РАЗДЕЛ II

ТЕРРОРИЗМ И ЭКСТРЕМИЗМ

ИГОРЬ ЮРЬЕВИЧ СУНДИЕВ,
доктор философских наук, профессор,
главный научный сотрудник ФГКУ «ВНИИ МВД России»;

АЛЕКСАНДР АЛЕКСАНДРОВИЧ СМИРНОВ,
кандидат юридических наук, доцент,
ведущий научный сотрудник ФГКУ «ВНИИ МВД России»

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ СЕТЕЙ В ЭКСТРЕМИСТСКОЙ И ТЕРРОРИСТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

Дается общая оценка использования Интернета террористическими и экстремистскими организациями, определяются основные направления и способы такого использования, показана роль социальных сетей в деятельности экстремистских формирований.

Ключевые слова: национальная безопасность, противодействие экстремистской и террористической деятельности, Интернет, киберпреступность, кибертерроризм, социальные сети, информационная война.

I. Y. Sundiev, DSc (Philosophy), Professor, Chief Researcher Russia MI FPOI National Research Institute; e-mail: vnii59@yandex.ru, tel.: 8 (495) 695-77-41;
A.A. Smirnov, Phd (Law), Associate Professor, Senior Researcher Russia MI FPOI National Research Institute; e-mail: smirnov research@bk.ru, tel.: 8 (495) 915-23-33.

The use of information networks in terrorism and extremism activity.

The general assessment of use of the Internet by the terrorist and extremist organizations is given, the main directions and ways of such use are defined, the role of social networks in activity of extremist formations is shown.

Key words: national security, counteraction against terrorism and extremism activity, Internet, cybercrime, cyberterrorism, social network, information warfare.

Терроризм и экстремизм в современном мире относятся к числу актуальных угроз национальной безопасности, представляющих высокую степень общественной опасности. Экстремистские группировки расширяют территориальные масштабы своей деятельности, усиливают интенсивность и жесткость совершаемых террористических атак. Происходят постоянное развитие форм и методов деятельности террористических и экстремистских организаций, повышение уровня их организованности и материально-технической оснащенности, их транснационализация и сращивание с организованной преступностью.

Существенное влияние на террористическую и экстремистскую деятельность оказывает формирование глобального информационного общества. Стремительные темпы внедрения информационных технологий, развития компьютеризации и информатизации всех сфер жизнедеятельности общества ведут к созданию единого мирового информационного пространства, в котором находятся во взаимодействии и взаимосвязи все средства сбора, накопления, обработки, обмена и хранения информации. Такое пространство становится мощным орудием в руках террористов, оказывающим устрашающее воздействие не только на отдельную личность, но и на целые государства, группы государств и мировое сообщество в целом[1].

История террористической деятельности в киберпространстве непродолжительна. В 1998 г.

около половины из тридцати террористических организаций, внесенных США в список иностранных террористических организаций, имели Web-сайты, к 2000 г. практически все террористические группы обнаружили свое присутствие в сети Интернет[2]. В настоящее время Интернет рассматривается многими террористическими и экстремистскими формированиями как один из ключевых инструментов реализации своих противоправных целей.

В сложившейся ситуации особую значимость приобретает адекватная оценка текущего состояния использования информационных сетей в экстремистской и террористической деятельности и построение эффективного механизма противодействия. В силу своей относительной новизны данная проблема сравнительно недавно стала разрабатываться в научных трудах[3].

Общая оценка использования Интернета террористическими и экстремистскими организациями.

Глобальная информационная сеть Интернет приобрела важное значение в нашей жизни и завоевала огромную популярность. По данным Международного союза электросвязи (ITU), в начале 2013 г. число пользователей Интернета в мире достигло 2,75 млрд человек, что составляет 38,8% населения мира[4]. Нахождение в социальных сетях является сегодня самой популярной формой активности интернет-пользователей. Число пользователей Facebook, хотя бы один раз в месяц посещающих эту социальную сеть, в октябре 2012 г. превысило 1 млрд человек[5].

Наша страна, находившаяся в числе аутсайдеров в начале 2000-х годов, совершила стремительный рывок и в 2012 г. вышла по показателям численности интернет-пользователей на 1-е место в Европе. Согласно данным, приведенным аналитической компанией TNS Россия на конференции i-Comference-2013, примерно 60% населения России старше 12 лет хотя бы раз в месяц пользуются Интернетом, что составляет около 74,4 млн человек[6]. По разным данным, от 75 до 80% россиян, пользующихся Интернетом, посещают социальные сети. Как показало исследование comScore, в августе 2011 г. объем времени, проводимого нашими соотечественниками на страницах социальных сетей, превышал средний общемировой показатель более чем вдвое. Таким образом, Россия оказалась страной с наивысшей в мире популярностью социальных сетей. Крупнейшей российской социальной сетью считается «ВКонтакте», в которой зарегистрировано более 140 млн пользователей. При этом ежедневно этой социальной сетью пользуются 38 млн человек. У социальной сети «Одноклассники» этот показатель равен 30 млн пользователей[7].

Столь обширная аудитория Интернета и колоссальные возможности распространения информации в ней привлекли к себе внимание террористических и экстремистских организаций. Сегодня все действующие террористические группы обнаруживают свое присутствие в Интернете. К наиболее значимым террористическим организациям, активно использующим ресурсы Интернета, можно отнести такие, как. ХАМАС, «Хизбапла», «Аль-Джихад», «Братья-мусульмане», «Народный фронт освобождения Палестины», «Конгрегел» (бывшая Рабочая партия Курдистана), «Реальная ИРА» и ряд других. С помощью глобальной сети данные организации решают свою главную задачу - при обеспечении наибольшего охвата потенциальной аудитории довести сообщение до каждого конечного потребителя быстро и без цензуры[8].

Как показал проведенный нами анализ, в России начало активного использования Интернета террористическими и экстремистскими организациями можно отнести к началу 2000-х годов В дальнейшем развитие данного процесса шло в геометрической прогрессии. Отмеченная негативная тенденция продолжает сохраняться и в настоящее время, при этом она корреспондируется с развитием киберпреступности в нашей стране

В Рунете существуют более ста активно действующих интернет-сайтов российских радикальных структур (*рп14. info, dpni.org, nazbol.ru, tor85.livejournal.com* и т.д.). Они, как правило, пропагандируют политические идеи, проводят агитационную и вербовочную деятельность, направленную на увеличение числа своих сторонников. Исследование показало динамику изменения (роста) количества субъектов террористической и экстремистской деятельности, использующих Интернет (табл.). Налицо резкий скачок в 2012 г Данная тенденция сохраняется и в 2013 г.

В качестве примера можно рассмотреть Дальневосточный федеральный округ, в котором проблема экстремистских проявлений в Сети возникла недавно. Интернет в нем стал общедоступен в 2004-2006 гг., и с этого времени органами внутренних дел фиксируется деятельность радикальных групп по созданию в Интернете негативного образа представителей государственной власти, распространению материалов, направленных на разжигание межнациональной и межконфессиональной вражды. Общедоступность распространяемой информации и ее быстрое тиражирование способствовали резкому увеличению количества сторонников радикальных объединений. В результате в 2008 г. зна-

Таблица

Предполагаемое (среднеарифметическое) количество субъектов экстремистской и террористической деятельности, использующих Интернет (доля по сравнению с неиспользующими), %

	Годы			
	2009	2010	2011	2012
Предполагаемое количество субъектов экстремистской и террористической деятельности, использующих Интернет	55,5	63,5	50,0	71,4

чительно увеличилось количество выявленных противоправных деяний экстремистской направленности. Данная тенденция сохраняется и в настоящее время. В таких неформальных движениях манипулируют общественным сознанием, дискредитируют органы государственной власти, создают собственные образы борцов за права и свободы, что привлекает молодежь. Участники этих объединений скрывают свои противоправные устремления, но посредством Интернета в короткие сроки вовлекают многих граждан в криминальную деятельность. Пропагандируемая идеология подменяет морально-этические нормы общества, формирует асоциальные мировоззрение и поведение у своих сторонников.

Терроризм в сети Интернет - очень динамичное явление: сайты появляются внезапно, часто меняют формат, а затем также стремительно исчезают или во многих случаях создают видимость исчезновения, меняя свой адрес, но сохраняя содержание. При этом отмечаются все более многочисленные случаи ежедневного использования сети Интернет террористами, которые носят внешне легитимный характер.

Основные направления и способы использования Интернета террористическими и экстремистскими организациями.

Собственно в использовании Интернета (и особенно социальных сетей) террористическими и экстремистскими организациями можно выделить два генеральных направления: ***обеспечивающее*** (пропаганда, сбор информации, связь, координация, вербовка, сбор денежных средств) и непосредственное - ***кибертерроризм***[9].

Более детальная классификация представлена 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) пропаганду; 6) вербовку; 7) организацию сетей; 8) планирование и координацию террористических действий[10]. Схожий перечень приводится в специальном аналитическом докладе Управления ООН по наркотикам и преступности (UNODC) «Использование Интернета в террористических целях»[11] (далее - Доклад ЮНОДК): 1) пропаганда (в том числе вербовка, радикализация и подстрекательство к терроризму), 2) финансирование; 3) подготовка террористов; 4) планирование (в том числе с использованием секретной связи и открытых источников информации); 5) исполнение; 6) кибератаки. Рассмотрим основные направления использования Интернета в деятельности террористических и экстремистских организаций на основе анализа названых источников.

Пропаганда.

Оценивается как приоритетное направление использования Интернета террористами. Основные цели состоят в максимально широком распространении своих идей среди населения и оказании психологического воздействия на целевые группы (сторонников, реальных или потенциальных жертв, правительство, международное сообщество). В качестве примера можно привести «Апь-Каиду», идеологи которой особо подчеркивают важность последовательного ведения так называемого медиа джихада[12].

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-порталы (официальные и неофициальные СМИ, сайты организаций и др.); интернет-форумы различной направленности, блоги, социальные сети и видео-хостинги.

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

многоязычные сайты. К примеру, баскская террористическая организация ЕТА предлагает информацию на испанском, немецком, французском и итальянском. Шри-ланкийская группировка «Тигры освобождения Тамил Илам» публикует свои материалы на английском, японском и итальянском, «Исламское движение Узбекистана» - на узбекском, арабском, английском и русском. Движение «Талибан» размещает информацию на своих аккаунтах в социальных сетях «Фейсбук» («ғaceЬook») и «Твиттер» («Twitter»). С мая 2011 г. страница в «Твиттере», помимо языка пушту, ведется на английском. Двуязычие уже позволило движению привлечь на свою страницу в «Твиттер» более 5,5 тыс. подписчиков.

Простой порядок размещения контента в Интернете устраняет зависимость террористических организаций от СМИ, редакционная политика которых может блокировать распространение пропагандистской информации о террористах.

Вербовка и подстрекательство.

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 онлайновые компьютерные игры, которые могут предусматривать выполнение «заданий» не только в виртуальном пространстве, но и 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.

В Докладе ЮНОДК отмечается, что грань между пропагандой терроризма и подстрекательством к совершению терактов зачастую достаточно тонкая. Поэтому в ряде стран, где сама пропаганда не запрещена, для привлечения к ответственности за подстрекательство требуется доказать наличие необходимого умысла и прямой причинной следственной связи между ним и действиями по подготовке и совершению теракта. 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.

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 документе, были обнаружены виртуальные учебные лагеря, предоставляющие инструкции по использованию оружия в форме дистанционного электронного обучения[13]. Еще одной «инновационной» формой обучения террористов являются онлайн-инструктажи, проводимые посредством 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, ғaceЬook).

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 г. в США использовали электронную почту для координации действий. В целях конспирации террористы активно применяют методы обеспечения анонимности в Интернете, такие как шифрование трафика, задействование программ-анонимайзеров и стеганографии (сокрытие сообщений в графических изображениях). Например, летом 2012 г. администрация *«Кавказ-Центра»* разместила копию своего ресурса в общедоступной *сети анонимизации Tor*, тем самым предоставив пользователям Рунета возможность получить свободный

анонимный доступ к информации, размещенной на своих страницах.

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

Финансирование.

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

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

б) *электронная торговля* - включает организацию 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 компьютерных ресурсов в качестве средства совершения террористических атак против информационных систем. Под *кибертерроризмом*, как правило, понимают действия по дезорганизации информационных систем, создающие 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 угрозу совершения указанных действий в тех же целях[14]. Орудием кибертеракта выступает вредоносное программное обеспечение (вирусы, «трояны», программы для массовой рассылки сообщений и т.п.).

Ключевой целью кибертеррористов служат 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 только киберпространством, а затронут объекты реального мира, такие как системы жизнеобеспечения городов (электроэнергетические сети, система теплоснабжения), объекты авиа-, морского (речного) и железнодорожного транспорта, атомной энергетики и т.д., что наглядно продемонстрировал вирус Stuxnet. Как известно, его атаке в 2010 г. подверглись программируемые логические контроллеры иранской АЭС, в результате которой был нарушен процесс функционирования. Как отмечалось в обзоре «Kaspersky Security Bulletin 2010», данный пример свидетельствует о том, что существовавшая ранее грань между виртуальным и реальным миром фактически оказалась стертой.

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». Они могут также создавать обычное программное обеспечение, которое в определенный момент может быть использовано против владельцев компьютеров, например, если террористам понадобится получить доступ к секретной информации, содержащейся на компьютере, где установлена подобная программа.

Пока еще не было зафиксировано масштабных актов кибертерроризма. Но представляется, что это лишь вопрос времени. Экспертные оценки и моделирования показывают неготовность государств и предприятий к кибератакам террористов. Так, Гари Дэвис (Gary Davis) из фирмы McAfee привел пример, когда система водоснабжения Южной Калифорнии наняла хакера проверить надежность ее сети управления. Хакер за час добился доступа и полного контроля над системой и осуществил добавление оговоренных химических веществ в воду[15]. В начале 2013 г. на хакерской конференции Hack In The Box в Амстердаме немец Хьюго Тезо представил программу для Android-устройств, которая позволяет дистанционно перехватывать управление самолетом с помощью смартфона[16]. Эти примеры демонстрируют потенциальные возможности террористических структур в киберпространстве, которые, впрочем, не стоит преувеличивать[17].

Говоря о кибертерроризме, следует иметь в виду возможную связь исполнителей таких терактов со спецслужбами определенных государств. Другими словами, террористы могут осуществлять кибератаки в интересах третьей стороны

против определенного государства в соответствии с полученными директивами, выполняя тем самым за нее «грязную работу». На это обращено внимание в Докладе группы правительственных экспертов ООН A/65/201, в котором отмечается, что физические лица, группы и организации, включая преступные группы, выполняют посреднические функции в осуществлении подрывной сетевой деятельности от имени других[18]. Для государства - заказчика такой операции - это отличный способ избежать ответственности за свои действия. При этом для обеспечения успеха операции оно может передать террористам всю необходимую информацию об объекте кибератаки (в том числе полученную разведывательным путем). Нельзя также исключать возможности использования спецслужбами террористов для указанных целей «втемную» - посредством организации контролируемых утечек информации и совершения определенных действий.

Еще одной формой кибертерроризма следует считать *хакерские атаки на правительственные и корпоративные сайты с целью блокирования их работы либо размещения на них пропагандистской информации*. Данная форма действий терроризма уже получила широкое распространение в мире. Например, авторы статьи «Сетевые медиабои на Ближнем Востоке» в качестве эпизода длительного противостояния в виртуальном пространстве израильских и исламских групп интернет-активистов приводят взлом палестинской группой хакеров Gaza Team сайтов израильской партии «Кадима» и Кнессета (парламента) Израиля, на которых было размещено требование освобождения всех заключенных палестинцев, а также прекращения строительства еврейских поселений на Западном берегу реки Иордан и археологических раскопок у мечети Апь-Акса в Иерусалиме. Другой пример, указанный в статье, - хакерская атака марокканской группы Team Evil более чем на 750 израильских сайтах. На атакованных ресурсах ими был размещен текст: «Вы убиваете палестинцев, мы убиваем серверы»[19].

Подобной атаке подвергалась и наша страна. Сирийские хакеры из группы Syrian Revolution Electronic Suite взломали сайт Полномочного представителя Президента РФ по Дальневосточному федеральному округу и разместили на нем обращение к российскому народу, в котором они призывали россиян отказаться от поддержки президента Сирии Б. Асада и прекратить поставки Дамаску тяжелого вооружения[20].

Социальные сети в деятельности экстремистских формирований.

Горизонтальные сетевые структуры самоорганизации людей существовали всегда и действовали на уровне частной и бытовой жизни. Однако координировать и быстро управлять ресурсами, необходимыми для решения масштабных задач, было под силу лишь несетевым, жестким вертикальным структурам с четким управлением. Ключевое отличие сегодняшней ситуации в том, что обладая цифровыми сетевыми технологиями, сетевые структуры впервые «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»[21].

Сегодня сетевые структуры противостоят классическому суверенному национальному государству (соответственно и правоохранительным органам) с двух направлений - как «снизу» в виде различных формальных и неформальных сообществ и НПО, так и «сверху» в виде «надгосударственных» сетевых структур. Использование социальных сетей террористическими и экстремистскими организациями выходит на новый уровень и приобретает системный характер. Социальные сети и сервисы микроблогов, предоставляющие возможность свободно размещать информацию, становятся одними из наиболее эффективных средств влияния на массы людей при планировании и непосредственном осуществлении террористических и экстремистских актов.

Ярким примером является массовое использование социальных сетей и сервисов микроблогов во время так называемой арабской весны. Подтверждением служит динамика количества входов в социальную сеть «Twitter» в Египте в период с января по март 2010 г. (пик соответствует переизбранию Хосни Мубарака на должность президента Египта). В своей книге «Революция 2.0» один из организаторов революционных выступлений в Египте Ваэль Гоним описывает методику мобилизации общественной поддержки политического протеста через ҒaceЬook, включающую 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 онлайновых кампаниях страницы и самим поставлять контент. На четвертой и последней стадии люди выходят на улицы»[22].

25 января 2010 г. на улицах Каира вспыхнули протесты против режима Хосни Мубарака. В попытке ограничить протестные действия правительство уже через три часа закрыло службы Интернета и мобильной связи, но ничего не вышло: развитая экосистема переговоров через

FaceЬook, Twitter и чаты уже объединила тысячи каирцев, которые продолжали бунтовать. Правительство отступило и восстановило связь, чтобы сохранить экономику и системы жизнеобеспечения страны, но протесты уже переросли в массовые беспорядки, и через 14 дней Мубарак ушел в отставку.

Всего несколькими неделями раньше в ходе «жасминовой революции» в Тунисе диссидент, блогер и организатор протестов Слим Амаму (Slim Amamou) использовал социальное приложение Foursquare, чтобы оповестить друзей о своем аресте 6 января. «Зарегистрировавшись» при помощи этого сервиса в тунисской тюрьме, он обозначил для глобального сообщества сторонников свое местонахождение, что сразу же привлекло внимание всего мира. С 8 января он был поддержан со стороны Anonymous (анонима, неизвестного - англ.), группы сопротивления, состоящей из хакеров, которые работают непрерывно «против цензуры в Интернете или в мире». В тот день из одного чата был распространен призыв к сотням людей: Anonymous запускает операцию «Тунис», чтобы атаковать правительственные сайты. Если верить одному из парижских членов этой группы, пожелавшему остаться неизвестным, атака была успешной. «Речь идет одновременно об атаках DDoS [Distributed Denial-of-Service - распределенные атаки типа «отказ в обслуживании»] или же об атакующей программе, как, например, LOIC [Low Orbit Ion Cannon - приложение, разработанное хакерской группой 4Chan, созданное для организации DDoS атак на веб-сайты с участием тысяч анонимных пользователей, пользующихся программой]. Это рассматривалось как психологическое освобождение Туниса, по словам наших контактов на местах»[23].

Везде, где происходили события «арабской весны», для привлечения союзников протестующие использовали новые интернет-приложения и мобильные телефоны, перебрасывая ресурсы из киберпространства в городское пространство и обратно[24]. Для посетителей социальных сетей создавалось впечатление, что в протестные действия включились миллионы людей. Однако в действительности число реально протестующих и число протестующих в сети отличается многократно. Достигается это с помощью специальных программ. В 2010 г. правительство США заключило договор с компанией HBGary Federal на разработку компьютерной программы, которая может создавать многочисленные фиктивные аккаунты в социальных сетях для влияния на общественное мнение по спорным вопросам и манипулирования им, продвигая пропаганду. С февраля 2011 г. эта программа активно используется и распространяется. Она также может быть использована для наблюдения за общественным мнением, чтобы находить точки зрения, которые не нравятся власть имущим. Затем их «фиктивные» люди могут теоретически проводить грязные кампании против этих «реальных» людей. Еще раньше ВВС США заказали разработку Persona Management Software (программы по управлению персонажами), которую можно использовать для создания и управления фиктивными аккаунтами на сайтах социальных сетей, чтобы искажать правду и создавать впечатление, будто существует общепринятое мнение по спорным вопросам. «Персонажи должны производить впечатление, что они происходят почти из любого места в мире и могут взаимодействовать посредством обычных онлайн-сервисов и платформ социальных сетей»[25]. Издание DailyKos сообщило, что Persona Management Software позволит небольшому числу людей создавать «армию виртуалов» (фиктивных пользователей), которые могут искажать правду, в то же время создавая впечатление «настоящего онлайн-восстания».

В настоящее время данный отработанный механизм использования социальных сетей террористическими и экстремистскими организациями представляет реальную угрозу Российской Федерации. В нашей стране направленность использования социальных сетей террористическими организациями связана с очагами тлеющих этнических конфликтов. Это прежде всего Республика Дагестан. Правоохранительными органами периодически фиксируются факты появления новых социальных сетевых ресурсов, пропагандирующих радикальные религиозные течения с целью вовлечения лиц в незаконные вооруженные формирования.

Заключение.

Все вышеизложенное позволяет сделать однозначный вывод - противодействие использованию информационных сетей террористическими и экстремистскими организациями, защита важнейших информационных инфраструктур от кибератак приобретают важное значение для национальной безопасности Российской Федерации в современную эпоху. В данной области требуется повышение эффективности работы правоохранительных и иных государственных органов, выстраивание взаимодействия и обмена информацией между ними и организациями частного сектора, включая интернет-отрасль, формирование и развитие соответствующего законодательства.

Отметим также, что меры по закрытию интернет-ресурсов экстремистского характера и

(или) ограничению доступа к ним имеют невысокую эффективность в борьбе с использованием сети Интернет в деятельности террористических и экстремистских организаций и могут быть успешно преодолены. В связи с этим требуются выработка и реализация комплекса альтернативных мер по противодействию данной угрозе, важнейшими из которых являются меры информационного реагирования и контрпропаганды. Другими словами, правоохранительным органам необходимо научиться вести информационную войну с террористическими и экстремистскими формированиями в Интернете, создав для этого необходимый кадровый и ресурсный потенциал.

ная безопасность России в контексте современных политических вызовов / Под общ. ред. А.В. Возженикова. - М.: РАГС, 2008. С. 248.

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

[3] Вейман Г. Указ. соч.; Конвей М. Использование террористами сети Интернет и борьба с этим явлением / Владивостокский центр исследования организованной преступности. URL: http://www.crime.vl.ru (дата обращения: 12.05.2013); Сундиев И.Ю. Оперативно-розыскная деятельность органов внутренних дел Российской Федерации по предотвращению вербовки в экстремистские и террористические организации с использованием сети Интернет: Монография. - М.: ВНИИ МВД России, 2010; Сундиев И.Ю. Введение в оперативно-розыскную террологию: Монография. - М.: Юнити, 2011; Герке М. Понимание киберпреступности: явление, задачи и законодательный ответ // Международный союз электросвязи. 2012; Использование Интернета в террористических целях / Управление Организации Объединенных Наций по наркотикам и преступности. 2013.

[4] International Telecommunication Union. Statistics. URL: http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx (дата обращения: 08.09.2013).

[5] Число пользователей соцсети FaceBook перевалило за миллиард // РИА Новости. 2012. 4 окт. URL: http://ria.ru/technology/20121004/766127348.html (дата обращения: 14.03.2013).

[6] Ежемесячно Интернетом пользуется около 60% населения РФ старше 12 лет // РИА Новости. 2013. 5 марта. URL: http://ria.ru/society/20130305/925928196.html (дата обращения: 05.03.2013).

[7] Фонд развития гражданского общества. Рунет сегодня. - М., 2012.

[8] 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.

[9] Threat assessment (abridged). Internet Facilitated Organised Crime. IOCTA. EUROPOL Public Information. 2012.

[10] Вейман Г. Указ. соч.

Управление Организации Объединенных Наций по наркотикам и преступности. 2013.

[12] Горбатова В В. Указ. соч. С. 24.

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

[15] Семенов Ю.А. Сетевые угрозы // Экономические стратегии. 2013. № 3. С. 51.

[16] Теперь с мобильного можно перехватить управление самолетом. URL: http://hitech.vesti.ru/news/view/id/1759 (дата обращения: 13.04.2013).

[17] Астахов А. Реалии и мифы кибертерроризма. URL: http://www.iso27000.ru/chitalnyi-zai/kiberugrozy-i-kiberterroMzm'realii-i-mify-kiberterrorizma (дата обращения: 20.08.2013)

ям в сфере информатизации и телекоммуникаций в контексте международной безопасности / Организация Объединенных Наций. - Нью-Йорк, 2012. С. 1-10.

[19] Газетов В.И., Ветров М.Н. Сетевые бои на Ближнем Востоке // Независимое военное обозрение. 2013. № 27

[20] Сирийские хакеры взломали сайт дальневосточного полпредства. URL: http://top.rbc.ru/society/18/03/2013/849534.shtml (дата обращения: 18.03.2013).

[21] Кастельс М. Информационная эпоха: экономика, общество и культура / Пер. с англ.; Науч. ред. О.И Шкаратан - М„ 2000.

[22] Гоним В. Революция 2.0: Документальный роман / Пер. с англ. Т.Даниловой. - СПб.: Лениздат; Команда А, 2012. С. 93.

[23] «Operation Tunisia»: la cyberattaque dAnonymous aux cotes des manifestants // Liberation (Франция). 2011. 12 янв.

[24] Методика и программные продукты были разработаны и внедрены американскими неправительственными организациями. (Руководство в помощь пользователям Интернета в репрессивных государствах: Доклад - презентация пособия. 2011. 12апр.). URL: http://www. Freedom House com

[25] Army of Fake Social Media Friends to Promote Propaganda // PCWorld. 2011. February, 23.