ИГОРЬ СУНДИЕВ, АЛЕКСЕЙ СМИРНОВ

Сетевые возможности и сетевые угрозы

Информационные сети в экстремистской и террористической деятельности

В настоящее время одним из приоритетных направлений обеспечения национальной безопасности любой страны становится широкомасштабное противодействие экстремистской и террористической деятельности. Для нашей страны этот тезис особенно актуален, поскольку острота угроз со стороны терроризма и экстремизма не спадает. В 2012 году было зарегистрировано 637 преступлений террористического характера (рост — 2,4 процента), в том числе 24 теракта и 696 преступлений экстремистской направленности (рост — 11,9 процента).

Современный международный терроризм и экстремизм необходимо рассматривать в контексте общемировых политических реалий. Преодолев открытое военное противостояние и «холодную войну», а также скрытое противоборство в рамках «международного сосуществования», мировое сообщество входит в новую эпоху — эпоху информационных войн. В отличие от традиционных вооружений, средства противоборства в информационном пространстве могут эффективно использоваться и в мирное время. Важной особенностью этих средств является то, что они доступны не только государственным, но и террористическим, криминальным структурам, а также отдельным лицам[1].

В условиях формирования «информационного общества» террористические и экстремистские организации в своей деятельности все шире используют новейшие технологии, создавая угрозу безопасности личности, общества и государства. История террористической деятельности в киберпространстве началась сравнительно недавно. В 1998 году около половины из 30 иностранных организаций, внесенных США в список террористических, имели Web-сайты, к 2000 году практически все террористические группы обнаружили свое присутствие в сети Интернет[2]. В настоящее время Интернет

[1] *См.* **А. Крикунов, Д. Литвинов**. Проблема терроризма в сети Интернет и пути ее решения. — «Мы против террора и насилия!» (http://antiterror.vologda-uni.ru).

[2] *См.* **Г. Вейман**. Как современные террористы используют Интернет. Специальный доклад № 116. — Центр исследования компьютерной преступности (www.crime-research.ru/analytics/Tropina_01/).

СУНДИЕВ Игорь Юрьевич — главный научный сотрудник ВНИИ МВД России, профессор, доктор философских наук.

СМИРНОВ Алексей Анатольевич — ведущий научный сотрудник ВНИИ МВД России, доцент, кандидат юридических наук.

Ключевые слова: угрозы, Интернет, международный терроризм, экстремизм, «революция Твиттера», «революция Фейсбука», пропаганда в Интернете, внешняя политика США, политическая дестабилизация, «Фридом хаус», киберпреступность.

рассматривается многими террористическими и экстремистскими формированиями как один из ключевых инструментов реализации своих целей. «Завоевание информационного пространства — такова первоочередная задача, которую пытаются решить современные террористические организации», — отмечает российский исследователь В. А. Гарев[3].

Согласно отчету, составленному американским исследовательским Институтом мира — USIP (United States Institute for Peace), Всемирная Сеть (Интернет) является идеальной средой для деятельности террористов[4]. Того же мнения придерживается автор известного доклада «Как современные террористы используют Интернет» Г. Вейман, выделивший следующие способствующие этому факторы: свобода доступа; минимальное регулирование, цензура и другие формы государственного контроля или полное их отсутствие; огромная аудитория во всем мире; анонимность связи; быстрое движение информации; невысокая стоимость создания сайтов и обслуживания присутствия в Сети; мультимедийная среда, позволяющая комбинировать текст, графику, аудио и видео, возможность загружать фильмы, песни, книги, постеры и т. д.; возможность охватить также аудиторию традиционных СМИ, которые все чаще используют Интернет как источник сообщений[5].

В сложившейся ситуации особую значимость приобретает адекватная оценка текущего состояния использования информационных сетей в экстремистской и террористической деятельности и построение эффективного механизма ее постоянного мониторинга. В силу своей относительной новизны данная проблема в последнее десятилетие только начала находить отражение в научных трудах. Применительно к рассматриваемой нами проблеме, наибольший интерес представляют упомянутый специальный доклад Габриэля Веймана и работа Мауры Конвей «Использование террористами сети Интернет и борьба с этим явлением»[6], а также изданный под эгидой Международного союза электросвязи труд «Понимание киберпреступности: руководство для развивающихся стран»[7]. В них определяются причины и факторы использования террористическими и экстремистскими организациями сети Интернет, рассматриваются основные его направления и способы.

Интернет в деятельности террористических и экстремистских организаций: общая оценка

Глобальная информационная сеть Интернет получила важное значение в нашей жизни и завоевала огромную популярность. По данным компании «Pingdom», число людей, включенных в глобальную Сеть, к концу 2012 года составило 2,4 миллиарда; 62 процента пользователей Интернета пользуются социальными сетями[8]. Пребывание 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 года

[3] **В. А. Гарев**. Информационные угрозы современного международного терроризма. М., 2010. С. 6.

[4] *См.* «Интернет идеальная среда для террористов». — «SecurityLab.ru» (www.securitylab.ru/news/213806.php).

[5] *См.* **Г. Вейман**. Как современные террористы используют Интернет.

[6] *См.* **М. Конвей**. Использование террористами сети Интернет и борьба с этим явлением. — www.crime.vl.ru

[7] *См.* **М. Герке**. Понимание киберпреступности: руководство для развивающихся стран. — www.gosbook.ru/node/23462 /

[8] *См.* www.pingdom.com/monitoring/ru

превысило 1 миллиард человек. Число активных пользователей «Twitter» в декабре того же года составило 200 миллионов человек. На «Facebook» каждый день загружается 300 миллионов новых фотографий. На «YouTube» ежедневно происходит 4 миллиарда просмотров видеороликов.

Наша страна, в начале 2000-х годов находившаяся в числе аутсайдеров, совершила стремительный рывок и в 2012-м вышла по показателям численности интернет-пользователей на первое место в Европе. Согласно последним данным, приведенным аналитической компанией «TNS Россия» на конференции «i-COMference-2013», примерно 60 процентов населения России старше 12 лет хотя бы раз в месяц пользуется Интернетом, что составляет около 74,4 миллиона человек[9].

Наша страна, находившаяся в числе аутсайдеров в начале 2000-х годов, совершила стремительный рывок и в 2012 году вышла по показателям численности интернет-пользователей на 1-е место в Европе.

По разным данным, от 75 до 80 процентов россиян, пользующихся Интернетом, посещают социальные сети (*см.* табл. 1).

Таблица 1

Проникновение социальных сетей в России, 2010–2014 годы

	2010	2011	2012	2013	2014
Пользователи соцсетей (млн)	41,7	46,5	51,8	57,6	62,2
– изменений (в процентах)	19,4	11,6	11,3	11,2	8,1
– пользователей Интернета (в процентах)	74,2	75,0	76,2	78,0	79,0
– населения (в процентах)	29,9	33,5	37,5	41,9	45,5

Примечание: пользователи Интернет, использующие соцсети не реже раза в месяц с помощью любых устройств.

Источники: www.eMarketer.com. www.searchengines.ru/news/archives/chetvert_polzov.html

Как показало исследование «comScore», в августе 2011 года 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 миллионов пользователей. При этом ежедневно этой социальной сетью пользуются 38 миллионов человек. У социальной сети «Одноклассники» этот показатель равен 30 миллионам пользователей[10].

Столь обширная аудитория Интернета и колоссальные возможности распространения информации в Сети привлекли к себе внимание

[9] *См.* «Ежемесячно Интернетом пользуется около 60 процентов населения РФ старше 12 лет». — РИА «Новости». 05.03.2013 (http://ria.ru/society/20130305/925928196.html).

[10] *См.* «Фонд развития гражданского общества. Рунет сегодня, 2012».

террористических и экстремистских организаций. Сегодня все действующие террористические группы обнаруживают свое присутствие в Интернете[11]. К наиболее значимым организациям такого рода, активно использующим ресурсы Интернета, можно отнести ХАМАС, «Хезболла», «Аль-Джихад», «Братья-мусульмане» («Аль-Ихван аль-Муслимун»), «Народный фронт освобождения Палестины», «Конгрегел» (бывшая Рабочая партия Курдистана), «Реальная ИРА» (Ирландия) и ряд других. С помощью глобальной сети все эти организации решают свою главную задачу: при обеспечении наибольшего охвата потенциальной аудитории донести сообщение до каждого конечного потребителя быстро и без цензуры[12].

Как показывает проведенный нами анализ, начало активного использования Интернета террористическими и экстремистскими организациями в России можно отнести к началу 2000-х годов. В дальнейшем развитие данного процесса происходило в геометрической прогрессии. Эта негативная тенденция продолжает сохраняться и в настоящее время. Она тесно связана с развитием киберпреступности в Российской Федерации в целом.

В российском сегменте Интернета существует свыше 100 активно действующих интернет-сайтов российских радикальных структур. Как правило, они пропагандируют свои политические идеи, а также проводят агитационную и вербовочную деятельность, направленную на увеличение числа сторонников. Исследование показало динамику изменения (роста) количества субъектов террористической и экстремистской деятельности, использующих Интернет (*см.* табл. 2). Налицо резкий скачок в 2012 году. Эта тенденция сохраняется и в 2013 году.

Таблица 2

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

2009 год	2010 год	2011 год	2012 год
55,5	63,5	50,0	71,4

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 годах, 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 году значительно увеличилось количество выявленных противоправных деяний экстремистской направленности.

Отмеченная тенденция сохраняется и в настоящее время. В таких неформальных движениях манипулируют общественным сознанием, создают

[11] *См.* «The use of the internet for terrorist purposes». N. Y., United Nations, 2012.

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

образы борцов за права и свободы, подменяют факты и интерпретируют обстоятельства в свою пользу, что привлекает молодежь. Участники этих объединений скрывают свои противоправные устремления, но посредством Интернета в короткие сроки вовлекают многих граждан в свою деятельность. Пропагандируемая идеология подменяет морально-этические нормы общества, формирует асоциальные мировоззрение и поведение у своих сторонников. В то же время правоохранительная деятельность государственных органов преподносится ими как ущемляющая права гражданина.

Терроризм в сети Интернет — очень динамичное явление: сайты появляются внезапно, часто меняют формат, а затем так же 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. Террористические группы создают и многоязычные сайты, дабы оказать влияние на людей, напрямую не вовлеченных в конфликт. К примеру, баскская террористическая организация ЕТА предлагает информацию на испанском, немецком, французском и итальянском; шриланкийская группировка «Тигры освобождения Тамил Илам» публикует свои материалы на английском, японском и итальянском; «Исламское движение Узбекистана» — на узбекском, арабском, английском и русском языках. Движение «Талибан» размещает информацию на своих аккаунтах в социальных сетях «Facebook» (Фейсбук) и «Twitter» (Твиттер). С мая 2011 года страница в «Твиттере» помимо языка пушту ведется на английском. Двуязычие уже позволило движению привлечь на свою страницу в «Twitter» более 5,5 тысячи подписчиков.

Тенденции развития Интернета позволяют эффективно прогнозировать развитие возможностей террористических организаций по разработке и внедрению новых форм и методов информационно-психологического воздействия. В частности, это разработка специальных информационно-коммуникационных технологий (ИКТ) по подготовке и осуществлению так называемых «оранжевых революций», их апробация и активное использование на практике. Особую опасность данные ИКТ представляют в силу того, что экстремистские и/или террористические организации активно маскируются под *легальные демократические движения*. Причем на определенном этапе использования таких технологий может произойти их смешение. Примером является деятельность организации «Братья мусульмане» в Египте[13].

Основные направления и способы использования Интернета террористическими и экстремистскими организациями

В использовании Интернета как таковом (и особенно — социальных сетей) террористическими и экстремистскими организациями можно выделить два генеральных направления: *обеспечивающее* (пропаганда, сбор информации, связь, координация, вербовка, сбор денежных средств) и непосредственно *кибертерроризм*[14].

[13] Подробнее *см.*: **А. М. Васильев, Н. И. Петров**. Рецепты Арабской весны: Русская версия. М., 2012; **Эль Мюрид**. Если завтра война. «Арабская весна» и Россия. М., 2013; **Б. В. Долгов**. «Арабская весна»: итоги и перспективы. — www.perspektivy.info/book/arabskaja_vesna_itogi_i_perspektivy_2012-04-19.htm

[14] Подробнее *см.* «Threat assessment (abridged). Internet Facilitated Organised Crime. iOCTA. EUROPOL Public Information». 2012.

Г. Вейман выделяет 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[15]. Интернет-ресурсы, включая социальные сети, дают уникальные возможности террористическим и экстремистским организациям *конспиративно получать развернутую информацию* практически по любому физическому и юридическому лицу. Персонально воздействовать на значительное количество индивидов, одновременно *управлять группами лиц*, не вступая с ними в непосредственный контакт. *Оказывать своим сторонникам и нужным им субъектам финансовую и иную поддержку*, *вести* максимально открытую и развернутую *пропаганду своих идей*, активно *участвовать в легальной деятельности различных государственных структур*, а также совершать сопутствующие экстремистской и террористической деятельности экономические, общеуголовные и иные преступления. ИКТ дают экстремистским и террористическим организациям широкий спектр возможностей: *свободный легендированный доступ* к необходимым ресурсам, большую аудиторию, анонимность, быстрое движение информации, дешевизну создания сайтов и их обслуживания, богатую мультимедийную среду, а также возможность использования СМИ, создания аудио- и видеоканалов. Все вышеперечисленное делает Интернет идеальной средой для противоправной деятельности террористических и экстремистских организаций.

Наиболее широко террористические и экстремистские организации в Интернете осуществляют *пропаганду своих идей*. К основным источникам пропаганды в сети Интернет относятся разнообразные интернет-порталы (это официальные и неофициальные СМИ, сайты организаций и др.); интернет-форумы различной направленности, блогосфера и, конечно же, видео-хостинги, поскольку видеоматериал является наиболее эффективным средством передачи информации, особенно в молодежной среде. По наблюдениям В. В. Горбатовой, в этом отношении идеологами «Аль-Каиды» особо подчеркивается важность последовательного ведения так называемого медиа-джихада[16].

Данный перечень далеко не исчерпывающий и постоянно изменяется. Так, в настоящее время террористическими и экстремистскими организациями наиболее широко стали использоваться социальные сети в силу их высокого уровня самоорганизации и возможности легендирования преступной деятельности.

Важнейшими факторами бесконтрольного распространения незаконных, экстремистских и террористических течений в сети Интернет является *условная обезличенность* и, как следствие, фактическая безнаказанность лиц, которые участвуют в интернет-пропаганде. Обезличенность в сети Интернет приводит к тому, что установить реальные данные и привлечь к ответственности технически подготовленного террориста в ряде случаев не представляется возможным даже с применением современных средств ведения ОРД. Кроме того, даже рядовые участники экстремистских движений с использованием современных программных средств без особого труда могут скрыть свое реальное местоположение. Так, летом 2012 года администрация «Кавказ-Центра» разместила

[15] *См.* **Г. Вейман**. Как современные террористы используют Интернет.

[16] *См.* **В. В. Горбатова**. Информационно-пропагандистская политика радикальных исламских организаций (на примере ХАМАС, «Хизбаллы» и «Аль-Каиды»). С. 24.

копию своего ресурса в общедоступной *сети анонимизации* «Tor», и тем самым предоставила пользователям с территории Российской Федерации возможность получить свободный, анонимный доступ к информации, размещенной на своих страницах.

В качестве примера: если экстремисту необходимо разместить материал на существующих интернет-ресурсах, к примеру, в социальных сетях, блогах или форумах, то анонимность процесса может обеспечиваться:

— во-первых, посредством беспроводного доступа (зачастую бесплатного) в общественных местах (кафе, гостиницах, парках, развлекательных комплексах);

— во-вторых, использованием средств анонимизации (таких, как «Tor», SOCKS, I2P), которые предоставляют возможность спрятать основной след, ведущий к источнику материала, его сетевому IP-адресу;

— в-третьих, если необходимо развернуть не отдельный пропагандистский материал на уже существующем ресурсе, а целый портал для ведения пропаганды, то для этого можно прибегнуть как к использованию бесплатных хостинг-площадок, так и к анонимной аренде площадок платных, с использованием электронных платежных систем, не обеспечивающих должного уровня проверки каждого пользователя их сервисов;

— в-четвертых, возможность использования в своих интересах противоречий в законодательствах стран мира в области «компьютерного права». Например, если в одной стране размещенный в Интернете материал будет признан экстремистским и подлежащим блокированию, то это не означает, что власти другой страны окажут содействие в приостановке его деятельности. Самым известным для России примером является сайт чеченских сепаратистов «Кавказ-Центр», успешно работавший на шведских, а ныне действующий на американских хостинг-площадках.

Другим следствием обезличенности, часто используемым в пропаганде экстремистских течений в сети Интернет, является технология «раздувания авторитета», используемая в манипулировании сознанием неопытных пользователей. В отличие от известных медийных экспертов, часть псевдоавторитетных блогеров (популярность которых особенно активно растет в сложные, нестабильные периоды политической и социальной напряженности) является чисто виртуальными персонами. Зачастую их авторитет поддерживается такими же виртуальными авторитетами, появившимися и «раскрутившимися» в критически значимый момент.

Ярким примером использования виртуальной личности для влияния на мнения интернет-пользователей является ситуация, связанная с высказываниями блогера, назвавшего себя «Девушка-гей из Дамаска», на основании которых некоторые эксперты делали выводы о ситуации в Сирии в 2011 году. При этом на размещенном в блоге фото была изображена английская гражданка Елена Лечич, узнавшая об этом только тогда, когда история получила широкую огласку. Точно так же под именем блогера «Амина Абдаллarраф» скрывался гражданин США Том Макмастер, обучавшийся в университете в Эдинбурге (Шотландия). Как выяснилось, информацию блогер черпал от своей супруги, которая пишет докторскую диссертацию о сирийской экономике.

Используя современные средства анонимизации и обладая достаточным опытом работы в ведении скрытой пропаганды, иностранному эксперту не составит большого труда выдать себя за авторитетного жителя республики Северного Кавказа, а компрометирующим его действия фактором может послужить только плохое знание языка.

Что касается *кибертерроризма*, то под ним, 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[17]. 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 они не ограничатся только киберпространством, а затронут объекты реального мира — такие, как системы жизнеобеспечения городов, объекты авиа-, морского (речного) и железнодорожного транспорта, атомной энергетики и т. д., что наглядно продемонстрировал вирус «Stuxnet». Как известно, его атаке в 2010 году подверглись программируемые логические контроллеры иранской АЭС в Бушере, в результате которой был нарушен процесс их функционирования. Как отмечается в обзоре развития киберугроз в 2010 году, подготовленном «Лабораторией Касперского» («Kaspersky Security Bulletin 2010»), данный пример свидетельствует о том, что существовавшая ранее грань между виртуальным и реальным миром фактически стерлась.

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», «троянские кони» и «логические бомбы». Они способны 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 ПК, где установлена подобная программа.

Масштабных актов кибертерроризма пока еще зафиксировано не было. Однако представляется, что это лишь вопрос времени. Экспертные оценки и моделирование 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. Тот за час добился доступа и полного контроля над системой и осуществил добавление оговоренных химических веществ в воду[18]. В начале 2013 года 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. Эти примеры демонстрируют потенциальные возможности террористических структур в киберпространстве[19].

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 определен-

[17] *См.* **А. В. Федоров**. Информационная безопасность в мировом политическом процессе. Учебное пособие. М., 2006. С. 111.

[18] *См.* **Ю. А. Семенов**. Сетевые угрозы. — «Экономические стратегии». 2013. № 3. С. 51.

[19] *См.* «Теперь с мобильного можно перехватить управление самолетом». — «Вести.net». 12.04.2013 (http://hitech.vesti.ru/news/view/id/1759).

ного государства в соответствии с полученными директивами, выполняя тем самым «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[20].

Государствам—заказчикам таких операций это дает возможность избежать ответственности за свои действия. При этом для обеспечения успеха операции они могут передавать 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.* Такая форма действий терроризма уже получила широкое распространение в мире. Например, авторы статьи «Сетевые медиабои на Ближнем Востоке» в качестве примера одного 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 Аль-Акса в Иерусалиме. Другой пример, указанный в статье, — хакерская атака марокканской группы «Team Evil» на более чем 750 израильских сайтов. На атакованных ресурсах ими был размещен текст: «Вы убиваете палестинцев, мы убиваем серверы»[21].

Подобной атаке подвергалась и наша страна. Сирийские хакеры из группы «Syrian Revolution Electronic Suite» взломали сайт полномочного представительства президента по Дальневосточному федеральному округу РФ и разместили на нем обращение к российскому народу. Злоумышленники попросили россиян отказаться от поддержки президента Сирии Башара Асада и прекратить поставки Дамаску тяжелого вооружения. Сетевые злоумышленники также принесли свои извинения «всем хорошим русским людям» за взлом портала. В свою очередь, сторонники сирийского лидера Б. Асада осуществили взлом аккаунта «Agence France Press (AFP)» в «Twitter». Хакеры потребовали объективного освещения ситуации в Сирии[22].

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

[20] *См.* «Доклад правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности». Нью-Йорк, Организация Объединенных Наций, 2012.

[21] *См.* **В. И. Газетов, М. Н. Ветров**. Сетевые бои на Ближнем Востоке. — «Независимое военное обозрение». 2013. № 27.

[22] *См.* «Сирийские хакеры взломали сайт дальневосточного полпредства». — «РБК». 18.03.2013 (http://top.rbc.ru/society/18/03/2013/849534.shtml).

ресурсами, необходимыми для решения масштабных задач, было под силу лишь несетевым, жестким вертикальным структурам с четким управлением. Ключевое отличие сегодняшней ситуации состоит в том, что благодаря цифровым сетевым технологиям 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»[23].

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 одним 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 года (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 «Facebook», 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»[24].

25 января 2010 года 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 «Facebook», «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», группы сопротивления,

[23] *См.* **М. Кастельс**. Информационная эпоха: экономика, общество и культура, 2000.

[24] **В. Гоним**. Революция 2.0: документальный роман. Пер. с англ. Т. Даниловой. СПб., 2012. С. 93.

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» для атаки правительственных сайтов. Если верить одному из парижских членов этой группы, пожелавшему остаться анонимным, атака была успешной. Немало официальных сайтов оказалось в самом деле недоступными в тот день. «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»[25].

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[26]. Для посетителей социальных сетей создавалось впечатление, что в протестные действия включились миллионы людей. Однако в действительности число *реально протестующих и протестующих в Сети* разнится многократно. Достигается это с помощью специальных программ. В 2010 году правительство США заключило договор с компанией «HBGary Federal» на разработку компьютерной программы, которая может создавать многочисленные фиктивные аккаунты в социальных сетях для манипулирования и влияния на общественное мнение по спорным вопросам, продвигая пропаганду. С февраля 2011 года эта программа активно используется и распространяется. Она также может быть применена 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 заказала 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»[27]. 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», что активно используется сейчас для борьбы против правящего режима в Сирии и ранее, в 2011—2012 годах, организацией «Движение белых ленточек» в Москве.

В настоящее время отработанный механизм использования социальных сетей террористическими и экстремистскими организациями представляет реальную угрозу Российской

[25] «"Opération Tunisia": la cyberattaque d'Anonymous aux côtés des manifestants». — «Liberation». 12.01.2011.

[26] Методика и программные продукты были разработаны и внедрены американскими НПО. Подробнее *см.* «Руководство в помощь пользователям интернета в репрессивных государствах. Доклад-презентация пособия. 12.04.2011». — www.freedomhouse.com/

[27] «Army of Fake Social Media Friends to Promote Propaganda». — «PCWorld». 23.02.2011.

Федерации. Эксперты высказываются о возможности апробации данного механизма на иных странах ближнего окружения России. В нашей стране направленность использования социальных сетей террористическими организациями связана с очагами тлеющих этнических конфликтов. Прежде всего речь идет о Республике Дагестан. Правоохранительными органами Российской Федерации периодически фиксируются факты появления новых интернет-ресурсов, пропагандирующих радикальные религиозные течения, с целью вовлечения лиц в незаконные вооруженные формирования.

Пути ограничения доступа к интернет-сайтам террористической и экстремистской направленности

На протяжении последних лет в российском обществе ведутся дискуссии о допустимых границах государственного регулирования контента в Интернете. Одним из последствий этих дискуссий стало принятие Федерального закона № 139-ФЗ от 28 июля 2012 года «О внесении изменений в Федеральный закон "О защите детей от информации, причиняющей вред их здоровью и развитию" и отдельные законодательные акты Российской Федерации» (известного как «Закон о черных списках интернет-сайтов»). Во время дебатов по поводу этого закона и его сторонники, и противники, которые составляют большинство среди лидеров мнений российского сегмента Интернета, активно апеллировали к международному опыту регулирования Сети.

Следует, однако, подчеркнуть, что, вопреки устоявшемуся мнению, ограничения в области интернет-контента являются прерогативой не только авторитарных и тоталитарных политических режимов. На деле практически все крупные страны мира в той или иной мере ограничивают доступ своих граждан к нежелательной, по мнению властей, информации в Сети — будь то социально опасная информация, нелицензионный контент или экстремистские материалы[28].

Методы ограничения контента в Интернете можно разбить на две категории: нетехнические и технические. К категории нетехнических относятся законы, запрещающие публикацию того или иного контента, давление на интернет-провайдеров, владельцев сайтов и пользователей с целью заставить их убрать нежелательные материалы или изменить их[29]. К категории технических методов относится блокирование интернет-ресурсов по IP-адресу, искажение DNS-записей, блокирование сайтов по URL, пакетная фильтрация, фильтрация через HTTP прокси-сервер, нарушение работы Сети и фильтрация результатов поиска. Для повышения эффективности механизмов цензуры также активно используются различные методы сбора информации в Интернете. Из-за сложности и несовершенства технических инструментов обхода фильтров к ним прибегают не более 2 процентов пользователей даже в тех государствах, где фильтрации подвергается большое число интернет-ресурсов.

Принятый в России Федеральный закон № 139 учредил *Единый реестр доменных имен, указателей страниц сайтов в сети Интернет и сетевых адресов, позволяющих идентифицировать сайты в сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено* (далее — Реестр). Реестр расположен в Интернете по ад-

[28] *См.*, например: «Фильтрация контента в Интернете. Анализ мировой практики». М., Фонд развития гражданского общества, 2013.

[29] Отдельная группа методов — оперативно-розыскные.

ресу zapret-info.gov.ru; его оператором является Роскомнадзор России. Помимо трех основных выделенных в законе категорий вредной информации (детская порнография, информация о наркотиках, пропаганда суицида), в Реестр также включаются доменные имена и (или) указатели страниц сайтов в сети Интернет, а также сетевые адреса сайтов, содержащих информацию, распространение которой в Российской Федерации запрещено. Под эту категорию попадают публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма и иные экстремистские материалы. Процессуальным основанием для их включения в Реестр выступает вступившее в законную силу решение суда.

После первичного решения оператора Реестра о включении в него соответствующей записи указателя страницы сайта в сети Интернет, содержащей запрещенный контент, вступает в действие трехступенчатый механизм реагирования, предусматривающий последовательное осуществление следующих шагов: 1) уведомление владельца сайта о наличии в нем запрещенной информации и принятие им мер по удалению такого контента; 2) ограничение провайдером хостинга доступа к сайту в сети «Интернет», содержащему запрещенную информацию; 3) внесение записи в Реестр сетевого адреса, позволяющего идентифицировать сайт в сети Интернет, содержащий запрещенную информацию, и ограничение доступа к такому сайту со стороны оператора связи (интернет-провайдера). При этом каждая последующая стадия реализуется только в том случае, если предыдущая не дала желаемого результата. Как видно, финальным результатом может стать блокирование доступа к сайту по сетевому (IP) адресу. Важным достоинством данного метода является возможность блокирования доступа к сайтам, размещенным на зарубежных хостинг-площадках, чем часто ранее пользовались террористические и экстремистские организации во избежание мер ответственности.

Учреждение Реестра и введение его в действие (это произошло 1 ноября 2012 года) стало важным шагом на пути совершенствования механизма противодействия распространению экстремистской информации в сети Интернет. Однако противники соответствующего закона обнаружились не только внутри страны, но и за рубежом. Дело в том, что США рассматривают Интернет как важный инструмент продвижения своих национальных интересов посредством поддержки оппозиционных сетевых активистов в тех странах, политический режим которых представляет угрозу для реализации таких интересов. Поэтому попытки фильтрации интернет-контента и иного ограничения доступа к нему рассматриваются как препятствие, требующее устранения. 12 апреля 2011 года на конференции в штаб-квартире организации «Фридом хаус» в Вашингтоне был представлен подготовленный этой организацией доклад «Руководство в помощь пользователям Интернета в репрессивных государствах». В ходе нее заместитель помощника государственного секретаря США Дэниел Бэр, возглавляющий Бюро по демократии, правам человека и труду, прямо назвал инструменты преодоления цензуры «самым важным способом поддержки цифровых активистов и других пользователей, живущих в обстановке репрессий и зажима Интернета»[30].

Ранее, в своей речи, произнесенной 15 января 2010 года, государственный секретарь США Хиллари Клинтон назвала ограничения в Интернете новыми стенами, разделяющими мир,

[30] www.freedomhouse.com/

и прямо заявила о поддержке Соединенными Штатами свободы выражения мнения в Интернете, дабы помочь «людям, которым затыкают рот деспотические правительства»[31]. По ее словам, Государственный департамент потратил на эту работу более 20 миллионов долларов, а в 2011—2012 годах намеривался израсходовать еще 60 миллионов. Там же анонсировался новый проект «революции гаджетов» с использованием технологий стелс-интернета.

Цель программы стелс-интернета — обойти запреты на пользование Интернетом и даже мобильными SMS, которые ряд правительств вводили в момент беспорядков в их странах. Подобные ограничения были введены весной—летом 2011 года в Сирии, Ливии, Египте и Иране. Стелс-станции, похожие на чемоданы с антеннами, предназначены для моментального доступа в Мировую паутину в районах массовых беспорядков. Как сообщают американские источники, агенты США уже заложили целые партии вместе с модернизированными мобильниками в землю в условленных местах в «проблемных странах» — для пользования «группами диссидентов в час X»[32]. Таким образом, правительства не смогут перекрыть протестующим информационный кислород, лишив их сотовой связи и доступа к Интернету, и последние смогут координировать свои действия друг с другом.

Другой проект, который опирается на технологии «Mesh Network», объединяют мобильные телефоны, смартфоны и персональные компьютеры для создания невидимой беспроводной сети без центрального концентратора — каждый такой телефон действует в обход официальной сети, то есть напрямую. Сообщается, что опытные включения такой «шпионской» сети уже производились в Венесуэле и Индонезии в 2012 году.

Приведенные примеры свидетельствуют о том, что ограничение доступа к определенным интернет-ресурсам экстремистского характера, равно как и иные методы информационной изоляции и подавления, имеют ограниченную эффективность в борьбе с использованием сети Интернет в деятельности террористических и экстремистских организаций и могут быть успешно преодолены. В связи с этим требуется выработка и реализация комплекса иных мер противодействия данной угрозе, важнейшими из которых являются меры информационного реагирования и контрпропаганды. Другими словами, правоохранительным органам и спецслужбам необходимо учиться вести информационную войну с террористическими и экстремистскими формированиями в Интернете.

Все изложенное выше позволяет сделать однозначный вывод: противодействие использованию информационных сетей террористическими и экстремистскими организациями, защита важнейших информационных инфраструктур от кибератак приобретают ключевое 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. ◆

[31] **H. R. Clinton**. Remarks on Internet Freedom. Washington, U.S. State Department, 21.01.2010. — www.state.gov/secretary/rm/2010/01/135519.htm

[32] *См.* **Ю. Алехина**. Америка готовит мировую интернет-войну. — «Комсомольская правда». 28.07.2011 (www.kp.ru/daily/25727.4/2717471/).