РИСКИ И УГРОЗЫ ИНФОРМАЦИОННОГО ТЕРРОРИЗМА В РОССИИ

А. В. Россошанский[1]

В статье рассматриваются основные виды информационного терроризма и связанные с ним угрозы информационной безопасности России, оценивается степень их опасности и вероятность возникновения.

Ключевые слова: кибертерроризм, информационный терроризм, информационная безопасность.

In this article the main kinds of informational terrorism and the threats to the informational safety in Russia are considered. Also the degree of their danger and the possibility of emerging are evaluated.

Key words: ciberterrorism, informational terrorism, informational safety.

Развитие Интернета не только обогатило общественно-политическую жизнь полезными технологиями, новыми формами социально-политической коммуникации, популярность которых постоянно растет, но и породило ряд сложных проблем в сфере информационной и национальной безопасности. К их числу относится и информационный терроризм. В России проблема терроризма, борьбы с ним стоит особенно остро, о чем свидетельствуют события не только на Северном Кавказе, но и в других регионах страны. Как показывает практика, в своей деятельности террористы стремятся использовать самые современные средства связи, различные коммуникационные каналы, в том числе и Интернет. В этой связи представляется интересным анализ рисков и угроз информационного терроризма в России с последующей оценкой их степени реальности и опасности.

Информационный терроризм — это новая разновидность террористической деятельности, основанная на последних достижениях науки и техники в области компьютерных и информационных технологий. Террористические организации и группировки по всему миру используют их в самых разных целях. Поэтому содержание понятия «информационный терроризм» носит весь-

[1] Россошанский Андрей Владимирович – кандидат политических наук, доцент кафедры политических наук Саратовского государственного университета им. Н.Г. Чернышевского. Эл. почта: up@gtrk.renet.ru.

ма широкий характер. В экспертном научном сообществе принято выделять два вида информационного терроризма. Одной из его разновидностей является кибертерроризм. Он представляет собой использование компьютерных сетей в качестве средства для нарушения функционирования важнейших национальных инфраструктур (энергетических, транспортных, правительственных), принуждения или запугивания правительства и гражданского населения [7]. По своему смыслу деятельность кибертеррористов очень напоминает деятельность компьютерных хакеров, в связи с чем между ними не всегда проводится четкая грань и иногда даже ставится знак равенства. Однако в отличие от хакеров кибертеррористы руководствуются политическими мотивами атак на информационно-компьютерные системы и ставят принципиально иные цели.

Некоторые исследователи определяют кибертерроризм с помощью соединения двух понятий «киберпространство» и «терроризм», основываясь на логике российского законодательства. Кибертерроризм рассматривается или как умышленная атака на компьютеры, компьютерные программы, компьютерные сети или обрабатываемую ими информацию, создающая опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных общественно опасных последствий [10].

Другая разновидность информационного терроризма подразумевает использование Интернета террористическими группами для имущественного, финансового, информационного и прочего обеспечения своей деятельности, но не для непосредственного совершения терактов. Известный американский террорolог Габриэль Вейман выделяет восемь способов использования Интернета террористами: 1) проведение психологической войны; 2) поиск информации; 3) обучение террористов; 4) сбор денежных средств; 5) пропаганда; 6) вербовка; 7) организация сетей; 8) планирование и координирование террористических действий [2]. Такой широкий спектр возможностей означает, что Интернет в силу своих функциональных особенностей (открытость, масштабность, неподцензурность, быстрота и т. д.) служит идеальным полем деятельности террористических организаций.

Современное общество неумолимо становится информационным, растет число пользователей, подключенных к Интернету, удовлетворяющих с его помощью самые разнообразные интересы, расширяется спектр электронных услуг, все больше зависит от компьютерных сетей работа важнейших инфраструктур (правительственных, банковских, транспортных, социальных и т. д.). Это обстоятельство уже сегодня порождает миф о полной зависимости жизнеобеспечения человека от информационно-компьютерных технологий и соответственно миф о страшной угрозе кибертерроризма и его ужасных последствиях. Многие исследователи необоснованно завышают риски угроз информационного терроризма, считая, что он несет опасную угрозу для чело-

вещества, сравнимую с ядерным, бактериологическим и химическим оружием [12], и способен продуцировать системный кризис всего мирового сообщества, особенно стран с развитой инфраструктурой информационного обмена [3].

На практике же результаты деятельности кибертеррористов существенно отличаются от многочисленных устрашающих сценариев. В основном они сводятся к «вирусным» атакам информационных ресурсов, «взлому» правительственных сайтов с целью нарушения их работы или размещения на них лозунгов и призывов, подобно граффити на стенах домов. Очевидно, что прямой опасности жизни людей такая деятельность не несет, хотя материальный ущерб может быть весьма значительным. Однако это относится главным образом к сфере интересов компьютерных хакеров, которые стали серьезным источником угроз информационной безопасности. Ежегодно во всем мире от их деятельности страдают миллионы людей. Они наносят немалый материальный ущерб рядовым гражданам, бизнесу и государственным институтам. Как правило, чаще других IT-преступлений совершаются мошенничества с пластиковыми платежными карточками, хищения денежных средств с банковских счетов, несанкционированный доступ к компьютерной информации и нарушения правил эксплуатации автоматизированных электронно-вычислительных систем, распространение компьютерных вирусов. Причем количество преступлений в этой сфере с каждым годом только увеличивается. Так, в России за первое полугодие 2009 г. 60% всех преступлений, совершенных с использованием телекоммуникаций, были связаны с Интернетом [6]. Но это скорее проблема киберпреступности, а не кибертерроризма.

Потенциальными мишенями для кибертеррористов служат подключенные к Интернету компьютерные системы управления так называемой критической инфрастуктурой, прежде всего транспортом, энергетикой и водоснабжением. Как показывает анализ ведущих экспертов, важнейшие системы обеспечения при рыночной экономике более распределены, разнообразны, избыточны и способны к самовосстановлению, чем может показать поверхностная оценка, что делает их менее уязвимыми к нападениям. Во всех случаях кибератаки менее эффективны и разрушительны, чем физические нападения. Фактически при нынешнем уровне информационного развития западного общества кибератаки являются не угрозами национальной безопасности, а скорее ее раздражителями. По наносимому ущербу такие атаки сопоставимы с периодически неизбежно возникаемыми сбоями, например, в системе электроснабжения, и не более того [7].

В России многие инфраструктуры жизнеобеспечения в силу своей изношенности и, как следствие, высокотехнологического отставания от Запада в еще меньшей степени подвержены несанкционированному дистанционному управлению через Интернет. Что же касается стратегических объектов — АЭС, ГЭС, ядерного оружия и т.д., то ввиду их изолированности, автономности

и секретности это просто невозможно. На наш взгляд, кибертерроризм может стать реальной угрозой национальной безопасности только в очень отдаленном будущем, когда уровень информатизации будет всеобъемлющим, государство станет «электронным», а общество информационным. Для этого сегодня прикладывается немало усилий: приняты Стратегия развития информационного общества в Российской Федерации, Концепция формирования электронного правительства и ряд других важных документов.

Одна из главных целей государственной политики в сфере информатизации — сократить цифровой разрыв между Россией и ведущими странами Запада. В рейтинге развития информационно-коммуникационных технологий, составляемом Международным союзом электросвязи, Россия в 2008 г. из 159 стран мира занимала 48 е место. Индекс развития ИКТ (IDI), включающий 11 показателей и охватывающий такие характеристики, как доступ к ИКТ, использование ИКТ и навыки в области ИКТ, равнялся 4,54 балла [4].

По самым же последним данным, согласно ежегодно составляемому рейтингу консалтингового подразделения журнала The Economist — Economist Intelligence Unit, наша страна находится в еще более удручающем положении. В рейтинге 2010 г. из 70 стран, в которых оценивалась готовность перехода к информационному обществу, Россия находится на 59-м месте, т. е. позитивные изменения за год не были выявлены. В данном исследовании индекс готовности России к электронному развитию оценивается в 3,97 балла. Оценка проводилась по десятибалльной шкале и складывалась из шести показателей: развитие коммуникационной инфраструктуры; состояние бизнес-среды, состояние социальной и культурной среды в стране, политика государства и его видение развития сектора ИКТ, правовое обеспечение электронного развития, уровень ИТ в частном и корпоративном секторах [14]. Полученные данные свидетельствуют о том, что уровень информатизации нашего государства остается все еще очень низким, следовательно, риски совершения кибертеракт минимальны, так как потенциальных мишеней для террористов очень мало и ущерб, который они могут нанести, весьма незначителен.

При низком международном рейтинге России нельзя отрицать стабильного ежегодного прироста интернет-аудитории в нашей стране. Так, регулярные исследования, проводимые Фондом «Общественное мнение», свидетельствуют о постоянном росте числа интернет-пользователей в России. По данным последнего исследования «Интернет в России», зимой 2010–2011 года доля интернет-пользователей среди взрослого населения составила 43% (50 млн чел.). При этом трое из каждых десяти пользователей составляют активную аудиторию — выходят в сеть хотя бы раз в сутки. Общая численность активной интернет-аудитории к концу 2010 г. достигла 36 млн чел. Среднеквартальный рост интернет-аудитории за 2010 г. в целом по стране для месячной, недельной и суточной аудиторий составил соответственно 4, 5 и 8%. При сохранении суще-

ствующих тенденций в развитии и распространении Интернета к концу 2014 г. число пользователей вырастет приблизительно на 30 млн чел. и приблизится к 80 млн чел., или 71% населения страны старше 18 лет [5]. Это обстоятельство фактически означает превращение Интернета в недалеком будущем в полноценное средство массовой информации и коммуникации, что значительно увеличит его пропагандистский потенциал. Увеличатся и риски, связанные с пропагандой экстремистами и террористами своих идей через Интернет.

Как показывает практика, Интернет уже сегодня активно используется экстремистскими силами, что придает реальные очертания данному виду угрозы. С помощью специализированных интернет-сайтов (http://www.kavkazcenter.com; http://www.chechenpress.info; http://www.jamaatshariat.com/; http://www.national-socialist.tk) осуществляются призывы к насильственным действиям, пропагандируются идеи радикального ислама, национализма, сепаратизма, религиозного превосходства и т. д. Так, по данным Министерства юстиции Российской Федерации, более 10 русскоязычных интернет-сайтов включено в федеральный список экстремистских материалов, запрещенных для распространения на территории России [13].

Помимо интернет-сайтов для пропаганды и поиска сторонников активно используются популярные социальные сети. В списке экстремистских материалов Министерства юстиции Российской Федерации значится около десятка персональных страниц пользователей в популярных социальных сетях «ВКонтакте», «Живой журнал» (livejournal.ru). И это не случайно. На сегодняшний день регистрация персональных страниц доступна всем желающим и не представляет никаких сложностей. Достаточно выполнить несколько простых стандартных процедур, затратив совсем немного времени, и вы получаете отличный инструмент общения в реальном времени, без каких-либо временных и пространственных ограничений, позволяющий охватывать миллионные аудитории.

Кроме социальных сетей растет популярность таких интернет-ресурсов, как видеохостинги (запрещены к просмотру несколько видеофайлов на «bashtube» и «YouTube»), а также форумы. Все это свидетельствует о том, что радикальные силы и отдельные элементы, исповедующие идеи массового насилия, для достижения своих целей используют все имеющееся сегодня многообразие интернет-сервисов. Это позволяет им компенсировать свою ресурсную недостаточность — преодолеть информационную и структурно-организационную ограниченность, а также минимизировать финансовые затраты.

Сайты экстремистских сил связывают в интернет-сети группы родственных экстремистских организаций протеррористического типа. Например, исламистские организации образуют в Интернете особое локализованное виртуальное информационное пространство джихадистской направленности.

В. Б. Петухов называет его парадоксальным словосочетанием «djihad-net» [9, с. 175]. Аналогично структурируются националистские и сепаратистские организации, создавая виртуальные коммуникационные сети и соответствующие им информационные пространства. Они представляют собой динамичную систему, хорошо адаптирующуюся к внешней среде, постоянно меняющую свою конфигурацию: одни сайты закрываются, взамен старых открываются новые и т. д. Фактически искоренить их представительства из виртуального пространства не представляется возможным. Методы классической либеральной демократии бессильны перед этой информационной угрозой.

Следует заметить, что для экстремистских и террористических сил интернет-коммуникация служит очень привлекательным инструментом воздействия на общественное мнение в силу ее больших манипулятивных возможностей. Скрытая опасность Интернета и других интерактивных кибернетических систем заключается в том, что, в отличие, к примеру, от телезрителя, пользователь сети психологически уверен в свободе своего информационного выбора, в невозможности манипулирования его поведением со стороны других сетевых субъектов. Кроме того, Интернет позволяет задействовать гораздо более широкий инструментальный спектр информационной стимуляции сознания и подсознания индивида, чем печатные СМИ и даже телевидение: звук, визуальный ряд (причем активный) с огромной палитрой красок и геометрических построений, текстовый материал (эта форма подачи данных апеллирует к логике реципиента), а также интерактивная обратная связь, порождающая у объекта манипуляции чувство причастности к происходящему [8, с. 142].

Экспериментально установлено, что лишь 13–14% потребителей печатной и телевизионной общественно-политической информации способны адекватно воспринимать предлагаемые им данные, т. е. более или менее четко выявлять в прочитанном или увиденном политический заказ [1, с. 43–44]. И это при том, что и читатель, и телезритель все же осознают себя пассивными выборщиками информационного канала, ибо вынуждены смотреть и читать то, что предлагает указанное СМИ. Пользователь Интернета считает себя активным выборщиком, поскольку убежден, что попал на данный информационный ресурс самостоятельно, в соответствии со своими интересами и волен обратиться к альтернативным источникам в любой момент. Это, как считается, может серьезно понизить порог рационально-критического восприятия информации.

На наш взгляд, недооцененными на сегодняшний день являются риски, связанные с проведением экстремистскими, террористическими силами политически мотивированных информационно-психологических атак с целью дестабилизации политической системы государства, социально-психологической обстановки в регионе или в стране в целом.

Эта разновидность информационного терроризма представляет собой воздействие на психику и сознание людей в целях дискредитации политических институтов власти, подрыва доверия к ним у населения, формирование в сознании людей состояния неопределенности и неуверенности в завтрашнем дне. Такое насильственное информационное воздействие на психику не оставляет человеку возможности для критической оценки полученной информации. В качестве источников подобного рода атак могут выступать не только экстремистские, террористические организации и силы, но и политические противники (как отдельные личности, так и государства). Масштаб атак может варьироваться от регионального до государственного.

В качестве основы такого информационно-психологического воздействия чаще всего используются слухи, которые содержат информационную бомбу, способную вызвать страх, панику и массовую истерию в обществе. Это может быть сообщение о технологической катастрофе или о вспыхнувшей эпидемии или еще что-нибудь в этом же духе. В данном случае достигается максимальный эффект. В качестве примера можно привести ситуацию, которая возникла в Саратовском регионе. Осенью 2004 г. в саратовские СМИ был запущен слух об аварии на Балаковской АЭС, который моментально всколыхнул все Поволжье. Как выяснилось в дальнейшем, определенные неполадки на АЭС действительно были, но они не несли угрозы жизнедеятельности людей, а допускались проектным планом, для их устранения были предусмотрены все технические возможности. По заявлению официальных лиц, подобные остановки блоков на БАЭС уже были, но они никогда не вызывали такого ажиотажа [11]. По слухам же, страну ждал чуть ли не новый Чернобыль, а в Интернете даже появился сайт (aesbalakovo.narod.ru), где были размещены ложные сообщения о погибших и раненых, с фотографиями плохого качества. Так же на сайте сообщалось о распространении радиационного облака в сторону соседних областей. В результате в Балаково, Саратове и ряде других городов Поволжья началась массовая паника населения. Люди стали скупать йод в аптеках, забирать детей из детских садов, изолироваться в собственных квартирах, в некоторых учебных заведениях были отменены занятия и т. д. В данном случае в качестве информационной бомбы был использован слух о техногенной катастрофе.

Другой информационный взрыв произошел в информационном пространстве Саратовской области в декабре 2009 г., когда в интернет-СМИ появилась информация о вспышке легочной чумы, о закрытии города на карантин и санитарной обработке зараженной территории с воздуха. Первая информация на эту тему появилась на интернет-сайтах информационных агентств «Четвертая власть», «Взгляд-инфо», «Rumorologi» и интернет-блогах. В частности, получил широкую известность в дальнейшем удаленный «живой журнал» одного из студентов СГМУ, в котором упоминалось о признаках легочной чумы у умерших. Затем информация стремительно стала распространяться

через неформальные каналы, сети межличностного общения, главным образом через звонки родственникам и знакомым, а также через интернет-форумы. Тем самым реализовывалась двухступенчатая модель коммуникации, когда информация через интернет-СМИ воздействовала на так называемых лидеров мнения, а те в свою очередь распространяли ее дальше, усиливая воздействие первичной информации.

Особенность запущенного слуха заключалась еще и в том, что он вызвал эффект коммуникационного резонанса. Во-первых, общество (т. е. адресат сообщения) уже заранее в неявном виде было готово к сообщениям подобного рода, так как именно в этот период наблюдалась вспышка заболеваний, вызванных высокопатогенными штаммами вируса гриппа. Фиксировались и придавались огласке случаи летального исхода заболеваний. Во-вторых, СМИ активно поддерживали эту «повестку дня», не только подробно освещая деятельность городского штаба по борьбе с гриппом, но и распространяя ложные слухи со ссылками на достоверные источники. Так, в новостной ленте «Взгляд-инфо» со ссылкой на областную службу спасения сообщалась, что опрыскивание действительно запланировано, и ночью в воздух должны подняться вертолеты с дезинфицирующим веществом.

В результате такого коммуникационного воздействия в городе началась паника, возникли трудности у операторов сотовой связи, люди стали бояться выходить вечером на улицу. Некоторые саратовцы даже обратились через Интернет к президенту Д. Медведеву с тем, что местные власти якобы скрывают масштаб эпидемии. Из Саратова паника быстро стала распространяться на соседние города области — Энгельс, Балаково и т. д. Возникла реальная угроза паники и в соседних областях, куда также стала доходить ложная информация. Образно выражаясь, «ударная волна» стала распространяться дальше от «эпицентра взрыва», поражая общественное мнение, и авторитет местной власти.

Доказательств того, что за этим стояли какие-то экстремистские силы выявлено не было, никто на себя ответственность за эти информационно-психологические атаки не взял. Но это не означает, что данные технологии не будут использоваться террористическими силами в будущем. На наш взгляд, вероятность повторения подобных ситуаций с использованием Интернета довольно высока, так как по-прежнему отсутствуют законодательные механизмы, регулирующие отношения в виртуальной среде. Кроме того, нельзя недооценивать существующие риски, связанные с пропагандой экстремистских идей и вербовкой сторонников через Интернет, с использованием популярных коммуникационных форм. В ближайшие годы, по мере информатизации российского общества, увеличения численности российской интернет-аудитории, можно прогнозировать рост количества экстремистских интернет-ресурсов и активности экстремистских элементов в социальных сетях.

Библиографический список

1. *Адамьянц Т. З.* Проблема диалога в общении с экраном: миллион картинок экрана — одна «картина мира» телезрителя // Мир психологии. 2000. № 2.
2. *Вейман Г.* Как современные террористы используют Интернет. Специальный доклад № 116. URL: http://www.crime.vl.ru/index. php? p=949&more=1&c=1&tb=1&pb=1.
3. *Газизов Р. Р.* Информационный терроризм // Проблемы противодействия преступности в современных условиях: материалы Междунар. науч.-практ. конф. Уфа: РИО БашГУ, 2003. Часть 1. URL: http://kalinovsky-k.narod.ru/b/ufa20034/30.htm.
4. Измерение информационного общества. ITU, 2010. URL: http://www.itu.int/ITU-D/ict/publications/idi/2010/index. html.
5. Интернет в России. URL: http://bd.fom.ru/report/map/bntergum07/intergum0703/pressr_130611.
6. Киберпреступность в России увеличивается. URL: http://www.eurosmi.ru/kiberprestupnost_v_rossii_uvelichivaetsya.html.
7. *Льюис Джеймс А.* Оценка риска кибертерроризма, кибервойны и других киберугроз // Терроризм в России и проблемы системного реагирования/под ред. А. И. Долговой. М.: Российская криминологическая ассоциация, 2004. URL: http://www.crimas.ru/5_izdani/books/2004_isbn_6/index. php? file=3.
8. *Морозов И. Л.* Информационная безопасность политической системы // Полис. 2002. № 5.
9. *Петухов В. Б.* Интернет как фактор информационного воздействия терроризма на социум-XXI // Свободная мысль. 2008. № 1.
10. *Рыбакова Е. Е.* Кибертерроризм как одна из разновидностей киберпреступности: понятие и виды // Терроризм в России и проблемы системного реагирования/под ред. А. И. Долговой. М.: Российская криминологическая ассоциация, 2004. URL: http://www.crimas.ru/5_izdani/books/2004_isbn_6/index. php? file=3.
11. Такой внезапный мирный атом. URL: http://www.saratoff.ru/articles/incidents/0/501.
12. *Тропина Т. Л.* Терроризм с помощью Интернета // Терроризм в России и проблемы системного реагирования/под ред. А. И. Долговой. М.: Российская криминологическая ассоциация, 2004. URL: http://www.crimas.ru/5_izdani/books/2004_isbn_6/index. php? file=3.
13. Федеральный список экстремистских материалов. URL: http://www.minjust.ru/ru/activity/nko/fedspisok.
14. Digital economy rankings 2010. Beyond e-readiness. URL: http://www.edemocracy-forum.com/2010/07/digital-economy-rankings-2010-beyond-ereadiness. html.