11. См.: «Демократический олигархизм», этатизм и гражданское общество в современном в современной России // Проблемы соответствия партийной системы интересам гражданского общества современной России. Вып. 2 / Отв. ред. В.Г. Игнатова. – Ростов/нД: Изд-во СКАГС, 2004. – С.81-83.

12. См.: Савченко И.А., Шпак, В.Ю., Юрченко В.М. Технология политического действия. Краснодар, КГУ, 2007.

13. См.: Мясников А.П. Роль выборов в формировании партийной системы // Проблемы соответствия партийной системы интересам гражданского обществаа современной России. Вып. 2 / Отв. ред. В.Г. Игнатова. Ростов/нД: Изд-во СКАГС, 2004.- С. 127-129.

УДК 32

Акопов Г.Л., к.полит.н., доц.

Феномен информационных войн в сети «Интернет» и его воздействие на современную политику

Рассматриваются вопросы становления и распространения информационных войн, а также их последствия. Обозначены основные цели и задачи ведения кибервойн. На практических примерах проиллюстрированы угрозы кибертерроризма.

Ключевые слова и словосочетания: *информационная война, кибервойна, кибертеррор, информационные угрозы, виртуальное пространство.*

С древнейших времен информация являлась важнейшей составляющей любых политически значимых действий. На протяжении веков общественно-политические элиты плели интриги, проводили заговоры и умело манипулировали мнением окружающих. Что же касается непосредственно войн, то чем более развитым становилось общество, тем более изощренными становились методы получения и распространения разнообразной политической информации и дезинформации, а также политической пропаганды. На современном этапе можно с уверенностью говорить об информационных баталиях, глобальных информационных противоборствах и локальных конфликтах, которые уже давно не ограничиваются только вбрасыванием дезинформации.

Говоря о политике в условиях тотальной информатизации, обойти вниманием такое явление, как информационные войны просто не представляется возможным. Для военного истеблишмента становится очевидным, что современное общество зависимо от информационных систем, а наиболее современный способ воздействия на противника – виртуальное воздействие на его граждан (манипуляция общественным сознанием). Эта стратегия весьма эффективна для нанесения вреда противнику. Чем более развитым становится общество, тем более значимым фактором в этом обществе является информация. Ин-

формационное противоборство присутствовало во всех войнах и проявлялось в различных формах, будь то ведение разведки, распространение дезинформации, либо проведение агитационных акций, захват средств получения и передачи информации и т.д. С появлением и развитием ядерного оружия перспектива реальных военных действий грозит трагедией для обоих участников конфликта, именно поэтому для достижения своих целей выгоднее использовать информационное оружие, нежели традиционное вооружение.

Первоначально термин «информационная война» использовал Т. Рона в отчете, подготовленном им в 1976 г. для компании Boeing и названном «Системы оружия и информационная война». Т. Рона указал, что информационная инфраструктура становится ключевым компонентом американской экономики. В то же самое время она становится и уязвимой целью как в военное, так и в мирное время. Этот отчет и можно считать первым упоминанием термина «информационная война» [1].

Публикация отчета Т. Рона послужила началом активной кампании в средствах массовой информации. Сама постановка проблемы весьма заинтересовала американских военных, которым свойственно заниматься секретными материалами. Военные аналитики США начали активно исследовать данное направление. Пик изучения данной проблематики пришелся на период распада СССР. Если вспомнить развал Советского Союза, то, без сомнения, можно сказать, что он стал отчасти результатом информационной открытости и беззащитности, которая пришла в страну вместе с перестройкой.

После окончания холодной войны термин «информационная война» был введен в документы Министерства обороны США. Он стало активно упоминаться в прессе после проведения операции «Буря в пустыне» в 1991 г., где новые информационные технологии впервые были использованы как средство ведения боевых действий. Официально же этот термин впервые был введен в директиве министра обороны США DODD 3600 от 21 декабря 1992 г.

Американские теоретики под информационной войной понимают форму агрессивной борьбы сторон, представляющую собой использование специальных методов, способов и средств для воздействия на информационную среду противостоящей стороны и защиты собственной.

В трактовке отечественных ученых информационная война – это действия, предпринятые для достижения информационного превосходства путем нанесения ущерба информации, процессам, основанным на информации и информационным системам противника при од-

новременной защите собственной информации, процессов, основанных на информации, и информационных систем.

Мы, в свою очередь, обозначим информационную войну как активное воздействие на информационную среду противника для достижения поставленных целей и обеспечение защиты собственного информационного пространства. Большинство исследователей рассматривают информационные войны и противоборства глобально, абстрагируясь от сетевой составляющей данного процесса. Наибольший интерес для нас представляет лишь отдельная площадка ведения информационных войн, которая, по нашему мнению, заслуживает особого внимания. Речь идет о всевозрастающем информационном противоборстве с использованием компьютерных сетей общего пользования. Еще в конце 1996 г. Роберт Банкер, эксперт Пентагона, на одном из симпозиумов представил доклад, посвященный новой военной доктрине вооруженных сил США XXI столетия (концепции «Force XXI»). В ее основу было положено разделение всего театра военных действий на две составляющих традиционное пространство и киберпространство, причем последнее имеет даже более важное значение. Особенно с учетом перспективы распространения ИКТ. Очевидно, что уже сегодня мировое сообщество стоит на пороге новой эпохи информационных противоборств, эпохи кибервойн. Кибервойна – это информационное противоборство с использованием информационно-коммуникационных компьютерных сетей общего пользования.

Цели и задачи ведения кибервойн:

- размещение в сети «Интернет» заведомо ложной или провокационной информации для ее последующего распространения в средствах массовой информации и сетевом сообществе;
- манипулирование общественным сознанием, навязывание необходимой идеологии (влияние на общественное мнение);
- вербовка сторонников и рекрутирование единомышленников;
- несанкционированный доступ к информационным ресурсам с последующим их искажением или хищением;
- подрыв международного авторитета государства;
- влияние на принятие политически значимых решений;
- создание атмосферы бездуховности и безнравственности, негативного отношения к культурному наследию;
- дестабилизация политических отношений в обществе;
- распространение компромата и иных сведений, порочащих честь и достоинство политической элиты страны;
- создание атмосферы напряженности между партиями, общественными объединениями и движениями;

- политический либо иной шантаж;

- разжигание межнациональной розни и расовой нетерпимости;

- воздействие на экономическую инфраструктуру государственного образования;

- инициирование массовых беспорядков и иных протестных акций.

В последние пять-семь лет граждане, работающие в сети «Интернет», со всеми вопросами в первую очередь обращаются к поисковым системам. Для любого политика, не говоря уже о политических институтах и тем более государственных образованиях, имидж в просторах глобальной паутины является одной из самых важнейших составляющих успеха, да и просто нормального функционирования. Вот почему многие политики и политические организации активно ведут борьбу за виртуальное превосходство, и все чаще эта борьба напоминает ноне информационной войны в виртуальном пространстве. В борьбу за создание положительного имиджа уже давно вступили многие цивилизованные страны. И побеждает в этой нелегкой борьбе тот, кто сумел закрепить за собой сайты в первой десятке поисковых систем. А это значит, что любой пользователь, который хочет открыть для себя страну, получит о ней подконтрольную информацию, что создаст необходимый имидж государственного образования.

Не случайно на открытии международной конференции «Информационные войны в современном мире» в августе 2008 г. Председатель Совета Федерации С. Миронов сказал: «Давно замечено, что крупные научные открытия и технические достижения быстрее всего находят применение в военной сфере. Так, увы, случилось и с результатами грандиозного прорва в информационных технологиях, который произошел за последние десятилетия». По его словам, «целью любой информационной войны является управляемое изменение сознания людей, их отношения к своему обществу, к государству, к самим себе. В результате люди могут потерять, сами того не осознавая, собственную волю, а государства – суверенитет. – Все это всегда и было целью любой войны. Но теперь этого можно добиваться более «мягкими», но оттого не менее опасными средствами, поскольку эти средства могут настичь буквально каждого. Чем не оружие массового поражения?», – подчеркнул С. Миронов [2].

Российские правоохранительные органы пытаются всеми доступными мерами бороться с экстремизмом в сети «Интернет», но пока не совсем успешно. Согласно сообщению ИТАР-ТАСС, 5 апреля 2009 г. в интернете появилась статья, призывающая участников неформальных молодежных объединений экстремистского толка к совершению неправомерных действий в отношении сотрудников правоохранитель-

ных органов и государственных учреждений. Прокуратурой было возбуждено уголовное дело по трем статьям УК РФ: по ч.1 ст. 280 (публичные призывы к осуществлению экстремистской деятельности), ч.1 ст. 205.2 (публичные призывы к осуществлению террористической деятельности) и ч. 1 ст. 282 (действия, направленные на возбуждение ненависти либо вражды, а также на уничижение достоинства человека либо группы лиц по признакам пола, расы, национальности, языка, а равно принадлежности к какой-либо социальной группе, совершенные публично). Российскую прокуратуру крайне беспокоит распространение экстремизма через интернет. Об этом рассказал заместитель генпрокурора В. Гринь на парламентских слушаниях.

По его словам, сегодня интернет-ресурсы активно используются для пропаганды экстремизма и насилия, что подтверждается практикой прокурорского надзора. Уголовные дела по терактам в различных российских городах говорят о том, что экстремисты пользовались сведениями, которые в Сети в открытом доступе. Эксперты сообщают, что в настоящее время в стране насчитывается более 500 интернет-сайтов, провоцирующих разжигание национальной вражды [3].

Генпрокуратура предложила депутатам законодательно определить такие понятия, как – «интернет-сайт» и «распространитель информации». Среди других предложений – ужесточить статьи Уголовного кодекса, которые касаются возбуждения ненависти либо вражды, унижения достоинства человека или группы лиц по признакам пола, расы, национальности, языка, происхождения, отношения к религии, а также за организацию экстремистского сообщества и организацию деятельности экстремистской организации.

Возможно, вскоре появится единый межведомственный банк данных по вопросам противодействия экстремизму. К тому же заместитель генпрокурора заявил о необходимости создания ведомства по межнациональным отношениям. В. Гринь отметил, что работа федеральных и местных органов власти в этой сфере по-прежнему неэффективна, а профилактические меры носят скорее «формальный, декларативный характер» [3].

Другой не менее интересный случай информационной атаки произошел в мае 2008 г. Когда люди стали получать пугающие «смс-сообщения», о том что якобы на Ленинградской атомной станции произошла авария. Новость обсуждали в интернете, в считанные часы слухи накрыли Санкт-Петербург и всю область. Едва не началась паника. Люди скупали в аптеках йод, чтобы обезопасить себя от радиоактивного заражения. Оперативникам удалось найти самое первое сообщение в сети – из целой серии подобных. Но источник информацион-

ной атаки остался неизвестен, прокуратура сделала вывод о том, что это была заранее спланированная акция.

Многие сайты, вызывающие на взгляд ряда пользователей информационные угрозы, пытаются взламывать политически активные хакеры либо организации хакеров. данное явление получило название «Хактивизм» [4]. Исходя из мировой практики, создается впечатление, что действия программистов, возможно, единственный адекватный ответ на акции сетевых провокаторов. Законодательные меры оказываются не вполне эффективными. В сентябре 2003 г., суд г. Вильнюса признал незаконными действия литовского департамента госбезопасности, который в июне 2003 г. закрыл сайт «Кавказ-Центр». Тогда создателей интернет-ресурса обвинили в пропаганде терроризма, национальной и религиозной розни. Были проведены обыски в офисе фирмы, которая размещала электронную страницу на своем сервере. Закрыть «Кавказ-Центр» требовали от Литвы и российские власти. Однако уже в конце сентября 2003 г. суд Вильнюса вынес решение в пользу создателей сайта. 13 сентября 2004 г. после ряда террористических актов Министерство иностранных дел России вновь потребовало прекращения работы сайта «КавказЦентр». Для этого в МИД был вызван посол Литвы в России Р. Шидлаускас. Как говорилось в сообщении ведомства, вопрос был поставлен перед ним «в жесткой форме». «Бездеятельность перед лицом продолжения существования сайта на литовском сервере будет рассматриваться в Москве как откровенно недружественный шаг литовских властей, негативно влияющий на атмосферу наших двусторонних отношений», – говорилось в заявлении [5].

Озабоченность российских властей была вполне обоснованной. Специализированные сайты террористов наносят ощутимый информационный урон государственной политике. На подобных сайтах боевики пишут о готовящихся терактах, выдвигают различные условия, запугивая общественность и шантажируя власти. Все чаще мы слышим из СМИ заявления о том, что боевики какой-либо организации взяли на себя ответственность за то или иное действие, далее следует фраза: «Об этом говорится на интернет-сайте боевиков».

Как известно, 24 августа 2004 г. самолеты Ту-154 и Ту-134, вылетевшие из Домодедово потерпели катастрофу. На протяжении двух дней российские власти отказывались верить в то, что падение самолетов – дело рук террористов. Высказывались разные аргументы и о том, что катастрофы произошли в разных местах и что авиакомпании разные, и тот факт, что самолеты вылетели из одного аэропорта и практически в одно время, ни о чем не говорит. Но ситуация прояснилась после того, как на некоем интернет сайте организация являющаяся ячей-

кой «Аль-Каиды», взяла на себя ответственность за взрывы российских самолетов. После того, как эту новость процитировали информационные агентства, официальные лица все чаще стали говорить о том, что произошел террористический акт.

Все чаще террористы берут на себя ответственность через интернет-сайты или, что еще хуже, вывешивают на своих сайтах фотографии жертв взрывов и даже видеоролики отснятых терактов. Нередко посредством своих сайтов боевики отчитываются о проделанной работе или обращаются с посланиями к определенной категории граждан. Порой через свои сетевые ресурсы террористы запугивают общественность, угрожая новыми террористическими атаками.

Наибольший эффект эти заявления вызывают благодаря массовому цитированию новых сообщений от террористов всевозможными средствами массовой информации и информационными лентами новостей в сети «Интернет». К тому же подобные сообщения практически моментально находят отклики в он-лайн дневниках (блогах) и обсуждениях в социальных сетях.

Наиболее интересным представляется зарубежный опыт ведения информационных войн в эпоху информационного общества, так как многие западные страны значительно опережают Россию в своем информационном развитии. Например, Израильское министерство абсорбции начало набор армии блогеров, владеющих, кроме иврита, другими языками. Они должны будут представлять точку зрения Израиля в антисемитских блогах и форумах. После регистрации добровольцев отправят в медиа-отдел министерства иностранных дел, а тот уже выпишет им адреса сайтов, признанных проблемными.

Транснациональная корпорация террора, действующая под маркой «Ал. Каиды», по достоинству оценила демократизм никем не контролируемой Сети. И активно использует ее как для пропаганды своих взглядов, так и для подготовки грядущих битв. Сеть изобилует информационными ресурсами, на которых можно ознакомиться с 1000-страничной энциклопедией джихада (войны против неверных), специализированные сайты обучают боевиков не только тому, как правильно изготовить и заложить взрывчатку, но и как эффективно организовывать различные террористические акты, в том числе и хакерские взломы.

По данным исследования, проведенного институтом United-StatesInstituteforPeace (USIP), террористы адресуют свои сайты трем типам аудитории: активным членам террористических формирований и их сторонникам, международной общественности – для формирования соответствующего мнения и противникам – с целью их деморализации.

Исследователями написаны тома на тему, как важен для любой террористической группировки доступ к СМИ. Ведь любой теракт – это некая PR-акция, призванная привлечь внимание как можно более массовой аудитории. Западные СМИ в силу и законодательных ограничений, и вполне уместной самоцензуры информацию подобного рода стараются отфильтровывать. Но, как продемонстрировало исследование одной из американских неправительственных организаций, 28 % американцев, подключенных к Сети, активно интересуются неотфильтрованной информацией и теми самыми зловещими картинами и казней, которых вы не найдете в традиционных СМИ. Таким образом, террористы с помощью Сети решают одну из своих главных задач – довести до конечного потребителя свое неотфильтрованное послание. И именно этим, как полагают эксперты, вызван бурный рост числа радикальных сайтов.

В настоящее время во Всемирной сети существует уже несколько сотен экстремистски настроенных информационных ресурсов. Если в 1998 г. примерно половина из 30 организаций, которых США причисляли к террористическим, обладали своими электронными страницами, то ныне в Сети представлены абсолютно все известные своими радикальными взглядами группы. Причем материалы они переводят не менее чем на 40 различных языков.

Связь через Всемирную компьютерную сеть идеально подходит для террористов. но некоторым данным, подготовка к терактам 11 сентября велась именно с помощью обмена зашифрованными посланиями по электронной почте. Используется и стеганография – кодирование посланий в графической информации. «Аль-Каида» поддерживает сейчас в Сети около 50 различных сайтов. «Интернет – это часть сегодняшнего поля битвы, – утверждает Брайан Дженкинс, специалист по антитеррору в мозговом центре «Рэнд корпорейшн» [6].

Администрации многих стран в меру сил пытаются бороться с проявлением кибертеррора. В конце 2003 г. США впервые внесли в свой список иностранных террористических организаций несколько интернет-сайтов. Список, опубликованный Госдепартаментом США в Федеральном регистре, включает сайты newkch.org, kahane.org, kahane.net, kahanetzadak.com в качестве другого названия еврейской организации «Кахане Хай» или «Ках», которая подозревается в организации нападений на палестинцев. Согласно американскому законодательству, эти сайты теперь вне закона и запрещена их любая материальная поддержка, их сотрудникам запрещен въезд на территорию США, а американские банки должны заморозить их счета. Однако, как

сообщило агентство Reuters, даже сам Госдепартамент пока не понимает, каким образом это будет сделано.

Новую волну возмущений практически по всему миру вызвали публикации сайта «Викиликс», неожиданно опубликовавший тысячи секретных документов американской армии об перациях США в Афганистане и Ираке. Копии секретных телеграмм госдепартамента США были переданы трем мировым средствам массовой информации – американской газете «Нью-Йорк таймс», британской газете «Гардиан» и германскому журналу «Шпигель». Основатель скандального сайта Джулиан Ассанж за несколько недель до того предупредил, что новая утечка во много раз превзойдет по своим объемам предыдущие публикации о войне в Ираке, которые в общей сложности насчитывали порядка 400 тыс. документов. США предупредили союзников о предстоящей публикации материалов их секретной дипломатической переписки сайтом «Викиликс». По данным источников британского телеканала «Скай-ньюс», речь идет о нескольких миллионах электронных писем из числа переписки госдепартамента США и различными посольствами по всему миру, в которых содержатся «откровенные замечания о мировых лидерах, послах, иностранных руководителях». Публикуемые документы, в частности, касаются Афганистана, Пакистана и России. «Это ставит американцев в неудобное положение», – отметил «Скай-ньюс». Как сообщила ранее электронная версия журнала «Вайрд» /Wired/, «утечка» телеграмм дипломатов США произошла по линии Пентагона [7]. Естественно подобная информация вызвала повышенный интерес не только пользователей сети «Интернет», СМИ, но и высокопоставленных чиновников вплоть до руководителей государств.

«Мы не параноики и мы не связываем, скажем, российско-американские отношения с какими-либо утечками, хотя эти утечки показательны: они показывают всю меру цинизма те оценок и зачастую тех суждений, которые превалируют во внешней политике различных государств, в данном случае я имею в виду США», – сказал Д.А, Медведев на совместной пресс-конференции по итогам российско-итальянских межгосконсультаций в пятницу. Вместе с тем Д.А. Медведев отметил, что представители США «имеют право на эти суждения». «Другое дело, когда эти суждения становятся публичными, они действительно способны нанести ущерб внешнеполитическим связям», – сказал Президент РФ [8].

Ситуацию со скандальным сайтом не обошел вниманием и российский премьер-министр В.В. Путин в своем интервью легендарному американскому тележурналисту Ларри Кингу на телеканале CNN В.В. Путин заметил: «Некоторые эксперты считают, что Wikileaks кто-то

специально «надувает». «Надувает» авторитет этого сайта, чтобы потом использовать его в каких-то своих политических целях. Это один из возможных вариантов, и таково мнение экспертов, которое и у нас тоже распространяется. Я думаю, что если это не так, то это говорит о том, что дипломатической службе нужно внимательнее следить за своими документами. Такие утечки бывали и раньше, и в прежние времена. Никакой катастрофы я в этом не вижу» [9].

Своими публикациями «Викиликс» не только рассекретил сотни тысяч документов, но и нанес один удар по репутации США, как государства, которому по зубам любая проблема. Все попытки закрыть скандально известный сайт не увенчались успехом, а во Всемирной паутине появилось более двух сотен зеркальных копий «Викиликс». В результате скандала в США вернутся те дипломаты, чьи фамилии и должности были названы на сайте «Викиликс». В текстах опубликованных телеграмм содержались весьма некорректные или критические высказывания как в адрес мировых лидеров, так и по отношению к проводимой ими политике. В итоге одними телефонными разговорами госсекретаря США Хиллари Клинтон со многими лидерами государств и министрами иностранных дел Вашингтону ограничиться не получилось. Американским властям все же придется перевести скомпрометированных дипломатов на новые должности, так как на старых местах им оставаться невозможно: их, по мнению большинства экспертов, просто «выжмут» из политики, и наладить диалог с местными властями они уже не смогут.

«Вот другая сторона этой трагедии... нам придется отозвать лучших из наших дипломатов... потому что они осмелились рассказать нам правду о том, что происходит в странах, где они работают», – заявил источник в администрации Обамы, пожелавший остаться неназванным. По его словам, несмотря на то, что мировые лидеры в большинстве своем скептически отнеслись к публикациям «Викиликс» и заверили США, что они никак не осложнят отношений с Вашингтоном, к «прокомпрометировавшимся» дипломатам все равно будут относиться как к персонам нон грата. Но кто заменит «лучших дипломатов»? И сможет ли теперь госдеп справляться с возложенными на него задачами?

Между тем британский адвокат Джулиана Ассанжа сообщил о еще одном подготовленном козыре его клиента. Он заявил, что у основателя «Викиликс» припасены материалы, которые могут быть обнародованы в случае, если что-то случится с ним или его сайтом. Адвокат Марк Стивенс назвал это «термоядерным устройством» эры интернета. Напомним, что 3 декабря Ассанж, отвечая на вопросы читателей на сайте британской газеты «Гардиан», сообщил, что ему и его колле-

гам в последнее время не раз угрожали: «Угрозы смерти в наш адрес – это не секрет, но мы приняли адекватные меры в тех рамках, которые мы можем противопоставить супердержаве» [10].

Как мы уже неоднократно писали [11], свободное распространение информации в Интернете не на шутку беспокоит спецслужбы всего мира, осознавшие свою слабость перед лавинообразно увеличивающимся потоком информации и, что не менее важно, дезинформации. Информационные атаки распространяемые через глобальные информационно-коммуникационные сети способны нанести ощутимый ущерб практически любому государственному образованию вплоть до свержения власти и организации революционных движений. Нечто подобное произошло в Тунисе. Как утверждают эксперты, тунисские события стали первой в истории революцией, которой способствовали откровения сайта Wikileaks.

«Хотя коррумпированное правление президента бен Али уже давно вызывало недовольство в стране, протесты стали набирать силу, когда Wikileaks опубликовал переписку посольства США», – указывает британская газета Daily Mail. – В недавно обнародованной депеше, датируемой июнем 2009 г., президента [Туниса] и его родных называют словом «семья», связывая их таким образом с мафиозной элитой, управляющей тунисской экономикой. В этой переписке говорится также, что жена президента Лейла бен Али сделала огромные деньги на строительстве эксклюзивной школы». Веб-сайт Джулиана Ассанджа с ситуацией в Тунисе связывает и другая выходящая в Лондоне газета, «Guardian». «Публикации добытых Wikileaks приватных разговоров американцев о коррупции и непотизме ненавистного «склеротичного» режима, предположительно, способствовали появлению тунисского протестного движения», – указывает автор [12].

Издание «Foreign Policy» также усматривает за событиями в Тунисе влияние разоблачений «Wikileaks» и прогнозирует развитие этой тенденции. Как отмечается в статье, депеши американских дипломатов осветили детали чудовищной коррупции в стране. В опубликованных посланиях говорится о том, что власть в стране принадлежит узкому кругу элиты, которая уже превратилась в мафиозный клан [13].

В целом, это не стало абсолютным откровением для жителей Туниса, однако их предположения стали подкрепляться фактами. В частности, у населения не мог не вызвать негодования тот факт, что зять президента заказывает себе на ужин десерты, которые ему привозят на самолете из Сан-Тропе. После того, как власти закрыли доступ к порталу Wikileaks в интернете, информация все равно просачивалась через блоги и социальные сети (преимущественно «Twitter» и «Facebook»).

Кроме того, молодые демонстранты закачивали видео с акций на «You Tube» с помощью различных ухищрений, несмотря на то, что видеохостинг был запрещен властями этой страны еще в 2007 г. Притеснения свободы слова в Сети отражались и в слоганах, звучавших на улицах, пишет CNN. В целом, материалы Wikileaks послужили катализатором последних событий, которые стали апогеем недовольства народа политикой властей и их отношением к своим гражданам [13].

К сожалению, перед подобными угрозами Российская Федерация уязвима ничуть не меньше зарубежных коллег.

Единственный метод, которым можно, с точки зрения официальных лиц, остановить появление информационных террористов – это цензура. Нечто подобное после 11 сентября 2001 г. практиковали США. Тогда из общего доступа были удалены многие ресурсы, представляющие хоть какую-то ценность для потенциальных террористов. Цензура введена и на территории Китая, где, помимо всего прочего, ограничен доступ к зарубежным СМИ и интернет-ресурсам. Несомненно, введение подобных правил помогает спецслужбам, которые начинают хотя бы отчасти контролировать информационные потоки. Но возникает вполне резонное возражение: как, же быть с правами человека на свободу слова и информации, предусмотренными конституциями многих стран? Достаточно создать прецедент, и соответствующие органы вряд ли упустят шанс взять под контроль Интернет, в том числе интернет-СМИ. Возможно, что с течением времени образуются предсказываемые М. Кастельсом «On-line полицейские патрули» [14].

Первые прототипы подобных организаций появились в августе 2004 г. во Вьетнаме. Там было сформировано специальное полицейское подразделение, в задачи которого входит расследование онлайн-преступлений и слежка за распространением запрещенных публикаций в киберпространстве [15]. Структуры, следящие за содержанием сети «Интернет», безусловно, востребованы уже сегодня. Как мы писали ранее, в сети масса явно вредных и провокационных сайтов. С их помощью экстремисты распространяют свои идеи и вербуют сторонников. С помощью специализированных сайтов можно овладеть многими опасными навыками (например, научиться взламывать сетевые ресурсы). В сети можно встретить и сайты, содержащие или даже продающие различные тайны, в том числе и государственные. Нельзя не отметить, что в сети открыто пропагандируются, а порой и продаются запрещенные товары, например, наркотики или оружие. А специализированные сайты учат, как это все грамотно использовать.

Огромные возможности для пропаганды своих идей благодаря сети общего пользования получают различного рода экстремистские

группы и течения, которым обычно закрыт доступ в традиционные СМИ. Имеет свой сайт, например, движение «Русское национальное единство» (www.rne.org). Сайт РНЕ настолько обширен и информативен, что по количеству публикаций, пожалуй, «заткнет за пояс» многие сайты информационных агентств, не говоря уже о сайтах политических партий. И это не удивительно. Для радикальных и экстремистски настроенных организаций сеть «Интернет» – чуть ли не единственная возможность донести свою информацию до масс. Не будем комментировать данную информацию, процитируем лишь некоторые заголовки статей этого сайта: «Президент Путин и еврейский экстремизм»; «Что не демократ, то уголовник»; «Принципы русского национализма» и т.д.

Подобных ресурсов в сети «Интернет» отнюдь не единицы, например разнообразные интернет-страницы скинхедов или сайты крайне националистического толка, а порой и просто экстремистские интернет-порталы. Самое печальное, что обозначенные интернет-ресурсы пользуются большой популярностью у посетителей всемирной паутины.

Все чаще на подобные проблемы обращают внимание и официальные лица. Например, 16-17 июля 2004 г. в Париже прошла специальная встреча ОБСЕ, посвященная вопросу взаимосвязи пропаганды расизма, ксенофобии и антисемитизма с преступлениями на почве ненависти. С докладом по проблемам распространения сетевых технологий выступил представитель российской делегации, доктор юридических наук, профессор В. Остроухов. В его докладе, отмечалось, что сегодня «в интернете функционирует большое количество информационных ресурсов (сайтов), способствующих развитию ксенофобии и экстремизма». По мнению докладчика, их можно условно разделить на четыре группы:

- сайты, непосредственно распространяющие идеи экстремизма, сепаратизма и терроризма;
- сайты нетрадиционных религиозных учений и сект;
- сайты, разжигающие ксенофобию на основе расовой или национальной принадлежности;
- интернет-ресурсы справочного характера, напрямую не призывающие к противоправной деятельности.

По мнению В. Остроухова, особую опасность представляют сайты последней, четвертой группы, так как на них «можно найти информацию о том, как в кустарных условиях изготовить взрывчатые вещества, получить сильнодействующие ядовитые вещества, собрать самодельное взрывное устройство.

Характеризуя третью группу сайтов, Остроухов перечислил те секты, знакомство с учением которых по интернету является потенци-

ально опасным для россиян. В список попали, в частности, религиозные организации «Свидетели Иеговы» и «Харе Кришна» [16].

Для противодействия владельцам и создателям упомянутых сайтов докладчик посчитал целесообразным:

- повысить уровень взаимодействия в сфере контроля и пресечения пропаганды терроризма и ксенофобии в интернете;

- проводить целенаправленную работу по унификации и совершенствованию национальных законодательств, регулирующих распространение информации в телекоммуникационных сетях общего пользования;

-выработать систему признаков интернет-ресурсов, пропагандирующих ксенофобию, расовую и религиозную нетерпимость, и на её основе создать единый перечень подобных интернет-ресурсов, в целях координации действий по их нейтрализации;

- проводить совместные мероприятия по идентификации, привлечению к ответственности реальных владельцев наиболее одиозных интернет-ресурсов [16].

К слову сказать, прецедент в России уже создан. В марте 2005 г. Ленинский суд г. Кемерово вынес обвинительный приговор студенту юридического факультета, публиковавшему в сети материалы экстремистского содержания. Как сообщил пресс-секретарь управления судебного департамента при Верховном Суде России в Кемеровской области Г. Мулинов, уголовное дело в отношении студента юридического факультета было возбуждено около трех лет назад по ст. 280 и 282 УК на основании публикаций, размещенных в Сети на сайте нелегальной организации. «Материалы, опубликованные под псевдонимом Хорд, привлекли внимание УФСБ и правоохранительных органов области. В них усматривались призывы к свержению конституционного строя и разжиганию национальной розни [17]», – отметил он.

Однако единичными, пусть даже показательными, судами проблемы не решить. Тем более что банальными публикациями в сети материалов современные экстремисты не ограничиваются. Наибольшую активность в использовании преимуществ сетевого общения проявляют неправительственные организации для осуществления гражданских инициатив, в том числе и актов общественного неповиновения. Достаточно, например, назвать ставшие уже обычным явлением во всем мире выступления антиглобалистов, организуемые посредством использования сетевого моделирования протестных акций [18]. Сеть позволяет антиглобалистам не только рекрутировать новых членов и поддерживать связь со своими отделениями по всему миру, но и управлять акциями общественного неповиновения. В частности, через сеть «Ин-

тернет» происходило координирование многих протестных акций, проведенных антиглобалистами.

Постепенно технологии, апробированные на Западе, пришли в Россию. И все чаще можно слышать, что протестные акции, митинги и антиправительственные выступления были спланированы и организованы через сеть «Интернет».

Террористы все чаще вербуют в свои ряды граждан США, поэтому необходимо ужесточить контроль над американским сегментом интернета, считает глава министерства национальной безопасности США Джанет Наполитано. В Сенат внесен законопроект, который позволит президенту перекрывать доступ в сеть в случае чрезвычайной ситуации. При министерстве безопасности предлагается создать специальный центр – он будет контролировать коммуникации. А в случае необходимости он станет управлять всеми компаниями США, деятельность которых так или иначе связана с интернет-технологиями, – от провайдеров до производителей программного обеспечения.

Представители компьютерных фирм уже обеспокоились возможным нарушением гражданских свобод в случае принятия законопроекта. По их мнению, неограниченная власть государства в интернет-пространстве приведет к непредсказуемым последствиям [19].

Отсюда вытекает логический вывод политико-правового характера о неотложной потребности существенного дополнения концепции информационной безопасности России новеллами, посвященными системе контроля за коммуникативной властью со стороны государства и институтов гражданского общества.

Проблема регулирования деятельности в сети «Интернет» назрела уже давно во всем мире. Осознавая это, еще в середине 2003 г. 45 государств – членов Совета Европы – приняли «совместную декларацию, где изложены принципы, на которых должно строиться общение в интернете. Страны-члены Совета Евро высказывают обеспокоенность попытками ограничить доступ населения к общению через интернет по причинам политического характера или по каким-либо другим причинам, несовместимым с принципами демократии» [20].

В декларации еще раз подчеркивается необходимость свободы слова и свободного распространения информации в интернете. Что примечательно, в основу декларации положен принцип применения к электронным средствам массовой информации тех же ограничений, что и к другим способам распространения информации. В связи с этим Совет Европы выступает против предварительной цензуры информации в любом виде, что, однако, не исключает возможности отбора информации, разрешенной несовершеннолетним.

Декларация напоминает о праве пользователей итернета на анонимность, что не исключает возможности разыскать тех, кто должен ответить перед законом за совершение противоправных действий. В то же время уменьшается степень ответственности провайдеров и владельцев сайтов, предоставляющих места для размещения информации.

Это положение было включено в декларацию по настоянию исправительного суда Парижа после того, как 11 февраля бывший президент американского портала Yahoo был отдан под суд за преступления против человечества в связи с тем, что на Yahoo продавались с аукциона предметы, ранее принадлежавшие нацистам [20].

Проблемы информационной безопасности обозначил в своем выступлении на экономическом форуме в Давосе 26 января 2011 г. Президент России Д.А. Медведев: «Сегодня действия политиков, международные отношения и принципы регулирования все меньше успевают за прогрессом. В то же время часть людей, часть политиков продолжает жить фантомами «холодной войны», увлекается примитивными силовыми амбициями. Но именно в этот период значительная часть людей, уже почти миллиард человек – давайте вдумаемся в эту цифру, пользуется социальными сетями, впервые в истории человечества, тысячелетней истории, общается друг с другом непосредственно, находясь на самых разных континентах. Это поражает. Современный мир становится, как принято говорить, всё более плоским, стирает формальные границы и барьеры. Благодаря интернету создаются сообщества людей, находящихся в разных странах, но объединённых одним делом или одной идеей, и ни одно национальное правительство не может претендовать на полноту влияния на такие сообщества. Может быть, это и к лучшему. С похожими факторами столкнулся и бизнес. Но есть и опасная сторона этих процессов, порой они служат очень важным инструментом для экстремистов, которые разжигают этническую и религиозную ненависть, для торговцев наркотиками и оружием, для террористов. Эти проблемы тоже усиливаются, и не видеть этого нельзя. Одновременно всеобщая связанность должна стать мощнейшим драйвером экономического роста, а любые попытки разорвать эти связи, например, ограничение свободы интернета или распространения инноваций, я думаю, это сегодня понимают все, приведут мир к стагнации. Россия не будет поддерживать инициативы, которые ставят под сомнение свободу в интернете, разумеется, свободу, которая основана на требованиях морали и законодательства» [21].

К сожалению, на сегодняшний день мировое сообщество не смогло найти достойные меры противостояния информационным агрессиям, а это означает только одно – в период тотальной информатизации главным оружием будут выступать информационные технологии, которые уже сегодня способны нанести значительный урон политической системе общества, вплоть до свержения действующей власти и организации переворотов и революций в государственном образовании.

Литература

1. Rona Thomas P. Weapon Systems and Information War, Boeing Aerospace Co., Seattle, WA, 1976.

2. Информационные войны в современном мире. Международная конф. с участием С. Миронова начала свою работу. http://www. spravedlivo.ru/news /anevs/7250.php

3. Интернет признали рассадником терроризма. http://www.utro.ru /articles/2008/09/30//771439.shtml

4. Хактивизм – «бескорыстное» хакерство в целях политического активизма.

5. «Кавказ-центр» Литва пока не закроет. http://nevs.bbc.co.uk/hi/russian/russia/newsid 3656000/3656426.stm

6. Терроризм побеждает в Интернете. http://lenta.ru/articles /2004/09/16/webterror

7. *Лавров С.* Публикации сайта «Викиликс» – забавное чтиво. Опубликовано на сайте rg.ru. 29 ноября 2010 г.

8. Опубликовано на сайте «Российской газеты» 3 декабря 2010 г. http://www.rg.ru/2010/12/03/medvedev-anons.html

9. Владимир Путин ответил на вопросы Ларри Кинга // Российская газета. 03.12.2010. http://www.rg.ru/2010/12/03/king-putin html

10. «ВикиЛикс» в зазеркалье // Российская газета. Федеральный выпуск. 2010. № 5355 (276). 7 дек.

11. *Акопов Г.Л.* Глобальные проблемы и опасности сетевой политики. Ростов н/Д, 2004; *Он же.* Правовая информатика: современность и перспективы. Ростов н/Д, 2005; *Он же.* Internet – джин, выпущенный из бутылки // Научно-аналитический журнал «Обозреватель». 2004. № 12 (179). Декабрь; *Акопов Г.Л., Кислицын С.А.* Политология: Учеб. пособие Ростов н/Д: Феникс, 2009.

12. Революция в Тунисе вызвана откровениями Wikileaks? BBC Russia http://www.bbc.co.uk/ russian/international/2011/01/110115_ tunisia_wikileaks_ connekction shtml

13. «Долой президента и его олигархов»! Первая Wikileaks-революция – в Тунисе. Освобожден из заключения лидер запрещенной компартии. KPRF.RU 2011-01-14 23:55

14. *Кастельс М.* Информационная эпоха. Экономика. Общество и Культура / Пер. с англ. Под науч. ред. проф. О.И. Шкаратана. М., УВШЭ. 2000. С. 510.

15. Утро.ру – ежедневная е-газета. «Во Вьетнаме создана киберполиция». 5.08.2004.

16. Полный текст выступления российского участника специальной встречи ОБСЕ по вопросу взаимосвязи пропаганды расизма и ксенофобии с преступлениями на почве ненависти. http://vip.lenta.ru/dok/2004/06/16/osce/

17. Кемеровский студент осужден за публикации в сети. Газета. ру http://www.gaseta.ru/2005/03/17/last 151565.shtml

18. От Маркса до Маркоса и далее. Два источника и множество составных частей оппозиции глобальному капитализму // Эксперт. 2002. № 18 (325). 13 мая. С. 67-69.

19. Власти США хотят контролировать Интернет для борьбы с терроризмом http://www.vesti.ru/

20. Утро.ру – ежедневная е-газета. «Совет Европы выступает за свободу слова в Интернете». 30.05.2003 г.

21. Президент России выступил на церемонии открытия Всемирного экономического форума. 26.01.2011. http://kremlin.ru/nevs/0163