработку политики, и практикующих специалистов и содержит конкретные практические примеры, касающихся роли образования в основанных на коммуникациях мерах реагирования на проявления насильственного экстремизма и терроризма в сети Интернет. Здесь описываются функции государства и других заинтересованных сторон, в том числе сектора образования, гражданского общества и частного сектора, а также ряд возможных методов, которые могут использоваться для защиты молодых людей в Интернете. Данный раздел содержит три подраздела: «Разработка системы мер реагирования в сфере образования», «Спектр мер реагирования в сфере образования» и «Реализация мер реагирования в сфере образования»

Соответствующие примеры передовой практики из Цюрихско-Лондонских рекомендаций:

Передовая практика 3. *Выработка четкой стратегии борьбы с насильственным экстремизмом и терроризмом в сети Интернет на основе подхода, объединяющего вовлечение соответствующих государственных учреждений и всего общества, координирующего меры реагирования как на основе контента, так и на основе коммуникаций, а также оффлайн-мероприятия, включая обучение и привлечение организаций гражданского общества в соответствующих случаях.*

Передовая практика 14. *Поощрение добровольного сотрудничества для создания аутентичных и инновационных основанных на коммуникациях подходов к решению проблемы террористического и сопряженного с насилием экстремистского контента в сети Интернет путем объединения усилий ИКТ компаний, организаций гражданского общества и других субъектов.*

ВВЕДЕНИЕ

Образование может сыграть ключевую роль как часть более масштабной коммуникационной стратегии по предупреждению насильственного экстремизма и терроризма в сети Интернет и борьбе с ними. Системы образования охватывают огромное количество молодых людей, которые зачастую являются основными целями группировок насильственных экстремистов и террористов, и при этом представляют собой значительный ресурс с точки зрения имеющихся навыков, существующих методов, сетей и инфраструктуры. Образование имеет определяющее значение для целей прививания молодым людям положительных ценностей и навыков, необходимых им для того, чтобы достичь успехов в цифровую эпоху, и способно спровоцировать положительные изменения в обществе, поощряя молодых людей быть активными и вовлеченными гражданами в Интернете. Кроме того, хотя большинство взрослых не принимают непосредственного участия в формальной системе образования, в ней имеются косвенные каналы для охвата взрослого населения, помимо молодежи: например, посредством взаимодействия школ с родителями.

Настоящий раздел преимущественно сосредоточен на внедрении и реализации системы мер и программ ПБНЭ в начальной и средней школе, но также в нем представлены и практические примеры из сектора неформального образования. Кроме того, здесь рассматриваются методы, которые не направлены непосредственно на решение проблемы насильственного экстремизма и терроризма в Интернете, но способствуют распространению онлайн-безопасности и цифровой гражданственности в большем масштабе. Как и в случае со всеми прочими формами мер реагирования на основе коммуникаций, образовательные методы следует рассматривать в том контексте, для которого они были разработаны, и в соответствующих случаях адаптировать их надлежащим образом в целях устранения конкретных движущих сил радикализации и вербовки насильственными экстремистами и террористами на местном уровне. Аналогичным образом, следует принимать во внимание конкретные контекст и систему образования, в которых они изначально применялись, с учетом того, что между этими условиями могут существовать огромные различия в разных странах или даже внутри одной страны.

A. Разработка системы мер реагирования в сфере образования

Подход основанный на вовлечении всего общества

Как и в случае с мерами реагирования на основе коммуникаций в целом, государствам следует применять к мерам реагирования в сфере образования подход, основанный на участии всего общества, сводя вместе все соответствующие заинтересованные стороны и обеспечивая, чтобы их усилия дополняли национальную стратегию по предупреждению насильственного экстремизма и терроризма в сети Интернет и борьбе с ними. Государственные учреждения, сектор образования, гражданское общество, сообщества и семьи, а также частный сектор должны сотрудничать в целях определения того, каким образом можно эффективно использовать образование для формирования устойчивости, а также сокращения объемов вербовки и радикализации насильственными экстремистами и террористами. При разработке системы мер и программ также следует учитывать фактор пола, в соответствующих случаях принимая во внимание потенциально различные потребности молодых женщин и молодых мужчин. Госструктуры могут сыграть важную роль в поощрении и поддержке сотрудничества между образовательными учреждениями и широким спектром заинтересованных сторон в целях создания эффективных и устойчивых мер реагирования в сфере образования, с момента первого приглашения и вовлечения участников в проведение оценки потребностей до разработки, реализации и оценки соответствующих программ.

Учитывая возможные незапланированные последствия, связанные с затрагиванием щекотливых тем в образовательной среде, следует уделять особое внимание недопущению избыточного страхования сектора образования от рисков в ущерб эффективности образовательных методов. Государствам следует обеспечить использование надлежащей терминологии, а также принять меры к тому, чтобы инициативы в сфере

образования, направленные на предупреждение насильственного экстремизма и терроризма в сети Интернет и борьбу с ними, были структурированы и четко разъяснены, для гарантии участия в них всех соответствующих заинтересованных сторон, а также молодежи. Таким образом, чрезвычайно важно обеспечить полную прозрачность всех мер реагирования и методов в сфере образования с точки зрения источника их происхождения, финансирования и целей, чтобы гарантировать участие соответствующих сторон и избежать обострения уже существующего недовольства, которое группировки насильственных экстремистов и террористов могут использовать в своих целях.

Начальное, среднее и высшее образование

Все уровни образовательной системы могут сыграть определенную роль в прививании молодым людям положительных ценностей, формировании у них навыков и устойчивости и, в конечном итоге — в предупреждении последствий насильственного экстремизма и терроризма в сети Интернет и борьбе с ними. Многие когнитивные навыки, связанные с формированием ценностей и развитием критического мышления, развиваются в раннем детстве. В этой связи в начальной школе акцент должен быть сделан на более неявных методах, включая формирование положительных ценностей, таких многообразие и терпимость к позициям других людей, а также развитие базовых навыков онлайн-безопасности и раннего критического мышления. Консультации с родителями и другими членами семьи, а также их участие в этой работе имеет особое значение в условиях начальной школы, учитывая щекотливые темы, которые могут затрагивать такие методы.

В средней школе эффективными могут быть как явные, так и неявные методы — от методов, связанных с онлайн-безопасностью и ценностями, которые используются в начальной школе, до методов, в большей степени сосредоточенных на положительном поведении в Интернете и активной цифровой гражданственности, а также более непосредственно затрагивающих щекотливые темы, такие как ненависть, насилие, насильственный экстремизм и терроризм в Интернете. Аналогичные методы могут использоваться и в рамках системы высшего образования, при этом молодым людям должны предоставляться дополнительные возможности для участия в профилактической деятельности с учетом принятия ими на себя ответственности за положительные изменения в их соответствующих онлайн-сообществах.

Неформальное образование

Наряду с сектором формального образования, свой вклад в предупреждение последствий насильственного экстремизма и терроризма в сети Интернет и борьбу с ними на уровне местного сообщества могут внести неформальные образовательные пространства и методы. Неформальное образование может помочь закрепить знания, навыки, позиции и поведение, которым молодые люди учатся в условиях формальной образовательной системы. Кроме того, неформальное образование зачастую предусматривает возможность для реализации более широкого и гибкого круга образовательных методов, создавая тем самым важный путь оказания поддержки молодым людям, которые могут стремиться узнать больше в рамках формального образования, а также обеспечивая больше времени и пространства для деятельности за пределами основной учебной программы.

Вовлечение молодежи

Молодых людей следует рассматривать не только как лиц, уязвимых перед угрозой насильственного экстремизма и терроризма в Интернете, но и как основные заинтересованные стороны в разработке и реализации эффективных мер реагирования на основе коммуникаций в сфере образования. Многие молодые люди демонстрируют желание добиваться справедливости, способствовать положительным изменениям в мире, а также участвовать в жизни своих сообществ и обществ; их энергия, креативность и энтузиазм могут быть направлены в положительную сторону — на борьбу с разрушительными идеями насильственных экстремистских и террористических группировок в Интернете. Молодые люди зачастую знают об условиях и движущих силах, которые приводят их ровесников к радикализации и вербовке; кроме того, они способны

обеспечить эффективные коммуникации со своими ровесниками и представителями младших возрастных групп, а также оказать на них влияние.

В связи с этим государства и образовательные учреждения должны поощрять молодых людей к тому, чтобы они становились активными партнерами и кураторами молодежи в рамках работы по предупреждению насильственного экстремизма и терроризма в сети Интернет и борьбе с ними. Это может включать взаимодействие между молодежью и положительными ролевыми моделями или разработку методов, предусматривающих повышение молодыми людьми осведомленности своих родителей, других членов семьи и местных сообществ в области онлайн-безопасности, насильственного экстремизма или терроризма.

Вовлечение родителей и прочих взрослых

Комплексные образовательные методы также должны предусматривать вовлечение родителей, других членов семьи и прочих взрослых в целях повышения осведомленности об опасностях насильственного экстремизма и терроризма в Интернете и формирования устойчивости к таким опасностям. Государственные институты и образовательные учреждения, организации гражданского общества и представители частного сектора могут сотрудничать в целях предоставления ресурсов и возможностей для обучения в области гарантий, онлайн-безопасности, предупреждения насильственного экстремизма и терроризма в сети Интернет и борьбы с ними, а также распознавания возможных ранних признаков онлайн-радикализации.

Школы как пользующиеся доверием учреждения, имеющие сложившиеся отношения с местными сообществами, могут выступать в качестве площадок для реализации таких инициатив. Их также можно включить в любые существующие программы, направленные на вовлечение родителей и других членов семьи. Получив необходимые ресурсы и пройдя соответствующее обучение, родители и другие члены семьи смогут закреплять знания, полученные молодыми людьми в рамках формального или неформального образования, дома.

Вовлечение частного сектора

Государства могут поощрять частный сектор к введению программ корпоративной социальной ответственности (КСР) в поддержку мер реагирования в сфере образования. Такие меры могут включать обмен опытом, предоставление ресурсов и проведение обучения для молодых людей и прочих заинтересованных сторон или оказание поддержки в распространении ключевых сообщений в области онлайн-безопасности и реализации программ в этой сфере. Это может предусматривать создание новых программ или адаптацию существующих инициатив в сфере безопасности посредством включения в них контента или понятий, связанных с ПБНЭ. Частный сектор также может сыграть важную роль с точки зрения охвата аудиторий старшего возраста в Интернете, способствуя, таким образом, развитию критического мышления, дискуссии в целях достижения взаимопонимания, а также обеспечению онлайн-безопасности в аудиториях любых возрастов.

B. Спектр мер реагирования в сфере образования

Попытки насильственных экстремистов и террористов осуществлять радикализацию и вербовку в Интернете достигают успеха в отсутствие критического мышления, цифровой грамотности, а также осведомленности о развитии онлайн-пространства. В формировании устойчивости и сокращении уязвимости перед угрозой насильственного экстремизма и терроризма в сети Интернет, а также в получении критически важных знаний, развитии необходимых навыков, собственных позиций и поведения у молодых людей поможет широкий спектр образовательных методов. Хотя такие методы могут сильно различаться с точки зрения основных целей, зачастую они во многом решают одни и те же задачи или стремятся к достижению одних и тех же результатов обучения, несмотря на то, что такие цели, задачи и результаты в значительной степени зависят от контекста.

Невзирая на тип используемого метода, такие формы образования, как правило, достигают наибольшего

успеха в случае применения активного и экспериментального стиля обучения, а не более традиционных обучающих методов и методик. Такой стиль обучения может включать моделирование, игры, групповые упражнения и практическую деятельность, а также использовать различные виды носителей информации для привлечения и удержания внимания молодых людей.

Для целей настоящего инструментария, меры реагирования в сфере образования можно разделить на две широкие категории: «явные» и «неявные» методы предупреждения насильственного экстремизма и терроризма в сети Интернет и борьбы с ними:

- **Явные (или ориентированные на ПБНЭ) методы** непосредственно затрагивают темы насильственного экстремизма и терроризма и, как правило, больше подходят для учеников средней школы (или старше).
- **Неявные (или связанные с ПБНЭ) методы** косвенно направлены на основополагающие факторы, которые могут способствовать формированию устойчивости и сокращению уязвимости перед сообщениями насильственных экстремистов и террористов, а также перед прочими угрозами для молодых людей. Указанные методы можно надлежащим образом адаптировать для любой возрастной группы молодых людей и для любого уровня образования.

В таблице ниже (*таблица 2*) описывается ряд мер реагирования в сфере образования, включая соответствующий уровень образования, цели, задачи и результаты обучения по каждому из видов мер реагирования.

Таблица 2. Явные и неявные методы принятия мер реагирования в сфере образования

	Явные (ориентированные на ПБНЭ)	**Неявные (связанные с ПБНЭ)**	
Вид меры реагирования	Обучение в области ПБНЭ	Обучение в области цифровой грамотности и	Обучение в области онлайн-безопасности
Уровень образования	Среднее, высшее	Начальное, среднее, высшее	Начальное, среднее
Цели	Сформировать устойчивость к угрозе насильственного экстремизма и терроризма	Поощрять использование Интернета и социальных сетей в положительном ключе и сформировать устойчивость к угрозе насильственного экстремизма и терроризма в Интернете и прочим онлайн-угрозам	Поощрять безопасное и эффективное использование Интернета и социальных сетей
Задачи и результаты обучения (примерные)	Понимание опасностей насильственного экстремизма и терроризма в Интернете и осведомленность о таковых Навыки критического мышления Медиаграмотность и противостояние онлайн-пропаганде Тактика вхождения в доверие и вербовки Рассмотрение альтернативных точек зрения	Навыки критического мышления Медиаграмотность и визуальная грамотность Архитектура Интернета и онлайн-коммуникации (например, эхо-камеры и пузыри фильтров) Коллективная ответственность и гарантии для равных в Интернете Рассмотрение альтернативных точек зрения Цифровая гражданственность и активность	Неприкосновенность частной жизни и репутация в Интернете («цифровая гигиена») Управление онлайн-информацией и безопасностью Манипуляции в Интернете Взаимоотношения и запугивания в Интернете Самовосприятие и самочувствие в Интернете

«... в рамках курса по визуальной грамотности ученикам следует рассказать о силе изображений и о том, что изображения основаны на эмоциях, а не на суждениях. Необходимо подчеркнуть, что изображения не могут ничего доказать так, как слова

способны доказать суждение. Следует обсудить влияние различных шрифтов, оттенков, цветов и визуальных стилей, а также воздействие музыкального фона, чтобы ученики поняли их воздействие. Школам следует рассказать ученикам о стандартах, применяемых различными видами СМИ в отношении использования измененных изображений, чтобы они могли лучше судить об их действительности», R. Hornik, *A strategy to counter propaganda in the digital era*, Yearbook of the Institute of East-Central Europe, 2016, Volume 14, Number 2, pp. 61–74.

Как и в случае с другими формами мер реагирования на основе коммуникаций, государствам следует обеспечить, чтобы образовательные методы разрабатывались на основе существующих эмпирических доказательств; это позволит гарантировать эффективность изменений в учебных программах или новых программ с точки зрения предупреждения последствий насильственного экстремизма и терроризма в сети Интернет и борьбы с ними. Соответствующие меры могут включать базовые исследования, такие как оценка потребностей, изучение восприятия, анализ существующей учебной литературы и данные онлайн-статистики, а также разработку и оценку пилотных программ.

В качестве примеров программ обучения в области ПБНЭ с использованием явных методов можно назвать Bounce — образовательную программу, финансируемую Европейской комиссией и координируемую Федеральной государственной службой внутренних дел Бельгии, которая направлена на формирование устойчивости молодых людей к угрозе насильственного экстремизма.[153] Второй пример — это Extreme Dialogue, проект, финансируемый Министерством общественной безопасности Канады посредством проекта Kanishka[154], а затем — через программу ISEC ЕС.[155] Extreme Dialogue — это ресурс интерактивного образования для родителей, учителей и молодых сотрудников, уделяющий основное внимание убедительным видеоматериалам, в том числе с участием бывших насильственных экстремистов и выживших жертв насильственного экстремизма в Великобритании, Канаде, Германии и Венгрии.[156]

Наконец, в 2016 году российский *Национальный Центр информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет* запустил онлайн-ресурс, предоставляющий информацию о планируемых в стране мероприятиях по развитию активной гражданской позиции у детей и молодежи. Кроме того, в преддверии Чемпионата мира по футболу 2018 г. была запущена программа «нулевой дискриминации» в целях повышения уровня знаний у молодых людей в возрасте 14-21 лет и сокращения риска экстремистских и дискриминационных действий с их стороны посредством закрепления гуманистических ценностей с использованием примеров из области спорта и, в частности, футбола. В рамках программы применяется интерактивный подход, сосредоточенный на коротких тематических видеороликах и серии коллективных мероприятий, включая групповые задания и обсуждения.

C. Реализация мер реагирования в сфере образования

Учитывая тот факт, что образовательные методы предупреждения насильственного экстремизма и терроризма в сети Интернет и борьбы с ними являются относительно новыми, государства с большой вероятностью столкнутся с проблемами с точки зрения их эффективного масштабирования и широкого внедрения посредством системы образования. Партнерства с образовательными учреждениями и молодежными организациями, представителями гражданского общества и частного сектора имеют определяющее значение для увеличения масштаба применения и охвата таких методов. При выборе подходящего метода государствам следует тщательно проанализировать существующие навыки, потребности и требования специалистов по работе с молодежью.

[153] См. https://www.bounce-resilience-tools.eu/.

[154] См. https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/r-nd-flght-182/knshk/index-en.aspx.

[155] См. https://ec.europa.eu/home-affairs/financing/fundings/security-and-safeguarding-liberties/prevention-of-and-fight-against-crime_en.

[156] См. https://extremedialogue.org/.

Безопасные пространства

В целях обеспечения эффективности образовательных методов, школы, а также прочие образовательные учреждения и структуры следует сделать «безопасными пространствами», где можно высказывать, обсуждать и оспаривать идеи без риска вынесения определенных суждений относительно них, не подвергаясь дискриминации, притеснениям или угрозе причинения эмоционального или физического вреда либо фактическому причинению такого вреда. Метод такого типа следует ввести и стандартизировать как институциональный этос, чтобы создать возможность для изучения нескольких точек зрения и устранения любого недовольства открытым и безопасным способом.

Образовательным учреждениям и молодежным организациям следует рассмотреть возможность проведения обучения для своих преподавателей или сотрудников в области способов безопасного и эффективного вовлечения молодых людей в дискуссии на щекотливые темы, а также способов избежания дальнейшего отчуждения или повышения уязвимости какого-либо лица. Аналогичным образом, в условиях, когда молодые люди могут подвергнуться травмам или насилию (например, беженцы, жители территорий, где происходит/происходил конфликт), преподаватели или сотрудники должны держать в уме последствия, которые такие события могут иметь, и учитывать данный аспект в рамках своих методов и методик обучения.

Использование существующих навыков и ресурсов

С точки зрения затрагивания щекотливых тем, обучение, касающееся ПБНЭ, может быть связано и сопоставлено с существующими социальными проблемами и угрозами, которые уже известны преподавателям и специалистам по работе с молодежью. В зависимости от контекста, это может включать увязывание вопросов насильственного экстремизма и терроризма в сети Интернет с другими вопросами, уже изученными практикующими специалистами, такими как бандитизм и групповая преступность, наркотики и алкоголь, причинение травм, вхождение в доверие и запугивание в Интернете. Такой подход помогает убедить практикующих специалистов в том, что предупреждение насильственного экстремизма и терроризма в сети Интернет и борьба с ними может потребовать дополнительных знаний и понимания, но они уже обладают многими из необходимых навыков.

Также следует рассмотреть возможность обучения и предоставления ресурсов для сектора образования в целом, чтобы обеспечить поддержку методов ПБНЭ по всей системе. Такая деятельность может охватывать широкий спектр заинтересованных сторон, включая учителей, руководителей или администраторов школ, государственные или местные должностные лица (например, сотрудников министерств образования, культуры, спорта, религии), поставщиков услуг обучения и образования, инспекторов или регуляторов школ, ученых и исследователей, а также работников профессиональных органов. Программа обучения этих групп лиц может включать базовый обзор онлайн-угроз, цели и задачи конкретных или соответствующих подходов к ПБНЭ, основную терминологию и роли различных заинтересованных сторон в осуществлении совместных образовательных мер реагирования на проявления насильственного экстремизма и терроризма в Интернете в рамках подхода, основанного на участии всего общества.

Интеграция в учебную программу

Государственные учреждения (будь то национальные, региональные или местные, в зависимости от системы образования), как правило, имеют хорошие возможности для интеграции изменений в учебную программу для гарантии всестороннего реагирования на проявления насильственного экстремизма и терроризма в Интернете, чтобы охватить таким образом всех молодых людей посредством формального образования. В зависимости от степени, в которой связанные предметные области уже развиты, государства могут увеличить и расширить освещение тем, которые подчеркивают важность воспитания гражданской позиции или соблюдения прав человека в рамках связанного с ПБНЭ контента и результатов обучения или касаются указанных аспектов. Интеграция связанного с ПБНЭ контента в существующие предметные области поможет уменьшить нагрузку на преподавателей посредством связывания щепетильных тем с областями, о которых им комфортно

рассказывать, а также избежать перегрузки учебного плана и уплотнения рабочего графика преподавателей.

Мониторинг и оценка

Мониторинг и оценка имеют определяющее значение для демонстрации результатов и степени воздействия различных программ, а также помогают обеспечить участие в программах основных заинтересованных сторон (см. раздел 4 B. «Мониторинг и оценка мер реагирования на основе коммуникаций»). При наличии пробелов в доказательной базе государствам следует провести или поддержать междисциплинарные исследования по выявлению передовой практики и непрерывному совершенствованию мер реагирования, а также реализовывать поэтапную адаптацию мер реагирования по мере развития цифровой среды и изменения угроз. Учитывая относительный недостаток апробированных программ в этой области, за примерами передовой практики можно обратиться к другим областям и сферам, включая теорию обучения или педагогики. Государствам также следует обеспечить наличие правильных стимулов для поощрения поставщиков образовательных услуг к проведению анализа и критической оценки своих программ, а также к обмену полученным опытом по всему сектору.

Практический пример: Предупреждение экстремизма и радикализации и борьба с ними — Национальный план действий (Дания)[157]

Датский Национальный план действий описывает комплексный подход к предупреждению насильственного экстремизма и радикализации и борьбе с ними, который объединяет национальные и местные власти, различные ведомства, сектор образования и гражданское общество, с особым вниманием к детям и молодым людям. Профилактические методы преимущественно направлены на содействие благополучию и успешному развитию детей, а также на гарантирование такого благополучия и развития посредством поощрения активной гражданской позиции, формирования демократического, социального критического мышления и развития трудовых навыков, а также порицания «рискованного поведения» и повышения устойчивости молодежи к воздействию экстремистских сообщений.

Данный подход предусматривает участие заинтересованных сторон на национальном уровне (Министерство по делам детей, образования и гендерного равенства и Национальное агентство по вопросам образования и качества), на местном уровне (муниципалитеты), местных учреждений (отделы полиции, социальные службы и «инфодома», распространяющие имеющийся опыт борьбы с экстремизмом и радикализацией) и сектора образования (детские сады, начальная школа и старшие классы средней школы, а также программы образования для молодежи и взрослых). На местном уровне заинтересованные стороны объединяются в партнерства по предупреждению преступлений SSP (школы (Schools), социальные службы (Social services) и полиция (Police)). Национальное правительство поддерживает эту работу посредством проведения исследований, организации обмена опытом и знаниями, предоставления консультаций и обучения, а также разработки независимой оценки конкретных методов и инициатив в области обмена передовой практикой.

Формальное образование: учебная программа

Особое внимание в Национальном плане действий уделяется развитию навыков критического мышления у молодых людей и понимания ими концепции гражданской позиции в рамках целей национальной учебной программы (дат. Folkeskole) для начальной школы и младших классов средней школы. Это подразумевает включение тематики прав человека в курс обществознания (обязательного предмета, охватывающего вопросы здравоохранения, взаимоотношений в обществе и образования в семье), а также особое внимание к аспектам цифровой грамотности и умению работать с источниками информации на уроках датского языка и истории. Этим темам уделяется особое внимание в рамках ежегодной «тематической недели», которая проводится

[157] Udlændinge-og Integrationsministeriet, *Preventing and countering extremism and radicalisation National action plan?* last updated 15 March 2017 [Министарство иммиграции и интеграции Дании, *Национальный план действий по предупреждению экстремизма и радикализации и борьбе с ними*, дата последнего обновления: 15 марта 2017 г.]

Министерством по делам детей, образования и гендерного равенства, чтобы дополнительно подчеркнуть важность демократии, сообщества и гражданской позиции во всей структуре системы образования.

Формальное образование: обучение и ресурсы

Чтобы обеспечить успешное освещение этих важных тем в рамках учебного плана и эффективную практическую реализацию этой работы, работники всех уровней сектора образования, а также связанные с ним заинтересованные стороны (такие как муниципалитеты) проходят педагогическое и профессиональное обучение и получают ряд ресурсов. Это включает предоставление услуг «консультантов по вопросам обучения» через Национальное агентство по вопросам образования и качества, которые проводят серию мероприятий по всей территории Дании, посвященных передовой практике обучения в области демократии и гражданской позиции. Кроме того, в избранных школах был реализован пилотный проект по предупреждению преступлений на почве ненависти в целях разработки и апробирования дополнительных ресурсов для борьбы с запугиванием, отчуждением, предубеждениями и стереотипами среди молодых людей. В рамках проекта было проведено обучение для преподавателей и руководителей школ в области педагогики и содействия диалогу на щекотливые темы.

Национальное агентство по вопросам образования и качества разрабатывает и распространяет материалы посредством национального обучающего портала (www.emu.dk), который предоставляет преподавателям, руководителям школ и прочим практикующим специалистам конкретные ресурсы, чтобы поощрить использование методов предотвращения маргинализации и радикализации, а также сформировать устойчивость к экстремистским и террористическим сообщениям в Интернете. Это могут быть ресурсы в области критического мышления, пропаганды и манипуляции, а также ресурсы, посвященные онлайн-безопасности и цифровой грамотности, для начальных, средних школ и учреждений факультативного образования. Наконец, также доступны методы и ресурсы для школ по вопросам вовлечения в эту работу родителей.

Неформальное образование, молодежь и гражданское общество

Кроме того, Национальный план действий также предусматривает различные методы работы в условиях неформального образования, ориентированных на молодежь организаций гражданского общества и религиозных организаций, а также организацию различных видов деятельности для молодых людей. Обучение и ресурсы также предоставляются муниципалитетам: такое обучение и ресурсы посвящены порядку эффективного сотрудничества с местным гражданским обществом и молодежными организациями, а также совместному созданию конструктивных возможностей для вовлечения молодых людей.

Датское Агентство по международному найму и интеграции (SIRI) создало национальную инициативу диалога между равными для молодых людей (в возрасте от 18 до 35), чтобы организовать обсуждение молодежью важных тем, поощрить их независимость, а также создать у молодых людей чувство принадлежности местным сообществам и обществу в целом. Указанная инициатива охватывает широкий круг вопросов, включая «личность, взаимоотношения в семье, возможности для самовыражения, социальный контроль, конфликты чести, социальное участие, свобода и ответственность, права и обязанности, проообщественные и антиобщественные группы, дискриминацию и недискриминацию, образы друзей и врагов, нетерпимость, [и] экстремизм. Кроме того, было создано партнерство между национальным правительством и различными образовательными учреждениями в целях мобилизации молодых людей для борьбы с радикализацией в Интернете посредством распространения положительных и альтернативных идей в формате обучения цифровым коммуникациям.

Наряду с указанными инициативами, SIRI также предлагает обучение по наращиванию потенциала для местных организаций гражданского общества, молодежных организаций и практикующих специалистов в целях совершенствования их возможностей по разработке программ в области предупреждения экстремизма и радикализации и борьбы с ними, поощрения их положительного участия в жизни местных сообществ и

соответствующих мероприятиях, а также вовлечения в такие программы уязвимых или подверженных риску групп населения. В дополнение к этому обучению Медиасовет по вопросам детей и молодежи также разработал обучающие ресурсы, посвященные критическому мышлению и цифровой грамотности, в особенности в условиях неформального обучения.

Дополнительные ссылки

Раздел 1. Разработка и принятие связанных с контентом законодательства и политики

Australian Government, Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act, April 2019 [Правительство Австралии, Закон о внесении изменений в уголовный кодекс («Обмен вызывающими отвращение материалами со сценами насилия», апрель 2019 г.]

Government of the United Kingdom, Online Harms White Paper, April 2019 [Правительство Великобритании, Причинение вреда в Интернете. Официальный документ, апрель 2019 г.]

Government of France, Creating a French framework to make social media platforms more accountable: Acting in France with a European vision, May 2019 [Правительство Франции, Создание французской сети по обеспечению большей подотчетности платформ социальных сетей: деятельность во Франции с европейской точки зрения, май 2019 г.]

Раздел 2. Разработка механизмов обеспечения прозрачности и подотчетности

Committee of Experts on Internet Intermediaries, Study on the human rights dimensions of automated data processing techniques and possible regulatory implications, Council of Europe, 2017 [Комитет экспертов по интернет-посредникам, Исследование аспектов прав человека в рамках автоматизированных методик обработки данных и возможных последствий их использования, Совет Европы, 2017 г.]

Conway, Maura and, Moign Khawaja, Suraj Lakhani, Jeremy Reffin, Andrew Robertson & David Weir, Disrupting Daesh: Measuring Takedown of Online Terrorist Material and Its Impacts, Studies in Conflict & Terrorism, October 2018.

Jourová, Věra, Code of Conduct on countering illegal hate speech online: Fourth evaluation confirms self-regulation works, European Commission, February 2019.

Pearson, Elizabeth, Online as the New Frontline: Affect, Gender, and ISIS-Take-Down on Social Media, Studies in Conflict and Terrorism, July 2017,

Раздел 3. Реализация мер реагирования по контенту посредством многостороннего сотрудничества

Huang, Medea and Faris Natour, Legitimate and Meaningful: Stakeholder Engagement in Human Rights Due Diligence: Challenges and Solutions for ICT Companies, Business for Social Responsibility, September 2014.

Keen, Florence, Public–Private Collaboration to Counter the Use of the Internet for Terrorist Purposes: What Can be Learnt from Efforts on Terrorist Financing?' Royal United Services Institute for Defense and Security Studies, February 2019.

UNCTED, More Support Needed For Smaller Technology Platforms To Counter Terrorist Content, November 2018 [Исполнительный директорат Контртеррористического комитета Организации Объединенных Наций (ИДКТК

ООН), Для борьбы с террористическим контентом небольшим платформам требуется больше поддержки, ноябрь 2018 г.]

Tech Against Terrorism: Analysis, ISIS use of smaller platforms and the DWeb to share terrorist content, 2019.

Раздел 4. Разработка, принятие и оценка системы мер

Bhulai, Rafia, Allison Peters & Christian Nemr, From Policy to Action: Advancing an Integrated Approach to Women and Countering Violent Extremism, Global Center on Cooperative Security and Inclusive Security, June 2016.

Cox, Kate, William Marcellino, Jacopo Bellasio, Antonia Ward, Katerina Galai, Sofia Meranto & Giacomo Persi Paoli, Social media in Africa A double-edged sword for security and development, UNDP & RAND Europe.

& Giacomo Persi Paoli, Social media in Africa A double-edged sword for security and development, UNDP & RAND Europe.

Directorate General for Internal Policies, Policy Department C: Citizen's Rights and Constitutional Affairs, The European Union's Policies on Counter-Terrorism Relevance, Coherence and Effectiveness, January 2017 [Генеральный директорат по внутренней политике, Отдел по политическим вопросам С: права граждан и конституционные дела, Политика Европейского союза в сфере значимости, связности и эффективности деятельности по борьбе с терроризмом, январь 2017 г.]

Feve, Sebastian and Mohammed Elshimi, Planning for Prevention: A Framework to Develop and Evaluate National Action Plans to Prevent and Counter Violent Extremism, Global Center on Cooperative Security, June 2018.

G7, G7 Action Plan on Counter Terrorism and Violent Extremism, October 2016 [Группа семи, План действий Группы семи по борьбе с терроризмом и насильственным экстремизмом, октябрь 2016 г.]

GCTF, Ankara Memorandum on Good Practices for a Multi-Sectoral Approach to Countering Violent Extremism, 2013 [Глобальный контртеррористический форум, Анкарский меморандум о надлежащей практике многосекторного подхода к борьбе с насильственным экстремизмом, 2013 г.]

GCTF, Good Practices on Women and Countering Violent Extremism, 2014 [Глобальный контртеррористический форум, Надлежащая практика борьбы с насильственным экстремизмом с участием женщин, 2014 г.] Hedayah, Guidelines and Good Practices for Developing National CVE Strategies.

Hedayah, Guidelines and Good Practices: Developing National P/CVE Strategies and Action Plans, September 2016.

Hedayah, The World of Communications Is the New Frontline in The Battle Against Violent Extremism.

Herrington, Rebecca, Emerging Practices in Design, Monitoring, and Evaluation for Education for Peacebuilding Programming, Search for Common Ground, October 2015.

IMPACT Europe, Innovative Methods and Procedures to Assess Counter-violent-radicalisation Techniques in Europe: Toolkit Manual.

Khalil, James & Martine Zeuthen, Countering Violent Extremism and Risk Reduction: A Guide to Programme Design and Evaluation, Royal United Services Institute, June 2016.

RAN Centre of Excellence, Developing a local prevent framework and guiding principles - Part 2, November 2018.

RAN Centre of Excellence, Monitoring & Evaluating counter- and alternative narrative campaigns, February 2019.

Russell, Olivia, Meet Me At The Maskani: A Mapping of Influencers, Networks, and Communications Channels in Kenya and Tanzania, Search For Common Ground, June 2017.

Tuck, Henry & Louis Reynolds, The Counter-Narrative Monitoring & Evaluation Handbook, 2017.

UNDP & International Alert, Improving the impact of preventing violent extremism programming: a toolkit for design,

monitoring and evaluation, 2018 [ПРООН и International Alert, Улучшение воздействия программ по предупреждению насильственного экстремизма: инструментарий для разработки, мониторинг и оценка, 2018 г.]

United Nations General Assembly, Plan of Action to Prevent Violent Extremism Report of the Secretary-General, December 2015 [Генеральная Ассамблея Организации Объединенных Наций, План действий по предупреждению насильственного экстремизма, доклад Генерального секретаря, декабрь 2015 г.]

United Nations Office of Counter-Terrorism, Developing National and Regional Action Plans to Prevent Violent Extremism [Контртеррористическое управление Организации Объединенных Наций, Разработка национальных и региональных планов действий по предупреждению насильственного экстремизма]

United Nations Security Council, Letter dated 26 April 2017 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter- terrorism addressed to the President of the Security Council, April 2017 [Совет Безопасности Организации Объединенных Наций, Письмо от 26 апредя 2017 г. от председателя Комитета Совета Безопасности, учрежденного в соответствии с резолюцией 1373 (2001 г.) о борьбе с терроризмом,адресованное Президенту Совета Безопасности, апрель 2017 г.]

United Nations Security Council, Resolution 2354, May 2017 [Совет Безопасности Организацие Объединенных Наций, Резолюции 2354, май 2017 г.]

Раздел 5. Сотрудничество с представителями отрасли ИКТ и работа с ОГО

Bhulai, Rafia, Going Local: Supporting Community-Based Initiatives to Prevent and Counter Violent Extremism in South and Central Asia, December 2017.

Committee on Legal Affairs and Human Rights Council of Europe Parliamentary Assembly,Counter-Narratives to Terrorism, March 2018 [Комиссия по юридическим делам и по правам человека Парламентской ассамблеи Совета Европы,Контрпропаганда терроризма, март 2018 г.]

Department of Homeland Security, Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States, October 2016 [Министерство национальной безопасности США, Стратегический план реализации по расширению прав и возможностей местных партнеров в области предупреждения насильственного экстремизма в Соединенных Штатах Америки, октябрь 2016 г.]

Elsayed Lilah, Talal Faris & Sara Zeiger, Undermining Violent Extremist Narratives in the Middle East and North Africa: a how-to guide, Hedayah, December 2017.

GCERF, A Youth Perspective on Preventing Violent Extremism [Глобальный фонд взаимодействия и устойчивости, Перспективы вовлечения молодежи в работу по предупреждению насильственного экстремизма]

GCTF, Ankara Memorandum on Good Practices for a Multi-Sectoral Approach to Countering Violent Extremism, 2013 [Глобальный контртеррористический форум, Анкарский меморандум о надлежащей практике многосекторного подхода к борьбе с насильственным экстремизмом, 2013 г.]

Hemmingsen, Ann-Sophie & Karin Ingrid Castro, The Trouble with Counter-Narratives, Danish Institute for International Studies, 2017.

ICCT & Hedayah, Developing Effective Counter-Narrative Frameworks for Countering Violent Extremism, September 2014.

OSCE, The Role of Civil Society in Preventing and Countering Violent Extremism and Radicalisation that Lead to Terrorism: A Focus on South-Eastern Europe, August 2018 [Организация по безопасности и сотрудничеству в Европе, Роль гражданского общества в предупреждении насильственного экстремизма и радикализации, ведущим к терроризму, и борьбе с ними. Фокус на Юго-Восточной Европе, август 2018 г.]

RAN Centre of Excellence, A Nimble (NMBL) Approach to Youth Engagement in P/CVE.

RAN Centre of Excellence, Developing counter- and alternative narratives together with local communities, October 2018.

RAN Centre of Excellence, Guidelines For Young Activists: How To Set Up A P/CVE Initiative - Part 1: How to develop your own PVE initiative, March 2019.

RAN Centre of Excellence, Guidelines For Young Activists: How To Set Up A P/CVE Initiative – Part 2: How to develop a project plan for your P/CVE initiative, March 2019.

Reed, Alastair, Haroro J. Ingram & Joe Whittaker, Countering Terrorist Narratives, European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, November 2017.

Zeiger, Sara, Counter-Narratives For Countering Violent Extremism (CVE) In South East Asia, Hedayah, May 2016.

Zeiger, Sara, Undermining Violent Extremist Narratives in East Africa: A How-To Guide, Hedayah, August 2018.

Раздел 6. Расширение прав и возможностей молодежи и формирование устойчивости посредством обучения молодежи в области противодействия насильственному экстремизму и борьбы с ним, обеспечения онлайн-безопасности и цифровой гражданственности

Centre on Global Counterterrorism Cooperation, The Role of Education in Countering Violent Extremism, December 2013.

GCTF & Hedayah, Abu Dhabi Memorandum on Good Practices for Education and Countering Violent Extremism [Глобальный контртеррористический форум и центр Hedayah, Абудабский меморандум о передовой практике в области образования и борьбы с насильственным экстремизмом]

MediaSmarts, Use, Understand & Create: A Digital Literacy Framework for Canadian Schools, 2019.

National Society for the Prevention of Cruelty to Children (NSPCC) [Национальное общество предупреждения жестокости по отношению к детям], https://learning.nspcc.org. uk/.

RAN Centre of Excellence, Handbook on CVE/PVE training programmes: Guidance for trainers and policy makers, December 2017.

RAN Centre of Excellence, Education and radicalisation prevention: Different ways governments can support schools and teachers in preventing/countering violent extremism, May 2019.

RAN Centre of Excellence, Transforming schools into labs for democracy: A companion to preventing violent radicalisation through education, October 2018.

UNESCO, A Teacher's Guide on the Prevention of Violent Extremism, 2016 [ЮНЕСКО, Руководство для преподавателей по предупреждению насильственного экстремизма, 2016 г.]

UNESCO, Global Media and Information Literacy Assessment Framework: Country Readiness and Competencies, 2013 [ЮНЕСКО, Глобальная система оценки медиаграмотности и информационной грамотности; готовность и компетенции стран, 2013 г.]

UNESCO, Preventing violent extremism through education: a guide for policy-makers, 2017 [ЮНЕСКО, Предупреждение насильственного экстремизма посредством образования: руководство для лиц, ответственных за формирование политики, 2017 г] UNESCO, Youth and Violent Extremism on Social Media, 2017 [ЮНЕСКО, Молодежь и насильственный экстремизм в социальных сетях, 2017 г.]

UNESCO & Mahatma Gandhi Institute of Education for Peace and Sustainable Development, Youth Led Guide on Prevention of Violent Extremism Through Education, 2017 [ЮНЕСКО и Институт Махатмы Ганди по образованию в целях мира и устойчивого развития, Руководство для молодежи по предупреждению насильственного экстремизма посредством образования, 2017 г.]

Youth Led Guide on Prevention of Violent Extremism Through Education, 2017.

United Network of Young Peacebuilders & Search for Common Ground, Translating Youth, Peace & Security Policy into Practice: Guide to kick-starting UNSCR 2250 Locally and Nationally, November 2016.

UK Department for Education, Educate Against Hate [Министерство образования Великобритании, Образование против ненависти] UK Home Office, E-Learning Training on Prevent [Министерство образования Великобритании, Электронное обучение в области профилактики]

UK Department for Education, Thomas Chisholm & Alice Coulter (Kantar Public), Safeguarding and Radicalisation Research Report, August 2017 [Министерство образования Великобритании, Томас Чисхольм и Элис Култер (Kantar Public), Гарантии и исследования в области радикализации, доклад, август 2017 г.]

GCTF

GLOBAL COUNTERTERRORISM FORUM