Зарубежный опыт противодействия деструктивным сетевым исламистским и тюркско-исламистским структурам в сети Интернет

Круглова Анна Юрьевна — соискатель Института социологии и регионоведения Южного федерального университета, г. Ростов-на-Дону

Современные тенденции распространения деструктивных сетевых исламистских и тюркско-исламистских сетевых структур напрямую связаны с активным использованием боевиками широких возможностей информационно-коммуникационных технологий. Экстремисты и террористы прочно обосновались в глобальном информационном пространстве. По данным аналитиков, количество сайтов, содержащих материалы экстремистского и террористического толка уже значительно превышает 2 тысячи, причем концентрируются они не только в США и Германии, но и в Канаде, Австрии, Польше, Швеции, Австралии, Испании, Южной Африке, Украине и России и многих других. В этой связи возникает необходимость принятия государствами соответствующих мер противодействия, в том числе контроля интернет-пространства и интернет-аудитории [1, 2]. Формирование эффективной стратегии минимизации деятельности деструктивных сетевых исламистских и тюркско-исламистских структур в сети Интернет должно предусматривать ведение профилактической работы. К ее основным целям относится отслеживание и принятие мер по блокированию или ликвидации сайтов, на которых размещены материалы, активно пропагандирующие идеологию национализма, экстремизма и терроризма, призывающие к совершению преступлений экстремистской и террористической направленности против людей другого вероисповедания и национальности, а также содержащие детальные инструкции по изготовлению взрывных устройств с последующим их использованием для совершения террористических актов («виртуальный джихад»). В связи с этим проблемы предупреждения и пресечения экстремизма и терроризма в глобальном информационном пространстве сегодня являются актуальными для всех стран мирового сооб-

щества, о чем свидетельствуют принимаемые для их решения меры [3].

Сложность противостояния терроризму в интернете обусловлена рядом факторов [4]:

– пространство интернета крайне обширно – предугадать характер информации, время, место, автора и ее цель практически невозможно. Современные технологии позволяют лишь частично отследить первоочередную информацию. Однако ряд программных средств, доступных обычному пользователю, позволяют обойти и эти технологии. Кроме того, террористы могут использовать для загрузки своих материалов ресурсы, не требующие регистрационных данных, и популяризировать ссылки на них через социальные сети. В этом случае появляется масса пользователей, которые, просматривая новостные ленты, случайно получают доступ к тому или иному материалу.

– вероятность того, что опубликованный где-либо материал сразу же обнаружат и удалят, крайне мала.

– отсутствие единой законодательной базы, регулирующей интернет-контент.

В противовес этому от государства требуется постоянная модернизация и совершенствование программ борьбы с терроризмом. Более того, регулярный контроль интернет-пространства должен стать неотъемлемой частью противодействия.

Возросшие за последние десятилетия масштабы международного терроризма поставили большинство стран мира перед необходимостью разработки национальных антитеррористических систем. Во многих странах были сформированы специальные антитеррористические организации, которые могут кооперироваться с другими государственными ведомствами, чтобы не допустить пропаганды терроризма и, как следствие, терактов.

За рубежом организация противодействия терроризму представляет собой совокупность следующих составляющих [2]:

– правовое обоснование незаконности подобной деятельности;

– работа правоохранительных органов, специальных служб и ведомств в сфере обеспечения безопасности;

– деятельность специальных контртеррористических групп и национальных антитеррористических центров;

– разработка методологии противодействия экстремизму;

– проведение контртеррористических операций;

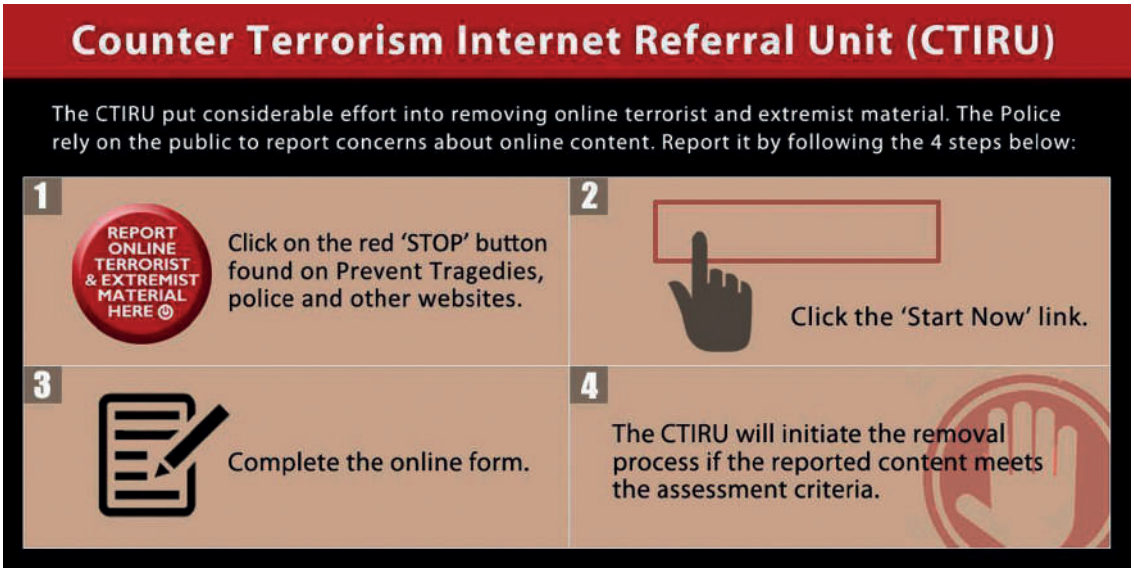
– работа служб, занятых ликвидацией последствий терактов;

– обеспечение тесного контакта со СМИ по вопросам борьбы с антитеррористической деятельностью;

– развитие соответствующей материально-технической базы (средства связи, новые компьютерные технологии и инфраструктурные элементы).

Больших успехов в сфере борьбы с экстремизмом и терроризмом в глобальном инфор-

мационном пространстве достигли Соединенные Штаты Америки. В стране функционирует большое количество организаций по противодействию проявлениям экстремизма и терроризма в интернет-пространстве. К ним относятся: национальный контртеррористический центр, командование боевых действий в кибернетическом пространстве (USCYBERCOM), центр стратегического контртеррористического взаимодействия. В задачи последнего входят меры по координации сотрудничества и взаимодействию с зарубежными странами в области борьбы с экстремизмом и терроризмом. Благодаря принятым мерам, в США, по сравнению с другими странами, осуществляется более эффективный контроль интернет-пространства. В общественных местах, где имеется свободный доступ в глобальную сеть, включая библиотеки и школы, применяются фильтры, которые ограничивают доступ к интернет-ресурсам, содержащим антиобщественную информацию, в том числе материалы экстремистского и террористического толка. С 2001 года в США действует закон о борьбе с терроризмом, в котором был введен новый документ – письмо-требование о раскрытии персональной конфиденциальной информации в целях национальной безопасности. Отличием письма от судебного ордера является то, что оно может быть написано ФБР или иной службой самостоятельно, без решения судьи. При наличии такого письма ФБР может получить доступ к любым данным пользователя и запретить руководству компании сообщать ему об этом. С 2016 года Вашингтон в целях выявления и недопущения въезда в страну лиц, связанных с террористическими организациями, такими как ИГ, начала предлагать иностранным гражданам, при-



бывающим в США в рамках программы безвизового въезда, указывать данные об аккаунтах в соцсетях [5].

Правительство Германии, несмотря на то, что большинство законодательных ограничений утверждаются при значительном противостоянии со стороны общественности и компаний, деятельность которых связана с компьютерными технологиями, уделяет серьезное внимание вопросам противодействия пропаганды экстремистских и террористических идей в интернет-пространстве. С начала 2007 года в ФРГ действует закон, в соответствии с которым регистрация электронной почты на вымышленное лицо расценивается как преступление. В январе 2007 года в правоохранительных органах Германии была создана специальная группа, в обязанности которой входит выявление случаев радикальной исламистской пропаганды, а также анализ работы отдельных интернет-ресурсов, представляющих потенциальную опасность. В октябре 2017 года в стране вступил в силу закон, согласно которому на социальные сети, например, такие как Facebook, Twitter и YouTube, будут налагаться штрафы на сумму до 50 млн евро за систематическое несвоевременное удаление публикаций, содержащих материалы или новости, разжигающие ненависть [1].

В Великобритании законодательный акт, касающийся неправомерного использования компьютерных технологий, был принят в 1990 году. С 2006 года в стране был увеличен срок тюремного заключения за хакерские атаки, направленные на взлом сайтов правительственных организаций и банков до десяти лет. Эффективно функционирует созданная правоохранительными органами Великобритании доктрина противодействия экстремиз-

му и терроризму в глобальной сети. Британское Национальное подразделение по борьбе с терроризмом в сфере Интернета (CTIRU) разместило обращение к населению с просьбой сообщать о наличии в сети материалов, содержащих информацию экстремистского и террористического толка. Для этого на веб-ресурсах действует красная кнопка «Стоп». При нажатии пользователем данной кнопки провайдеры незамедлительно перенаправляют его на специальный сайт, где просят ввести адрес веб-страницы, на которой был обнаружен подозрительный материал на условиях анонимности. CTIRU анализирует и проверяет полученную информацию и в течение 36 часов осуществляет удаление материала, если он признается экстремистским. CTIRU работает в постоянном сотрудничестве с провайдерами, что позволило ему добиться высоких результатов. Так, за период с 2010 года по 2017 год из интернета было изъято более 160 тысяч материалов экстремистского и террористического толка. Данные статистики свидетельствует, что активность участия населения в работе CTIRU с каждым годом увеличивается. В Великобритании ведется и информационно-пропагандистская работа в данном направлении. Например, организована работа интернет-сайта, на страницах которого представлен обзор стратегии деятельности полиции графства Суррей по противодействию экстремизму. На сайте регулярно размещается конкретная информация о том, как отдельные граждане, являющиеся членами местного сообщества, могут оказать помощь полиции в ликвидации угроз терроризма и экстремизма [6].

28–29 августа 2018 года пятью странами (Австралия, Великобритания, Канада, Новая Зеландия и США) разведывательного альянса «Пять глаз», был подписан меморандум, в котором они призывают ИТ-компании обеспечить доступ к зашифрованным данным своих пользователей. В случае несогласия компаний страны альянса намерены принять меры, чтобы заставить их сотрудничать. В 2013 году Эдвард Сноуден опубликовал материалы, в которых указал, что власти государств разведывательного альянса «Пять глаз» ведут слежку за гражданами других стран-участниц и обмениваются полученной информацией. Таким образом, им удается обойти национальные ограничения на слежку каждого правительства за собственными гражданами [1].

В Израиле целенаправленную работу по профилактике терроризма и экстремизма осуществляют некоторые неправительственные организации. Среди них Международный институт по противодействию терроризму (International Institute for Counter-Terrorism) – израильская общественная организация, предоставляющая информацию об истории терроризма, о современном положении дел, уровне угрозы, ме-

тодах и способах борьбы, а также о принимаемых на государственном уровне решениях. Популяризация методического пособия «Все, что нужно знать о терроризме», подготовленного этим институтом, не только привлекает внимание к проблеме, но и систематизирует представление населения об особенностях проявления терроризма в Израиле. Согласно некоторым утверждениям, деятельности израильских общественных контртеррористических организаций присущ пропагандистский характер, они стремятся донести до аудитории мысль о недопустимости пособничества террористам, а также об угрозе «гражданской халатности» – нежелании населения беспокоится о своей безопасности и безопасности окружающих [7].

В Индии существует несколько спецслужб, которые отслеживают террористическую деятельность не только внутри страны, но и за рубежом. Аналитический и исследовательский отдел (Research and Analysis Wing) является подразделением внешней разведки, а разведывательное бюро (Intelligence Bureau) – подразделением внутренней разведки. Указанные подразделения, в частности, отслеживают интернет-пространство на предмет появления в нем ненадлежащей информации или активизации нехарактерной деятельности. Кроме того, существует антитеррористическое отделение полиции (Anti-Terrorism Squad), у которого есть определенная зона контроля [6].

Полезно также будет рассмотреть систему блокирования интернет-угроз в странах СНГ. Так, например, в Республике Беларусь Президент страны Александр Лукашенко 1 февраля 2010 года подписал указ № 60 «О мерах по совершенствованию использования национального сегмента сети Интернет», призванный защитить, прежде всего, рядовых пользователей от деструктивного воздействия экстремистских сайтов и пропаганды терроризма в сети Интернет. По мнению бе-

лорусского правительства, одним из основных способов донесения идей антитеррористической борьбы до широкой общественности являются СМИ, которые уделяют особое внимание содержанию сообщений, посвященных террористической и антитеррористической тематике [6].

В Республике Казахстан также большое внимание уделяют информационной безопасности в интернет-пространстве. В республике существует закон, приравнивавший все интернет-ресурсы к СМИ, которые стали нести уголовную и гражданскую ответственность наравне с традиционными средствами массовой информации. Действие закона от 10 июля 2009 года № 178-IV «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам информационно-коммуникационных сетей» распространилось на сайты, блоги, чаты, интернет-магазины, электронные библиотеки и др. Данная норма позволяет судебным органам требовать от владельцев сайтов удаления материалов, которые идут вразрез с законодательством [6].

Обобщив опыт противодействия деструктивным исламистским и тюркско-исламистским сетевым структурам в зарубежных странах стоит отметить, что вне зависимости от того, какие силы и средства станут применяться в качестве мер противодействия, с противоположной стороны всегда следует ожидать контрмеры, на которые соответствующие органы и ведомства должны дать адекватный ответ. Таким образом, одной из главных задач современности остается недопущение распространения идей террористической и экстремистской идеологии и, как следствие, самих терактов, межконфессиональных и этнонациональных конфликтов.

Литература и ссылки:

1. Бураева Л. А. Кибертерроризм как новая и наиболее опасная форма терроризма //Пробелы в российском законодательстве. 2017.№ 3. С. 35–37.

2. Дадова З. И. Социализация молодёжи как фактор предупреждения экстремистских и террористических идей и настроений // Социально-политические науки. 2018. № 3. С. 62-64.

3. Бураева Л. А. Зарубежный опыт противодействия экстремизму и терроризму в интернет-пространстве // Противодействие терроризму в интернете. 2018, № 4. С. 283.

4. Акопян О. А. Противодействие терроризму как общая задача властей и граждан. Зарубежный опыт // Национальный институт развития современной идеологии. М., 2016. С. 45.

5. Европейский опыт противодействия экстремизму URL: http://49e.ru/ru/2013/8/8 (дата обращения: 29.04.2020г.).

6. Завьялов С. Зарубежный опыт в области борьбы с пропагандой терроризма в интернете // Зарубежное военное обозрение. 2014. №4. С. 34–39.

7. Искусство борьбы с терроризмом в Израиле URL: https://crss.uz/2018/12/25/iskusstvo-borby-s-terrorizmom-v-izraile/ (дата обращения: 29.04.2020 г.).