Вестник Национального антитеррористического комитета N 1[12] 2015

И.Ю. Сундиев — доктор философских наук, профессор;

А.А. Смирнов — кандидат юридических наук, доцент

Глобальная информационная сеть Интернет является наиболее значимым фактором развития информационного общества на современном этапе. Ее территориальное проникновение и популярность среди пользователей стремительно возрастают. По данным Международного союза электросвязи (ITU), число пользователей Интернета в мире в 2013 году превысило 2,7 млрд человек, что составляет 39 % мирового населения[1].

Увеличивающаяся востребованность Интернета обусловливается предоставляемыми им беспрецедентными информационными и коммуникационными возможностями. Последние во многом обеспечиваются технологическими разработками, которые принято обозначать термином Web 2.0. (второе поколение интернет-технологий), ключевыми из которых являются социальные сети.

Количество активных пользователей самой популярной в мире социальной сети Facebook по итогам 2013 года превысило отметку в 1,2 млрд. человек ежемесячно[2].

В последние годы получил развитие такой технологический тренд, как «Интернет вещей», основу которого составляют использование интернет-протокола для объединения различных устройств в единую вычислительную сеть, в рамках которой они способны обмениваться информацией между собой. Все более широкое применение в повседневной жизни находят носимые компьютерные устройства, подключенные к сети Интернет, начиная от «умных часов» (smart watch) и заканчивая нательными компьютерами (устройство «Google Glass» и т.п.).

Наряду с правительствами, предприятиями, общественными объединениями и простыми гражданами, возможности Интернета активно осваивают и террористические организации. Автор известного доклада «Как современные террористы используют Интернет?» Габриэль Вейман называет Интернет идеальной средой для деятельности террористов, чему способствуют следующие особенности глобальной сети: а) свобода доступа; б) минимальное регулирование, цензура и другие формы государственного контроля или вовсе их отсутствие; в) потенциально огромная аудитория во всем мире; г) анонимность связи; д) быстрое движение информации; е) невысокая стоимость создания сайта и обслуживания присутствия в сети; ж) мультимедийная среда, позволяющая комбинировать текст, графику, аудио и видео, возможность загружать фильмы, песни, книги, постеры и т.д.; з) возможность охватить также аудиторию традиционных СМИ, которые все чаще используют Интернет как источник сообщений[3].

История террористической деятельности в киберпространстве началась в конце 1990-х годов. В настоящее время Интернет рассматривается многими террористическими и экстремистскими формированиями как один из ключевых инструментов реализации своих противоправных целей. «Завоевание информационного пространства — такова первоочередная задача, которую пытаются решить современные террористические организации», — отмечает российский исследователь В.А. Гарев[4].

Как показало проведенное ФГКУ «ВНИИ МВД России» в 2013 году исследование, основанное на изучении материалов деятельности Главного управления по противодействию экстремизму МВД России (далее — ГУПЭ МВД России) и его территориальных подразделений, начало активного использования Интернета террористическими и экстремистскими организациями в нашей стране относится к началу 2000-х годов. В дальнейшем развитие данного процесса шло в геометрической прогрессии. Отмеченная негативная тенденция сохраняется и в настоящее время, при этом она корреспондируется с развитием киберпреступности в нашей стране.

Характеристика основных направлений и способов использования Интернета в террористических целях

В использовании Интернета террористическими организациями можно выделить два главных направления: обеспечивающее (пропаганда, планирование и координация, финансирование и др.) и кибертерроризм.

Более детальная классификация содержится в научных работах. Так, Г. Вейман выделил восемь способов использования Интернета террористами: 1) ведение психологической войны; 2) поиск информации; 3) обучение; 4) сбор денежных средств; 5) пропаганда; 6) вербовка; 7) организация сетей; 8) планирование и координация террористических действий[5]. Схожий перечень приводится в докладе Управления ООН по наркотикам и преступности (далее — ЮНОДК) «Использование Интернета в террористических целях»: 1) пропаганда (в т.ч. вербовка, радикализация и подстрекательство к терроризму); 2) финансирование; 3)

подготовка террористов; 4) планирование (в т.ч. с использованием секретной связи и открытых источников информации); 5) исполнение; 6) кибератаки[6].

Рассмотрим характеристику основных направлений использования Интернета в деятельности террористических организаций, сохранив авторскую классификацию на основе интеграции представленных подходов.

Пропаганда, вербовка и подстрекательство

Оценивается как приоритетное направление использования Интернета террористами. Основные цели состоят в максимально широком распространении своих идей среди населения, оказании психологического воздействия на целевые группы (сторонников, реальных или потенциальных жертв, правительство, международное сообщество), вовлечении новых участников в деятельность террористических формирований. В качестве примера можно привести «Аль-Каиду», идеологи которой подчеркивают важность последовательного ведения т.н. «медиа джихада»[7].

Распространение идей терроризма и экстремизма через информационно-телекоммуникационную сеть Интернет и средства массовой информации названо в числе основных внешних факторов, способствующих возникновению и распространению терроризма в Российской Федерации, в Концепции противодействия терроризму в Российской Федерации, утвержденной Президентом Российской Федерации 5 октября 2009 года.

Обычно пропагандистские материалы имеют форму мультимедийных коммуникаций, содержащих идеологические или практические наставления, разъяснения, оправдания или рекламу террористической деятельности. К ним могут относиться виртуальные сообщения, презентации, журналы, теоретические работы, аудио- и видеофайлы, а также электронные игры, разрабатываемые террористическими организациями или их сторонниками. К основным источникам пропаганды в сети Интернет относятся разнообразные интернет-сайты (прежде всего собственные сайты террористических организаций, такие, например, как «ИсламДин» — «Официальный сайт Имарата Кавказ КБК»); интернет-форумы различной направленности, блогосфера, социальные сети и видеохостинги.

Широкая область влияния распространяемой через Интернет информации значительно увеличивает аудиторию, на которую она может воздействовать. Для обеспечения большей доступности террористические группы создают многоязычные сайты.

Ресурсы Интернета активно используются в деятельности экстремистских и террористических организаций для привлечения новых участников. Совокупная аудитория Интернета обеспечивает данным организациям глобальный резерв потенциальных новобранцев. Для целей вербовки могут использоваться как информационные сайты террористов, так и коммуникационные веб-платформы: чаты, блоги, социальные сети, IP-телефония и мессенджеры, электронная почта. Еще одним средством вовлечения сторонников (особенно несовершеннолетних) в террористическую деятельность могут служить онлай-новые компьютерные игры, предусматривающие выполнение «заданий» не только в виртуальном пространстве, но и в реальной жизни (совершение актов насилия, погромов, иных действий по устрашению). В последнем случае можно говорить уже о подстрекательстве к совершению преступлений террористического характера. Хотя чаще оно осуществляется посредством индивидуального общения в Интернете с потенциальным исполнителем теракта с целью склонения его к реализации задуманного. Как правило, для этого используются «приватные» инструменты коммуникации, такие как закрытые чаты, электронная почта и IP-телефония.

Промежуточной ступенью между первичной вербовкой и непосредственно подстрекательством к совершению теракта является психологическая обработка неофита с целью привития ему экстремистских взглядов и обеспечения готовности к активным действиям («радикализация»).

Подготовка (обучение) террористов

Террористические организации активно используют Интернет для подготовки завербованных новобранцев и действующих членов незаконных вооруженных формирований. С учетом доминирования сетевого типа структуры таких организаций, включающих территориально распределенную сеть подпольных ячеек, именно Интернет предоставляет возможность простого и безопасного доступа к учебным материалам террористического характера.

Интернет обеспечивает возможность широкого распространения учебно-методической литературы и мультимедийных обучающих материалов, касающихся тактики подготовки и совершения терактов, самодельного изготовления оружия и взрывных устройств, сбора необходимой информации, обеспечения защиты используемых каналов коммуникации и т.п. Как отмечается в исследовании, были обнаружены виртуальные учебные лагеря, предоставляющие инструкции по использованию оружия в форме дистанционного электронного обучения[8].

Еще одной «инновационной» формой обучения террористов являются онлайн-инструктажи, проводимые посредством использования интернет-телефонии.

Планирование и координация деятельности

Данное направление включает в себя несколько составляющих. Одной из них является использование Интернета для сбора информации из открытых источников о потенциальных объектах террористической атаки, возможных орудиях и средствах ее совершения. Может включать в себя применение популярных интернет-сервисов, в частности геоинформационных ресурсов (например, Google Earth) и социальных сетей (например, Facebook).

Другим аспектом является использование Интернета в качестве канала коммуникации (связи) между различными ячейками террористической организации или отдельными ее членами как в «повседневной» деятельности, так и при планировании и осуществлении конкретного теракта. Для этих целей задействуются интернет-мессенджеры, электронная почта, IP-телефония. Например, было установлено, что исполнители теракта 11 сентября 2001 года в США использовали электронную почту для координации своих действий. В целях конспирации террористы активно применяют методы обеспечения анонимности в Интернете, такие как шифрование трафика, программы-анонимайзеры и стеганографию (сокрытие сообщений в графических изображениях).

Кроме того, Интернет может использоваться для совершения онлайн-покупок материалов и средств, необходимых для совершения теракта.

Финансирование

Террористические организации используют возможности Интернета для финансового обеспечения своей деятельности. Оно включает в себя несколько способов сбора средств:

а) сбор пожертвований — осуществляется путем прямых призывов о пожертвовании средств, размещаемых на веб-сайтах, в чатах, социальных сетях или распространяемых посредством массовых рассылок;

б) электронную торговлю — реализуется посредством организации интернет-магазинов, предлагающих информационные материалы (книги, аудио- и видеозаписи), символику и атрибутику и т.д.;

в) использование платежных систем в Интернете — предполагает применение данных систем для электронного перевода средств террористическим организациям, а также совершение актов интернет-мошенничества с помощью таких приемов, как хищение личных данных, кража кредитных карт и т.д.;

г) посредничество благотворительных организаций — включает создание фиктивных «благотворительных» организаций для сбора средств или внедрение в существующие организации для оказания поддержки террористическим формированиям.

Кибератаки на информационные системы (кибертерроризм)

Данное направление включает прямое использование ресурсов Интернета в качестве средства совершения террористических атак против объектов инфраструктуры. Под кибертерроризмом, как правило, понимают действия по дезорганизации информационных систем, создающих опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных общественно опасных последствий, если они совершены в целях нарушения общественной безопасности, устрашения населения либо оказания воздействия на принятие решения органами власти, а также угроза совершения указанных действий в тех же целях[9]. Орудием кибертеракт выступает вредоносное программное обеспечение. По данным Международного института антитеррористической политики (International Policy Institute for Counter-Terrorism), террористы уже использовали или в состоянии использовать такие виды «кибероружия», как компьютерные вирусы, «черви» и «троянские кони», «логические бомбы».

Ключевой целью кибертеррористов выступают системы управления критически важными объектами инфраструктуры (транспорт, атомная энергетика, электросети и т.д.), нарушение работы которых может повлечь значительные негативные последствия. Причем последние не ограничатся самими атакованными компьютерными системами, а затронут объекты жизнеобеспечения городов (электроэнергетические сети, систему теплоснабжения), авиа-, морского, речного и железнодорожного транспорта, атомной энергетики и т.д., что наглядно продемонстрировал вирус Stuxnet. Развитие «Интернета вещей» усиливает круг потенциальных объектов кибератак и повышает их уязвимость.

Еще одной формой кибертерроризма следует считать хакерские атаки на правительственные и корпоративные сайты с целью блокирования их работы либо размещения на них пропагандистской информации. Такие атаки получили широкое распространение в мире.

Таким образом, использование Интернета в террористических целях представляет собой достаточно разнообразное и многоаспектное явление, включающее в себя ряд направлений и способов. Многие из них уже стали частью «обыденной» деятельности террористических организаций, другие — перспектива ближайшего будущего. В этих условиях важное значение приобретает задача выработки системы мер противодействия данным угрозам. Президент Российской Федерации В.В. Путин на расширенном заседании коллегии МВД России 21 марта 2014 года подчеркнул необходимость пресекать пропаганду ненависти и радикализма, в т.ч. в Интернете или с помощью других информационных технологий и ресурсов[10].

Одним из важнейших направлений выступает информационное противодействие терроризму (далее — ИПТ), под которым нами понимается система информационно-пропагандистских, правовых, организационных и иных мер, направленных на предупреждение и блокирование негативного информационно-психологического воздействия террористических организаций на общество или личность, а также использование информационно-коммуникационных технологий в деструктивной деятельности данных организаций и их участников. Информационное противодействие терроризму рассматривается в Концепции противодействия терроризму в Российской Федерации в числе задач его предупреждения (профилактики).

Сеть Интернет является приоритетной сферой реализации мер ИПТ. Важнейшим принципом ИПТ является системность осуществляемых мер, что предполагает выработку целостной стратегии, в которой необходимо определить субъекты, принципы, методы и средства данной деятельности. Полагаем, что все перечисленные элементы должны найти отражение в соответствующем акте стратегического планирования Российской Федерации.

Ключевыми государственными органами в механизме ИПТ в сети Интернет являются МВД России и ФСБ России, а также Минкомсвязь России и подведомственный данному министерству Роскомнадзор. Учитывая трансграничный характер сети Интернет, важную роль в ИПТ на международной арене, помимо указанных ведомств, выполняют МИД России и СВР России.

Особое место среди субъектов ИПТ отводится Национальному антитеррористическому комитету (НАК), в составе которого имеется Информационный центр, выполняющий функции информационно-пропагандистского сопровождения деятельности по противодействию терроризму, информирования населения об угрозах терроризма и контрпропаганды. Официальный сайт НАК является мощным инструментом противодействия распространению идеологии терроризма.

Считая существующую систему государственных органов ИПТ вполне достаточной для решения обозначенных выше задач, полагаем, что основным вектором ее совершенствования должно стать увеличение потенциала и возможностей этих органов по ИПТ. Оно предполагает обучение их личного состава, материально-техническое оснащение, создание необходимых правовых основ деятельности.

Важную роль в системе ИПТ в сети Интернет должны играть негосударственные субъекты — общественные объединения, СМИ, владельцы и администраторы интернет-сайтов, блогеры и иные пользователи Интернета. Роль государства здесь видится не в дирижировании деятельностью негосударственных акторов (это невозможно в силу их численности), а в активном сотрудничестве с ними в рассматриваемой сфере деятельности, применении методов стимулирования общественно полезной гражданской активности. Считаем целесообразным активно задействовать в рассматриваемой области возможности привлечения к решению отдельных задач по ИПТ неопределенного круга лиц на основе использования интернет-платформ (краудсорсинг)[11].

Формы такого краудсорсинга могут быть самыми разнообразными: от проведения интернет-конкурсов плакатов антитеррористической направленности до организации синхронных массовых акций по рассылке сообщений в социальных сетях.

Основными средствами ведения ИПТ в сети Интернет выступают:

официальные интернет-сайты правоохранительных и иных государственных органов;

сайты СМИ в сети Интернет;

иные информационные интернет-ресурсы;

социальные сетевые интернет-ресурсы;

компьютерные сетевые игры;

специализированные компьютерные программы;

средства защиты информационных систем от компьютерных атак.

Методы ИПТ в сети Интернет весьма многообразны.

Первую их группу составляют методы поискового и информационно-аналитического характера, которые направлены на обнаружение, сбор и анализ сведений об информационной деятельности террористических организаций и включают проведение научных исследований, оперативно-разыскных, разведывательных и контрразведывательных мероприятий, осуществление мониторинга информационных ресурсов террористических организаций в сети Интернет (сайты, блоги, сообщества в социальных сетях), а также последующий анализ полученных сведений.

Вторую группу составляют административные методы ИПТ в сети Интернет, направленные на предотвращение и пресечение пропаганды идеологии терроризма, распространения экстремистских материалов через сеть Интернет, привлечение к юридической ответственности виновных в совершении данных деяний физических и юридических лиц. Помимо апробированных правовых инструментов, предусмотренных федеральными законами «О противодействии терроризму» и «О противодействии экстремистской деятельности» (вынесения предупреждения о недопустимости распространения экстремистских материалов и осуществления экстремистской деятельности, прекращение деятельности СМИ, приостановление оказания услуг связи юридическим и физическим лицам или ограничение использования сетей связи и средств связи в условиях КТО и т.д.), с 1 февраля 2014 года запущен новый механизм ограничения доступа к информации экстремистского содержания в сети Интернет, введенный в действие Федеральным законом от 28 декабря 2013 года N 398-ФЗ «О внесении изменений в Федеральный закон „Об информации, информационных технологиях и о защите информации"». Им предусматривается алгоритм ограничения доступа к информации, содержащей призывы к осуществлению экстремистской деятельности, который применяется Роскомнадзором во взаимодействии с операторами связи по требованию прокуратуры. В эту же группу входят меры уголовной и административной ответственности за совершение правонарушений в сети Интернет членами террористических организаций.

Однако в связи с заведомой ограниченностью эффективности мер фильтрации информации в Интернете наиболее важное значение в системе мер ИПТ имеют методы пропаганды и контрпропаганды в киберпространстве. Они включают в себя распространение официальных информационных сообщений в сети Интернет, проведение брифингов или пресс-конференций для интернет-СМИ, создание специализированных интернет-сайтов антитеррористической направленности, подготовку и распространение контента контрпропагандистского характера, участие в дискуссиях на форумах и в социальных сетях.

Особое внимание необходимо уделять дискредитации в общественном сознании организаторов и членов террористических организаций, разоблачению их истинных намерений, вскрытию источников и каналов финансирования и информационной поддержки.

Именно в рамках данной группы методов целесообразно использование механизмов краудсорсинга для максимально широкого вовлечения пользователей Интернета в проведение пропагандистской работы в киберпространстве.

Учитывая, что ее основной целевой аудиторией выступает молодежь, целесообразно использовать в этих целях «таргетированный» на нее интернет-контент (видеоролики, аудиозаписи, демотиваторы и прочие плакаты (изображения), компьютерные игры, анекдоты, заготовленные интернет-мемы и т.п.). Наряду с деятельностью гражданского общества требуется реализация комплекса мер со стороны государственных органов.

Угроза кибертерроризма требует применения организационно-технических методов по защите критически важных объектов инфраструктуры от компьютерных атак. Данное направление деятельности относится к обеспечению информационной безопасности и требует отдельного рассмотрения. Здесь же ограничимся тезисом о необходимости включения обозначенного информационного аспекта уязвимости в перечень критериев оценки антитеррористической защищенности критически важных объектов инфраструктуры.

---

[1]Мир в 2013 году. Факты и цифры, касающиеся ИКТ // Международный союз электросвязи: официальный сайт. URL:http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013-r.pdf (дата обращения: 15.03.2014).

[2]Ежемесячная аудитория Facebook превысила 1,2 миллиарда пользователей // Лента.Ру. 30 января 2014. URL:http://lenta.ru/news/2014/01/30/somenumbers (дата обращения: 15.03.2014).

[3]Вейман Г. Как современные террористы используют Интернет? Специальный доклад No 116 // Центр исследования компьютерной преступности. URL: http://www.crime-research.ru/analytics/Tropina_01/ (дата обращения: 12.04.2013).

[4]Гарев В.А. Информационные угрозы современного международного терроризма. М. : Институт Африки РАН, 2010. С. 6.

[5]Мир в 2013 году. Факты и цифры, касающиеся ИКТ // Международный союз электросвязи : официальный сайт. URL:http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013-r.pdf (дата обращения: 15.03.2014).

[6]Использование Интернета в террористических целях. Управление Организации Объединенных Наций по наркотикам и преступности, 2013. С. 3-12.

[7]Горбатова В.В. Информационно-пропагандистская политика радикальных исламских организаций (на примере Хамас, «Хизбаллы» и «Аль-Каиды») : Автореф. дис. ... канд. полит. наук. М., 2013. С. 24.

[8]Герке М. Понимание киберпреступности: явление, задачи и законодательный ответ / Международный союз электросвязи, 2012. С. 37.

[9]Федоров А.В. Информационная безопасность в мировом политическом процессе: Учеб. пособие. М. : МГИМО, 2006. С. 111.

[10]Расширенное заседание коллегии МВД России // Президент Российской Федерации : официальный сайт. 21 марта 2014 года. URL: http://www.kremlin.ru/news/20624 (дата обращения: 21.03.2014).

[11]Демидов О. Социальные сетевые сервисы в контексте международной и национальной безопасности // Индекс безопасности. 2013. No 1 (104). С. 65-86.

Информация с сайта http://nac.gov.ru