

РОЛЬ И МЕСТО PR-ДЕЯТЕЛЬНОСТИ В ПРОТИВОДЕЙСТВИИ ПРОЯВЛЕНИЯМ ЭКСТРЕМИЗМА В СЕТИ ИНТЕРНЕТ

О.В. Тепляков, доцент кафедры организации кадровой и воспитательной работы ФКУ ДПО Санкт-Петербургский институт повышения квалификации работников ФСИН России, кандидат политических наук, доцент

Аннотация: Работа посвящена анализу проблем, связанных с распространением деструктивного феномена экстремизма в сети Интернет. В статье рассматриваются наиболее острые вопросы, связанные с природой экстремистской деятельности в интерактивном пространстве, ролью и местом PR-деятельности в процессе противодействия экстремистским проявлениям в сети Интернет.

Ключевые слова: экстремизм, терроризм, антитеррористическая идеология, пропаганда, сети Интернет, PR-деятельность.

Продолжает нарастать угроза экстремизма национальной безопасности Российской Федерации. В Стратегии национальной безопасности Российской Федерации до 2020 года деятельность террористических организаций выделена как один из основных источников угроз национальной безопасности в сфере государственной и общественной безопасности [1].

В настоящее время «информационная революция» способствует формированию глобального информационно-коммуникационного пространства, которая началась на закате XX века и продолжает развиваться в настоящее время. Информационно - коммуникационные технологии (далее - ИКТ) активно влияли вчера и продолжают воздействовать сегодня на все сферы жизни современного общества, деятельность государственных и общественных институтов, и индивидуумов.

Наиболее ярким компонентом информационной сферы современности является непрерывно развивающаяся и совершенствующаяся информационно-телекоммуникационная сеть Интернет (далее - сеть Интернет). Открывающиеся благодаря ИКТ (в т.ч. сети Интернет) широкие возможности были успешно поставлены на службу социуму в сфере политики, экономики, культуры.

Однако научно-технический прогресс в сети Интернет имеет свою обратную сторону, состоящую в использовании их потенциала в деструктивных целях. К этому процессу следует отнести деятельность экстремистских организаций в интерактивном пространстве, которые представляют собой быстро расширяющееся явление, которое обязывает органы государственной безопасности и правопорядка принимать активные и скоординированные контрмеры с подобными угрозами. Подобный деструктивный процесс деятельности экстремистских организаций в сети

Интернет следует отнести к следующим обобщённым группам угроз: информационные войны; информационный экстремизм; информационная преступность.

Как отмечается в Концепции общественной безопасности Российской Федерации, члены экстремистских организаций активно используют новые технологии, в том числе информационно - телекоммуникационную сеть Интернет, для распространения экстремистских материалов, привлечение в свои ряды новых членов и координации противоправной деятельности [2].

Информационное пространство становится мощным средством в руках террористов, оказывающим устрашающее воздействие не только на отдельную личность, но и целые государства, группы государств и мировое сообщество в целом [3].

Сегодня именно сеть Интернет стала оружием в войнах нового поколения. «Цветные революции» в различных уголках мира - это проявления возможностей этого оружия. Таким образом, ИКТ базируются на определённом проекте действий, предусматривающим целенаправленную организованную работу, включающую систему особых информационных процедур, устрашающих мероприятий и действий, направленных на формирование экстремизмогенного образа реальности, в создании пласта сопротивления, управления и манипулирования информационными потоками для создания в обществе страха, чтобы мнение народных масс выступала в роли пресса давления на властные структуры для принятия определённых политических решений.

«Цветная революция» - это организованный извне государственный переворот. В его основе лежат информационные технологии с помощью, которых осуществляется манипуляция, протестным потенциалом населения. Посредством глобальной сети Интернет осуществляется целенаправленное воздействие на человеческое сознание. Таким образом, за считанные дни раскачивается ситуация внутри страны.

Сравнительно недавно в конце XX века началась деятельность в сети Интернет экстремистских организаций. В 1998 году около половины из тридцати террористических организаций, внесённых США в список иностранных террористических организаций имели веб-сайты, к 2000-му году практически все террористические группы обнаружили своё присутствие в сети Интернет [4].

В отчёте института мира USIP (United States Unstitute for Peace) отмечается, что Всемирная сеть является идеальной средой для деятельности террористов [5].

Подобному негативному процессу способствуют следующие факторы сети Интернет: открытость - свобода доступа; минимальная цензура и государственный контроль; глобально-транснациональная аудитория; анонимность общения; высокоскоростное движение информации; минимальная стоимость создания сайта и его обслуживание; благодаря мультимедийной среде возможность осуществлять комбинирование текста, графики, аудио и видео, возможность загружать фильмы, песни, книги,

постеры и т.д.; охват аудитории традиционных СМИ по причине использования Интернета как источника информации.

Сеть Интернет предоставляет возможности экстремистским организациям для распространения информации о своих акциях, позволяет обращаться к широкой аудитории в режиме реального времени; проводить информационно-пропагандистскую работу по привлечению в организации новых членов. Таким образом, в настоящее время большинство экстремистских организаций перешли из реальной социальной сферы в виртуальный мир.

Соответственно киберпространство способствует формированию более гибких сетевых форм взаимоотношений экстремистского сообщества. Создаются транснациональные сетевые рынки наёмников международных экстремистских организаций (далее-МЭО); незаконного оборота оружия, взрывчатых веществ и наркотиков; работоторговли и т.д..

Подобные ситуации складываются благодаря функционированию в сети в виртуальном пространстве «тёмного Интернета» (Darknet), объединяющий информационные ресурсы, недостижимые для обычных пользователей Интернета. Информация здесь находится под покровом специализированного программного обеспечения, которое обеспечивает шифрование и анонимность пользователей, используя протоколы и домены, на которые средний интернет - пользователь никогда не наткнётся [6]. Термином «Darknet» обозначают скрытые веб-коммуникации, большинство из которых ассоциируются в противозаконной или диссидентской деятельности. Основными сегментами этого веба является сеть «Тор» и платёжная сеть «Биткойн» [7].

Киберпространство представляет МЭО следующие направления использования ИКТ в экстремистской деятельности: с помощью СМИ, сети Интернет и иных СМК пропагандировать экстремистскую идеологию; осуществлять террористические атаки в киберпространстве; организовывать и планировать теракты, фандрайзинг, вовлечение в МЭО новых членов и т.д. с помощью ИКТ.

В настоящее время экстремизм в сети Интернет является динамичным явлением, которое благодаря внезапному появлению и исчезновению сайтов, смене форматов и адресов, сохраняют содержание. Также экстремистское сообщество ежедневно легитимно использует киберпространство для создания многоязычных сайтов, чтобы воздействовать на мировоззрение людей напрямую не вовлечённых в эту деструктивную среду.

Примером может являться высокая медиаактивность МЭО «ИГ», которая сформировала систему многоязычных медиаресурсов для трансляции информации на различные целевые аудитории. Например, на платформе «Аль-Хайят» присутствует сайт, на русском языке созданный на высоком профессиональном уровне и имеющий название «Халифат. Исламское государство». Структура сайта состоит из нескольких рубрик (новости, статьи, видео) с наличием ссылок на аккаунты в социальных сетях

и раздел «контакты», благодаря которому можно направить обращение администратору или перейти в чат для общения.

На сайте осуществляется пропаганда экстремистской идеологии, основное общение осуществляется на форуме по следующим направлениям: идеология, где представлены сведения об идеологических установках; аналитические материалы; новости; фильтрационный раздел предусматривает множество закрытых для сторонников-участников тем для обсуждения.

Особую опасность представляют МЭО маскирующиеся под легальные демократические организации с помощью «условной обезличенности», когда идет активная подготовка к революционным событиям. Примером может являться «арабская весна» на Ближнем Востоке. Используя, анонимизацию в процессе ведения скрытной пропаганды модератор может выдавать себя за жителя той или иной «горячей точки».

Наиболее полный перечень направлений использования киберпространства МЭО представлен в специальном аналитическом докладе Управления ООН по наркотикам и преступности (UNODC) «Использование Интернета в террористических целях»: пропаганда (в т.ч. вербовка, радикализация и подстрекательство к терроризму); финансирование; подготовка террористов; планирование (в т.ч. с использованием секретной связи и открытых источников информации); исполнение; кибератаки [8].

Пропаганда приспособлена для воздействия на потенциальных и реальных сторонников, а также противников, прямых и косвенных жертв террористических актов. Данная PR - технология является приоритетным направлением деятельности экстремистов в сети Интернета, с целью максимального использования своих идей среди населения и оказания информационно - психологического воздействия на целевые аудитории.

К пропагандистским материалам следует отнести: виртуальные сообщения; презентации; журналы; аудио и видео материалы; электронные игры. Весь комплекс информационно - пропагандистских материалов имеет форму мультимедийных коммуникаций, содержащих идеологические и практические наставления, разъяснения, а также рекламу экстремистской деятельности.

Источниками пропагандистских продуктов в сети Интернет являются: интернет порталы (это официальные или неофициальные СМИ, сайты организации и др.); интернет форумы различных направлений; блоги; видео - хостинги и социальные сети.

Пропагандистская деятельность МЭО в киберпространстве предусматривает решение следующих задач: осуществление информационно - психологического воздействия на потенциальных и реальных сторонников; противников общих воззрений того или иного экстремистского сообщества; на прямых или косвенных жертв террористических актов; на международное сообщество.

Благодаря пропагандистской деятельности МЭО в сети Интернет создаётся психологическая почва для радикализации и вовлечения в

экстремистскую среду новых членов, формирования лояльного общественного мнения у определённых групп населения, создание обстановки страха и хаоса с целью воздействия на поведение власти и населения.

Также активно используются в экстремистской деятельности ресурсы Интернета для вербовки и подстрекательства. Для этих целей используются сайты МЭО, коммуникационные платформы, чаты, блоги, социальные сети, IP-телефония, мессенджеры, электронная почта.

Процесс вербовки носит многоступенчатый характер. Выделяются следующие этапы: первоначальный (подготовительный; исполнительный; заключительный). Применительно к «духовному джихаду» реализуется следующая формула - «размораживание сознания»+ «изменение сознания» + «замораживание сознания» = «готовый боец джихада» (Теория изменения сознания Крута Левина) [9].

Первая степень (первоначальный этап) предусматривает широкое распространение информации пропагандистского характера о деятельности МЭО по всем каналам сети Интернет, которая носит ознакомительный характер. Второй этап уже предусматривает непосредственное вовлечение в экстремистскую деятельность, когда идеология МЭО приобретает характер убеждения в сознании вовлекаемого лица. Таким образом, осуществляется психологическая обработка новых членов с целью привития им экстремистских взглядов и обеспечение готовности к активным действиям.

На данном этапе осуществляется обучение новобранца экстремистской деятельности и потребность в непосредственных контактах с представителями МЭО для участия в диверсионно-террористических операциях.

Заключительный этап предусматривает готовность новобранцев к практическим действиям под воздействием идеологии МЭО, являющейся главным мотивирующим фактором, т.е. на данном этапе происходит самоопределение личности человека как последователя экстремистской идеологии и исполнителя диверсионно-террористических операций.

Таким образом, модель радикализации, разработанная Крисом Хеввельфингером охватывает четыре стадии: 1. Введение в экстремистскую идеологию. 2. Погружение в «тип мышления и образ мыслей» данной идеологии. 3 Разочарование, бездействие других приверженцев идеологии; 4. Решимость осуществить насилие во имя утверждения идей [10].

В последнее время одним из средств вовлечения новых членов в МЭО являются онлайн-компьютерные игры, предусматривающие выполнение заданий не только в виртуальном пространстве, но и реальном мире (погромы, теракты, и т.д.). Этот процесс вербовки носит индивидуальный характер общения в киберпространстве с потенциальным исполнителем теракта с целью его склонения к задуманному. Общение происходит с помощью «приватных» инструментов коммуникации (закрытые чаты, электронная почта, IP-телефония.).

Также интернет-пространство дает широкие возможности МЭО осуществлять подготовку новобранцев, благодаря распространению учебно-методической литературы, мультимедийных обучающих материалов, которые касаются самодельного изготовления оружия и СВУ, сбора необходимой информации, конспирации и обеспечения защиты используемых каналов коммуникаций, тактики подготовки и совершения терактов.

Данное направление предусматривает формирование виртуальных учебных лагерей в виде дистанционного электронного обучения или онлайн инструктажа с помощью интернет - телефонии.

Планирование и координация деятельности МЭО включает в себя использование сети Интернет для сбора информации из открытых источников о потенциальных объектах поражения, возможных орудиях и средствах совершения. Источниками необходимой информации являются популярные интернет-сервисы, социальные сети.

Также важнейшим аспектом в данном направлении является использование интернет-пространства как канала коммуникации (связи) между различными ячейками МЭО. Подобный контакт необходим для общения в «повседневной» деятельности, а также при планировании и осуществлении террористической атаки.

ИКТ позволяют МЭО в ходе подготовки и организации диверсионно-террористических операций координировать с ячейками исполнителей бесконтактным способом (передавать команды, давать инструкции, информировать об объекте поражения), а также целях и средствах совершения теракта, и координировать практическую деятельность.

Для маскировки в МЭО применяют методы обеспечения анонимности, с помощью беспроводного доступа WI-FI в общественных местах, используя вымышленные электронные адреса отправителя в программах пересылки электронной почты, шифрования трафика, задействование программ анонимайзеров стенографии (сокрытие сообщений в графических изображениях).

Также представители МЭО широко используют возможности Интернета для финансовой деятельности, которая включает: фандрайзинг (сбор средств) с помощью прямых призывов, размещаемых на веб-сайтах, в чатах, в социальных сетях, или посредством массовых рассылок; интернет-торговля в виде магазинов в киберпространстве, предлагающих всякую утварь (информационные материалы, символику, атрибутику и т.д.); оказание фиктивно созданных МЭО благотворительных организаций, которые организуют и проводят PR-кампании в режиме фандрайзинга (сбор средств).

Не чужд современным экстремистам «кибертерроризм», под которым понимают действия по дезорганизации информационных систем, создающих опасность гибели людей, причинения значительного имущественного ущерба либо поступления иных общественно опасных последствий, если они совершены в целях нарушения общественной безопасности устрашения

населения или оказание воздействия на принятия решения властными структурами, а также угрозу совершения указанных действий в тех же целях [11].

Соответственно МЭО не отказываются использовать социальные сети в своей деятельности. Горизонтальные социальные сети способствуют самоорганизации людей, а также помогают координировать и быстро управлять ресурсами, необходимыми для решения организационных задач. Сетевые технологии способны в одно и то же время быть гибкими и адаптивными благодаря своей способности децентрализованных действий сети, автономных ячеек, и при этом оставаться способными координировать всю эту децентрализованную активность в соответствии с общей целью принимаемых решений [12].

Приход МЭО в пространство современных социальных компьютерных сетей выводит их на новый уровень и приобретает системный характер. Активное использование сетевых интернет-ресурсов способствует эффективному влиянию на массы людей при планировании и осуществлении террористических атак устрашения или практики проведения массовых уличных и иных акций, которые получили образное определение «войны пчелиного роя», отражающего принципиальную особенность организации сетевой деятельности, когда невозможно выявить управление экстремистскими и террористическими группами и другими участниками событий [13].

Киберпространство расширяет возможности вовлечения пользователей Интернета в экстремистскую деятельность, а также в процессе координации деятельности многочисленных ячеек МЭО, находящихся в различных уголках планеты с использованием сетевых технологий. Использование сетевых интернет-ресурсов значительно ускоряет передачу информации, адаптацию к изменениям в окружающей среде с целью маскировки экстремистской деятельности в киберпространстве, чтобы быть неуязвимыми для правоохранительных органов.

Социальные сети способствуют МЭО оказывать влияние на различные группы пользователей, благодаря возможности размещать на платформах пропагандистского характера ауди/видео продукты и текстовую информацию, привлекающую общественное мнение с целью обсуждения социальных проблем и радикального их решения. Ярким примером эффективных интернет-ресурсов являются тематические чаты с голосовыми и видеовозможностями, которые позволяют экстремистам делиться информацией с минимальным риском.

Благодаря виртуальным сообществам широко вовлекается в экстремистскую деятельность молодежь, которая активно общается в социальных сетях. Примером использования социальных сетей в организации «цветных революций» является «арабская весна». Один из руководителей революционных выступлений в Египте Ваэль Гоним в своей книге «Революция 2.0.» описывает методику мобилизации общественной поддержки политического протеста через «Facebook», включающая

несколько стадий. «На первой стадии убеждаешь людей присоединиться к странице и читать записи. На второй подталкиваешь их взаимодействовать с контентом, ставя «лайки» и комментируя. На третьей – принимать участие в онлайн-кампаниях страницы и самим поставлять контент. На четвертой и последней стадиях люди выходят на улицы» [14]. Везде, где происходили события «арабской весны», для привлечения союзников протестующих использовали новые интернет-приложения и мобильные телефоны перебрасывая ресурсы из киберпространства в городское пространство и обратно [15].

Не забывают МЭО и про модный интернет-ресурс «YouTube», который является хорошим источником трафика, а также третий по посещаемости сайт и вторая поисковая система в России. Благодаря бесплатному размещению видео, рупор пропаганды экстремистов выкладывают свои ролики, несмотря на улучшение кампанией «Google» автоматического распознавания и удаление роликов, связанных с идеологией экстремизма. Сегодня «YouTube» является отличным инструментом по распространению замаскированной экстремистской идеологии с помощью видеороликов, которые помогают вовлекать в ряды МЭО новых сторонников. Также пропагандисты от МЭО учитывают тот фактор, что данный интернет ресурс в 2006 году был приобретен кампанией «Google», с тех пор в запросах этой поисковой системы на первых страницах можно встретить «YouTube» - видео. Это отличный способ предоставления экстремистского контента и грамотное продвижение видеороликов имеющих развлекательный или ознакомительный характер. Ярким примером может являться МЭО «ИГ», которая использует социальные сети «YouTube», «Facebook», «Twitter» для создания «джихад форумов». Подконтрольные экстремистские ячейки «ИГ» не только привлекают в свои ряды новых членов через интерактивное пространство, но и пользуются шифровальным мессенджером «Telegram» и другими инструментами социальных медиа, чтобы поддерживать связь между собой и инструктировать исполнителей о том, как осуществлять террористические вылазки. Также МЭО разрабатывают собственные платформы социальных медиа, чтобы обходить суровые меры безопасности на уже существующих виртуальных площадках и избегать утечек информации.

Информационно-пропагандистское противодействие экстремистской идеологии в России отражено в Концепции противодействия терроризму, утвержденной Президентом Российской Федерации от 5 октября 2009 года, а также в «Комплексном плане противодействия идеологии терроризма в Российской Федерации на 2013-2018 годы», который был подписан первым лицом государства 26 апреля 2013 года за № Пр-1069.

Соответственно, к основным задачам информационного противодействия идеологии экстремизма в интерактивном пространстве следует относить: осуществление мероприятий, направленных на противодействие пропаганде экстремистской идеологии; препятствовать использованию ИКТ для коммуникации членов МЭО между собой и иными

лицами в целях организации и осуществления экстремистской деятельности; не допускать посредством ИКТ осуществлять вербовку в ряды МЭО; препятствовать с помощью ИКТ осуществлять мероприятия в режиме фандрайзинга, направленные на финансовое обеспечение МЭО; не допускать осуществление кибератак МЭО на критически важные информационные структуры.

Главным принципом процесса противодействия проявлениям экстремизма в сети Интернет является выработка целостной стратегии, в которой все меры будут взаимосвязаны между собой.

В основе этой структуры должна быть заложена коммуникационная модель Г. Лассуэла, которая, имеет основные элементы связи: кто сообщает?; что сообщает?; по какому каналу сообщает?; кому сообщает?; с какими эффектом? [16].

Подобная модель должна быть использована для выявления имеющихся и возможных в будущем форм коммуникаций интерактивного пространства МЭО. Соответственно определяются субъекты такой коммуникации в структуре МЭО, определяются формы и виды информационных продуктов, их типовое содержание, устанавливаются основные каналы их трансляции в обществе, идентифицируются адресаты данных сообщений, и оценивается эффект воздействия каждого из них.

Данный подход необходим, чтобы иметь четкие характеристики каждого из выделенных элементов, чтобы выработать адекватные меры информационного противодействия в интерактивном пространстве. Таким образом, приоритеты информационного противодействия должны быть сфокусированы на доминирующих каналах информационного влияния МЭО.

К сожалению, в настоящее время отсутствует единая концепция антитеррористической PR-деятельности, охватывающей все возможные целевые аудитории и каналы коммуникации.

В сложившейся ситуации основным направлением информационного противостояния экстремизму, в том числе с учетом киберпространства является противодействие идеологии экстремизма, где приоритетом будет профилактика в сфере PR-деятельности.

Антитеррористический PR включает методы информационного реагирования и использования полного комплекса коммуникационных технологий в реальном и виртуальном мире. Коммуникационный процесс предусматривает организацию и проведение PR-мероприятий, подготовку и распространение информационной продукции контрпропагандистского характера, участие в спорах и обсуждениях, проводимых на форумах и в социальных сетях.

Ранее перечисленный информационный процесс должен осуществляться в рамках антитеррористических PR-кампаний, чтобы формировать «информационный иммунитет» общества к пропаганде экстремистской идеологии.

Главным принципом антитеррористического PR является стимулирование позитивной социальной активности, для этого должна быть

создана PR-концепция о противодействии идеологии экстремизма, закрепляющая следующие меры: информационно-аналитическое обеспечение противодействия терроризму и экстремизму (выпуск всевозможных памяток, брошюр, книг, обращений, плакатов, и т.д.); пропагандистское обеспечение (своевременное доведение объективной информации о результатах деятельности в указанной сфере); контрпропагандистское (адекватная и своевременная реакция на дезинформацию, выступления, высказывания прекративших свою преступную деятельность главарей бандформирований, распространение листовок и пропагандистской литературы); идеологическое (формирование религиозной и межнациональной терпимости, патриотизма, здорового образа жизни, приоритетов общечеловеческих ценностей и т.д.); организационное содействие деятельности религиозных объединений традиционной, конструктивной, в том числе антитеррористической направленности; взаимодействие со СМИ; проведение конференций, слетов, круглых столов, конкурсов на лучшие материалы антитеррористического характера и т.д.); образовательное направление (создание системы подготовки специалистов, в том числе из числа гражданских лиц, в области противодействия идеологии терроризма [17].

Отдельно следует остановиться на осуществлении вербовки новых членов МЭО с использованием ИКТ, т.е. сети Интернет и особенно, социальных сетей. В данном направлении должны использоваться организационно-правовые меры, направленные на закрытие сайтов в сети Интернет или интернет-страниц с соответствующим контентом, блокирование аккаунтов отдельных активистов и сообществ в социальных сетях. Подобное направление носит технический характер.

Соответственно, помимо вышеуказанного курса, необходимо осуществлять комплексную PR-деятельность с целью разоблачения истинных целей и намерений МЭО, описание реальных положений «новобранцев» в их составе, дискредитации лидеров ячеек МЭО, раскрытие информации о невинных жертвах террористических атак.

Главная задача PR-деятельности в сети Интернет – это создание единого антитеррористического пространства в виртуальном и реальном мире. Таким образом, в современной обстановке ключевой задачей данного направления деятельности является правовое воспитание, которое формирует надежную защиту сознания человека от воздействия экстремистской идеологии.

Список использованных источников

1. Стратегия национальной безопасности Российской Федерации до 2020 года (утв. Указом Президента РФ от 12 мая 2009 г. №537) // СЗ РФ. 2009. № 20. Ст. 2444.

2. Концепция общественной безопасности Российской Федерации 20 ноября 2013 г.) // Президент России: официальный сайт. <http://kremlin.ru/acts/19653> (дата обращения 9.09.2018).
3. Буркин А.И., Возженников А.В., Синсок Н.В. Национальная безопасность России в контексте современных политических вызовов. Изд. Второе, доп. / Под общ.ред. А.В. Возженникова. М.: Изд-во РАГС, 2008. С. 248.
4. Вейман Г. Как современные террористы используют Интернет. Специальный доклад № 116 // Центр исследования компьютерной преступности. http://www.crime-research.ru/analytics/Tropina_01/ (дата обращения 9.09.2018)
5. Интернет идеальная среда для террористов// SecurityLab.ru/ <http://www.securitylab.ru/news/2130806.php> (дата обращения: 13.09.2018)
6. Чакос Б. Darknet - темная сторона сети// DGL.ru 11.10. 2013 [http://www.d61.ru/articles/darknet - temnaya - storona - seti_4222_4222, html](http://www.d61.ru/articles/darknet-temnaya-storona-seti_4222_4222.html) (дата обращения: 14.09.2018).
7. Ларина Е., Овчинский В. Кибервойны XXI века. Возможности и риски для России или о чем умолчал Эдвард Сноуден. М.: Книжный мир, 2014. С. 7.
8. Использование Интернета в террористических целях. Управление Организации Объединенных Наций по наркотикам и преступности, 2013.
9. Вершинин М.В. Методы вербовки и идеологическая работа террористических религиозных движений в Поволжье, на примере Хизб-т-Тахрир». // Psifactor/ [http://psifactor/ org/lib/vershinin5. html](http://psifactor.org/lib/vershinin5.html) 26.03.2008. (дата обращения: 16.09.2018).
10. Радикализация и организация насилия в Интернете. Интервью с директором центра изучения террористической радикализации Давидом Гартенстайн-Россом //Российский совет по международным делам. 14 июня 2013 г. [http://www.russian council.ru/inner/2id_4=1969#top/](http://www.russiancouncil.ru/inner/2id_4=1969#top/) (дата обращения: 15.09.2018).
11. Федоров А.В. Информационная безопасность в мировом политическом пространстве: Учеб.пособие. М.: МГИМО, 2006. С.111.)
12. Кастельс. М. Информационная эпоха: экономика, общество, и культура, 2000.
13. Гоним В. Революция 2.0. Документальный роман./ Пер. с англ. Т. Даниловой. СПб. : Издательская группа «Лениздат» «Команда А», 2012. С. 93.
14. Методика и программные продукты были разработаны и внедрены американскими НПО. Подробнее см: Руководство в помощь пользователям интернета в репрессивных государствах. Доклад-презентация 12.04.2011. [www. Freedom House.com](http://www.freedomhouse.com). (дата обращения: 15.09.2018).
15. Lasswell H.D. The structure and funct; on of communicat: on in. society. In: Beyson, (ed) The cjmmunication of ideas N.Y. : Harper and Brothers? 1948/ P. 32-51.

16. Терроризм в современном мире. 2 изд. / под ред. В.Л. Шульца.
М.: Наука, 211. С.387-388.