Е.С. ЗИНОВЬЕВА

ВЫЗОВЫ И РИСКИ ГЛОБАЛЬНОГО ИНФОРМАЦИОННОГО ОБЩЕСТВА*

Зиновьева Елена Сергеевна, *к. полит. н.,*
доцент кафедры мировых политических процессов МГИМО МИД России.
119454, Москва, просп. Вернадского, 76. E-mail: zinovjeva@mail.ru

Аннотация

Статья посвящена исследованию вызовов и рисков для международной безопасности, возникающих в связи с развитием глобального информационного общества. Охарактеризованы основные тенденции развития глобального информационного общества, а также подходы к его изучению и оценке влияния на современную мировую политику. В статье изучены основные вызовы, риски и угрозы, возникающие в связи с развитием глобального информационного общества, а также рассмотрены перспективы международного сотрудничества по обеспечению международной информационной безопасности.

Ключевые слова: *информационное общество, информационная безопасность, интернет, международная безопасность.*

РАЗВИТИЕ ГЛОБАЛЬНОЙ СЕТИ ИНТЕРНЕТ И ЕЕ ВЛИЯНИЕ НА МИРОВУЮ ПОЛИТИКУ

За всю историю человечества Интернет стал самым быстро растущим средством коммуникации. Масштабы использования глобальной сети неуклонно возрастают: если в начале 2008 г. насчитывалось 1,4 млрд пользователей, то в 2014 г. их число удвоилось и достигло 2,8 млрд, то есть составило уже более трети населения Земли [33]. В сети размещено несколько миллиардов сайтов и изображений, а объем передаваемых через Интернет данных удваивается ежеквартально. В России на 2014 г. Интернетом пользовалось 47 % населения страны, то есть около 68 млн человек [4]. Если телефону, чтобы занять 30 % рынка домаш-

*Статья подготовлена в рамках проекта РНФ «Долгосрочное прогнозирование развития международных отношений» № 14-18-02973

них хозяйств, потребовалось 38 лет, то Интернету – всего 7. В целом с 2000 г. количество пользователей Интернета в мире выросло на 342 % [33].

Зарождение Интернета датируется 1969 г., когда четыре компьютера впервые были объединены в сеть в рамках научно-исследовательских работ Министерства обороны США. Современный Интернет состоит из технической инфраструктуры, включающей в себя серверы, маршрутизаторы, кабельные и беспроводные, в том числе спутниковые каналы связи, компьютеры конечных пользователей, и передающейся по этим сетям информации, то есть собственно содержания Интернета. Самым популярным сервисом Интернета, делающим его столь удобным для пользователя, является «Всемирная (коммуникационная) паутина» (World Wide Web, WWW), представляющая собой связанные гиперссылками графически представленные текстовые страницы, изображения, видео в сочетании с необходимым программным обеспечением для их распространения и воспроизведения. Другими видами сервисов являются электронная почта, файлообменные или peer-to-peer сети, IP-телефония, электронные платёжные системы и др. Слаженную работу Интернета как единой информационной системы обеспечивает система доменных имен и корневых серверов.

В западной литературе часто используется понятие киберпространства, под которым понимается виртуальная сфера хранения информации и оперирования с ней, не привязанная ни к какой определенной территории, но доступная в любой точке мира через Интернет. Несмотря на то, что информация, размещенная в Интернете, физически хранится в компьютерных системах, которые расположены на территории той или иной страны, киберпространство транснационально, оно как бы находится вне территории государств.

На сегодняшний день охват Интернета глобален, при этом наибольшее число пользователей проживает в Азии (44 % от общего числа, всего более 1 млрд), на втором месте Европа (21,5 % от общего числа, всего 518 млн), затем Северная Америка (11 % от общего числа, всего 273 млн). Менее всего пользователей в Австралии и Океании (1 % от общего числа, всего 24 млн; впрочем, там и численность населения меньше, чем в любой другой части света) [33]. В России 2014 г. Интернетом пользовалось 47 % взрослого населения страны, то есть около 55 млн человек, при этом по числу пользователей лидируют Москва и Санкт-Петербург, несмотря на постепенное преодоление цифрового разрыва, особенно за счет сельской местности. В целом уровень проникновения Интернета в РФ относительно невысок – 47 %, однако в крупных городах он превышает 65 % [14]. Статистические данные показывают, насколько велик вес Интернета как средства коммуникации в современном обществе.

На современном этапе можно выделить ряд тенденций, характерных для развития интернета, которые неизбежно окажут существенное влияние на будущий облик глобального информационного общества, в том числе в контексте безопасности его развития.

1. Основное количество вновь подключающихся пользователей проживает в странах Азии и Ближнего Востока. По экспертным оценкам, эти регионы сохранят свой потенциал для Интернет-технологий и в обозримом будущем. Как следствие: второй по распространенности после английского языка в Интернете – китайский [33], и у него есть все шансы обойти английский, особенно после внедрения многоязычных доменных имен (многоязычные доменные имена – имена, представленные символами национальных алфавитов, а не только латинского алфавита). Россия также стремится занять достойное место в Интернет-пространстве и упрочить позиции русского языка. В 2010 г. был создан домен на кириллице «.рф». Таким образом, в будущем мы станем свидетелями действительно многоязычного Интернета.
2. Идет формирование так называемой повсеместной сети, или Web 3.0. Большая часть подключений осуществляется не с помощью стационарных компьютеров (как это было предусмотрено создателями сети), а с помощью мобильных телефонов и иных типов устройств, использующих, как правило, динамические IP-адреса (динамические IP-адреса присваиваются устройству, подключаемому к сети, только на время подключения, в отличие от традиционных, статических IP-адресов, которые присваиваются устройствам – персональным компьютерам – на постоянной основе).

3. Широкое распространение получают блоги, социальные и peer-to-peer сети, вследствие чего пользователи уже не являются пассивными получателями информации, а ее активными создателями, зачастую создавая серьезную конкуренцию ведущим медиакомпаниям. В 2009 г. число пользователей социальных сетей впервые превысило число пользователей электронной почты. В настоящее время число пользователей социальной сети Facebook превышает 1 млрд, причем наибольший прирост пользователей Facebook наблюдается в таких регионах, как Россия, Индия, Бразилия, Ближний Восток и Африка. Быстро развиваются и национальные социальные сетевые сервисы. Так, по данным компании Alexa, российская социальная сеть «В контакте» занимает 26-е место в мире по объему трафика (для сравнения Facebook занимает 1-е место, Twitter – 7-е, а китайская социальная сеть QQ – 10-е) [42].
4. Наметилась тенденция к конвергенции телекоммуникаций или появлению унифицированных коммуникаций. Постепенно происходит объединение Интернета и других телекоммуникационных технологий: радио, телевидения, телефона и др. на основе IP-сетей или сетей, основанных на пакетной передаче данных.
5. Широкое распространение получает «облачная» обработка данных. Все больше цифровых ресурсов отдельных пользователей и организаций хранится и обрабатывается на так называемых «серверных фермах», то есть комплексах крупных хранилищ данных. Услуги «облачной» обработки данных предоставляют такие компании, как Google, Microsoft, Apple, Amazon и Facebook. Распространение такого рода технологий в условиях возрастающей зависимости общества от информации делает Интернет действительно трансграничным, но при этом обостряет политическое измерение контроля перемещения информационных потоков в Интернете.
6. К перспективным технологическим тенденциям развития Интернета относят также появление так называемых «больших данных» (англ. Big Data). Как правило, под «большими данными» понимают массивы данных, размер которых превышает чисто аппаратные возможности их хранения, управления и анализа. Сам термин получил распространение во второй половине 2000-х гг. в связи с оцифровкой больших массивов данных, а также появлением значительных объемов цифровой персональной информации пользователей социальных сетей. Появление «больших данных», а также специального программного обеспечения и разнообразных интеллектуальных технологий, делающих возможным преодоление аппаратных ограничений и позволяющего анализировать «Большие данные», в перспективе может стать, помимо всего прочего, очередным пунктом в повестке дня международной информационной безопасности. Как отмечают К.Н. Кукьер и В. Майер-Шёнбергер: «Если говорить об ускорении экономического роста, оказании услуг населению или о ведении войн, преимущества получат те, кто сможет поставить «большие данные» себе на службу» [8].

Как и любая другая технология, информационные технологии и сформировавшееся на их основе информационное общество оказываются тесно связанными с политикой, так как определение ключевых характеристик технологий является предметом политических противоречий, в том числе на международном уровне. Транснациональная природа информационного пространства, а также ряд иных его характеристик и перспективных тенденций развития диктуют необходимость международного взаимодействия, в том числе с целью обеспечения безопасности информационно-коммуникационных технологий и глобального информационного общества.

Теоретики глобализации обращали внимание на сжатие пространства-времени в связи с развитием Интернета, спонтанность событий, а также возрастающее глобальное самосознание, которые связаны с целым рядом современных организационных форм [23]. Исследователи социального капитала признают появление новых форм социального взаимодействия и взаимосвязи и упадок или исчезновение традиционных организаций,

которые обладают возможностью создания управляемых персональных взаимодействий [25]. Кроме того, политологи отмечают формирование альтернативных публичных сфер политики в связи с информационной революцией [24].

Интернет усиливает многие значимые тенденции и процессы современной мировой политики, в том числе глобализацию, размывание государственных границ, взаимозависимость в экономической сфере, выход на мировую арену негосударственных акторов. Одним из негативных последствий глобальной информатизации стало ее влияние на межгосударственное противоборство, которое активно проникает в цифровую среду, порождая такой феномен, как информационные войны и конфликты, а также кибершпионаж. Террористическая и преступная деятельность также пополнилась новым арсеналом средств информационного воздействия, порождая новые угрозы национальной и международной безопасности.

ТЕОРЕТИЧЕСКИЕ ПОДХОДЫ К ИССЛЕДОВАНИЮ ГЛОБАЛЬНОГО ИНФОРМАЦИОННОГО ОБЩЕСТВА

Важная роль информационных технологий выражается сегодня в том, что современное общество описывается как информационное. Термин «информационное общество» получил широкое распространение и в официальных документах на международном (напр., Окинавская хартия глобального информационного общества, принятая «Группой восьми» в 2000 г., итоговые документы *Всемирной встречи на высшем уровне по вопросам информационного общества*, проходившей под эгидой ООН в 2003 и 2005 гг. и др.) и национальном уровнях (в том числе в официальных документах Российской Федерации, таких как *Стратегия построения информационного общества 2008 г., Долгосрочная федеральная целевая программа «Информационное общество 2011–2018»* и др.).

В научной литературе концепция «информационного общества» является относительно устоявшейся, при этом общепризнано, что Интернет является ключевой инфраструктурой, вокруг которой формируется глобальное информационное общество. Как правило, термины «постиндустриальное», «технотронное», «информационное», «сетевое», «общество, основанное на знаниях» используются как синонимы, что, вообще-то, неправомерно, поскольку данные термины отражают различные сущностные характеристики современного этапа развития (подробнее см. [12]).

Под информационным обществом понимают общество, ключевое значение в формировании, развитии и функционировании которого играет информация[1]. Причем информация и используемые для ее передачи технологии определяют экономические, политические, культурные, социальные и другие характеристики информационного общества. Большинство исследователей соглашаются в том, что международные отношения на протяжении последних десятилетий изменились под влиянием информационной революции.

В западной литературе для обозначения нового качества глобального информационного общества часто используют уже упоминавшийся выше термин (фактически – метафору, одну из разновидностей так называемой метафоры вместилища) «киберпространство». В науке о международных отношениях данный термин не обрел четкой формулировки. Р. Ридон и Н. Чоукри на основании анализа академических и публицистических статей из сферы международных отношений заключили, что термин «киберпространство» тесно связан с такими понятиями, как Интернет, информационные технологии, коммуникационные технологии, глобальные сети, социальные медиа и базы данных [41].

Несмотря на то что большинство исследователей соглашаются с тем, что категория информации является ключевой в определении информационного общества, даваемые ими определения понятия «информационное общество» существенно отличаются. Так, знаменитый испанский социолог М. Кастельс (с 1979 г. работает в США) понимает под информационным обществом общество, построенное по сетевому признаку, где ключевое значение имеет принадлежность к той или иной сети – такой, например, как сети крупных транснациональных компаний или СМИ. Глобальная информационная сеть формирует новую организационную структуру информационных процессов и потоков, которые в свою

[1] Это лишь одно из многих определений информационного общества (ср. ниже. – *прим. Ред.*).

очередь изменяют иные существующие социальные структуры, преобразуя их в сетевые. М. Кастельс полагает, что на сегодняшний день сложилась определенная культура сетевого общества, которая обуславливает глобализацию экономики, информации и культуры. М. Кастельс показывает, что сетевое общество включает в себя государства, но не ограничивается ими и представляет собой общность более высокого порядка. В заключении книги «Сетевое общество» Кастельс утверждает, что власть над потоками информации менее значима, чем власть потоков информации [23]. Социологи Д. Белл и А. Турэн обращали внимание на формирование постиндустриального общества, полагая, что потоки информации трансформировали индустриальное общество [22]. Авторитетный социолог, представитель критической школы М. Постер связывает современные медиаструктуры и общество постмодерна [40]. По мнению исследователя СМИ Г. Шиллера, придерживающегося, как и Кастельс, неомарксистских взглядов, в информационном обществе ключевое значение имеют капиталистические отношения, информация становится товаром, а крупные транснациональные корпорации получают возможности эксплуатации слаборазвитых в экономическом плане государств. Теоретическое осмысление и систематизация различных концепций информационного общества представлено в работе Ф. Уэбстера «Теории информационного общества» [18] (см. также [12; 15]).

Т. Фридман в книге «Лексус и оливковое дерево», написанной в 1999 г., подчеркивает взаимосвязь между развитием Интернета и процессами глобализации [30]. Позднее, в 2005 г., в книге «Плоский мир» он утверждает, что Интернет и другие информационные технологии сделали нас «соседями», убивают географию, расстояние и язык [31]. По его мнению, все то, что сегодня понимается под глобализацией: свободный обмен товарами, капиталами, рабочей силой, невзирая на расстояния и государственные границы, не было бы возможным без обмена информацией, знаниями и идеями.

Соглашаясь с доводами Т. Фридмана, нельзя не отметить, что развитие Интернета отнюдь не влечет за собой гомогенизацию и универсализацию мира, а также не разрешает проблему конфликтности, присущей международной системе. Ответом на стремительный рост объёма мировой информации и глобализационные процессы является сегментация и маргинализация общества. Государственные, географические разграничения дополняют новые информационные границы. Развитие Интернета создает новые линии неравенства между «инфобогатыми» и «инфобедными», что порождает противоречия на международной политической арене. Речь идет о так называемой проблеме «цифрового разрыва», нашедшей свое отражение в Окинавской хартии информационного общества, в которой призывалось сделать все возможное, чтобы каждый человек имел «возможность доступа к информационным и коммуникационным сетям» [10].

Информатизация становится доминирующей характеристикой современности. Соответственно, уровень развития общества определяется сегодня уровнем информатизации протекающих в нем процессов. Между развитым и развивающимся миром существует «цифровой разрыв». Таким образом, политическое лидерство в мире предполагает также и информационное лидерство, лидерство в информационных технологиях. Как правило, многие авторы отмечают, что сегодня информация и информационные технологии выступают в роли важной составляющей т.н. «совокупной мощи» государства. По выражению Г. Моргентау, «международная политика, как и любая другая, есть борьба за власть» [37, с. 82]. Показателями информационной силы государства являются наличие/отсутствие на его территории больших баз данных (хранение информации), суперкомпьютеров (обработка данных), а также корневых серверов и доступа к широкополосному Интернету (передача информации).

Интернет не является независимым агентом изменений, определяющим ключевые характеристики современного общества и мировой политики. Как и любая другая технология, Интернет вписан в более широкий социальный, политический, экономический контекст и чувствителен к происходящим в обществе, в том числе и на международном уровне, процессам. В сфере международной политики влияние информационной глобализации может быть систематизировано следующим образом:

- Возрастает значимость информации и знаний, вследствие чего экономическое развитие в большей степени, чем раньше, зависит от идей и знаний, а государства,

на территории которых расположены центры инноваций и высокотехнологичных производств, усиливают свое влияние на международной арене.

- Размываются границы между международной и внутренней политикой, между военной и гражданской сферами, межгосударственные границы становятся более проницаемыми, что способствует «размягчению» государственного суверенитета, однако сильные государства сохраняют потенциал влияния в глобальной информационной сфере.
- Развивается «диффузия власти» в мировой политике, вследствие чего негосударственные акторы (в частности, бизнес-структуры, неправительственные организации, исследовательские и академические сообщества, а также отдельные индивиды) активно выходят на международную арену.
- Происходит сжатие времени и пространства – в условиях глобальной информатизации изменения, в том числе и международно-политические, развиваются быстрее, и ими сложно управлять.
- Изменяется природа власти в мировой политике, происходит расширение публичной сферы, формируются транснациональные движения, организованные по сетевому признаку, контроль над информацией, знаниями, верованиями и идеями начинает рассматриваться как важный компонент контроля над материальными ресурсами: ИКТ позволяют накапливать информацию и трансформировать ее в знания, которые являются ресурсом власти.
- В условиях отсутствия общепринятых правил взаимодействия и обеспечения безопасности формируются национальные, но не международные инициативы, что создает новые и обостряет уже существующие риски и угрозы для международной информационной безопасности.

ГЛОБАЛЬНОЕ ИНФОРМАЦИОННОЕ ОБЩЕСТВО В КОНТЕКСТЕ МЕЖДУНАРОДНОЙ БЕЗОПАСНОСТИ

Одно из негативных последствий бурного развития Интернета и других информационно-коммуникационных технологий – возникновение новых форм международных конфликтов, включая информационные войны, сетевые войны, хакерские атаки и т.п. Как отмечает посол по особым поручениям МИД России, представитель Президента по международному сотрудничеству в области информационной безопасности А.В. Крутских, «основная озабоченность в сфере обеспечения международной информационной безопасности связана с возможностью применения информационно-коммуникационных технологий в целях, несовместимых с задачами обеспечения международной стабильности и безопасности» [7, с. 28–37].

Доктрина информационной безопасности России дает следующее определение: «под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства» [6]. Как справедливо отмечает российский эксперт А.В. Федоров, «в результате распространения информационно-коммуникационных технологий изменяется характер социума, следовательно, изменяется характер возникающих в нем противоречий и их разрешения» [19, с. 82]. Все большее число государств вовлекаются в создание программ информационных средств воздействия, а также ведения информационных войн. Террористические и преступные группировки также берут на вооружение средства информационного воздействия.

Категория информационной безопасности появилась в международно-политической повестке дня и, как следствие, в исследовательском и публицистическом дискурсе после окончания «холодной войны» в результате изменения геополитической ситуации и информационной революции. Изначально термин «информационная безопасность» использовался в контексте развития ИКТ для обозначения технических проблем, связанных с функционированием компьютерных сетей. Впоследствии, однако, он получил более широкое употребление, выходящее за рамки исключительно технологической сферы.

В современной российской исследовательской литературе международная информационная безопасность рассматривается в контексте так называемой «триады

угроз» международной информационной безопасности, определяемой через целеполагание ее субъектов, которая включает в себя террористическую, военную и криминальную угрозы; именно такая позиция зафиксирована в ряде документов ГА ООН [27]. Публикации западных исследователей проблем безопасности в цифровую эпоху, как правило, посвящены анализу следующих тем: защита критических информационных инфраструктур, информационные войны, информационные операции, преступность и терроризм в сфере ИКТ, информационная революция в военном деле. В основном научная литература по данной проблематике ориентирована на лиц, принимающих решения, и мало занимается разработкой и применением теории. При этом многие авторы, как российские, так и зарубежные, отмечают, что именно военно-политическое измерение угроз безопасности представляет наибольшую угрозу международной стабильности (см., напр., [37] и др.). Кроме того, в России широко представлен подход к международной информационной безопасности, который предполагает подведение под это понятие как технологических угроз безопасности, так и более широкого спектра информационно-психологических угроз (в другой терминологии социо-гуманитарных [17] или политико-идеологических [20])[2], связанных с распространением и содержанием контента информационных сетей.

В российских официальных документах и выступлениях официальных лиц практикуется расширенный подход к определению информационной безопасности, включающий в себя в себя как информационно-технические, так и политико-идеологические аспекты (что обосновывается возможным негативным влиянием некоторой части контента глобальной сети на общественное мнение в стране). Россия выступает за использование термина «информационная безопасность» в ходе международных переговоров, что подразумевает широкий подход к определению безопасности в цифровой сфере. Схожего подхода придерживается Китай. Страны Запада, особенно США, в дипломатической практике используют термин «кибербезопасность», что предполагает учет исключительно информационно-технических проблем, прежде всего обеспечение стабильной работы информационных сетей и систем, а также защиту данных.

Отметим, впрочем, что в последние годы среди западных исследователей также появляются представители подхода, подчеркивающего значимость политико-идеологической составляющей угроз информационной безопасности. В частности, М. Данн, глава отдела в Центре исследований безопасности (Швейцария) отмечает, что было бы неправильным сводить проблему информационной безопасности исключительно к инфраструктурной составляющей, к кибератакам или киберинцидентам или, напротив, к объектам безопасности, так как средства атаки могут быть физическими или виртуальными [29].

На экспертном уровне ведется работа по согласованию этих подходов. В 2011 г. Институт Восток–Запад, базирующийся в США, и Институт проблем информационной безопасности МГУ разработали и согласовали список 20 базовых терминов в сфере информационной безопасности, которые, по мысли экспертов, могли бы лечь в основу возможной двусторонней договорённости между Россией и США [40]. Список включает в себя три группы терминов, классифицированных тематически:

1) ***поле действий*** (киберпространство, кибернетическая инфраструктура, киберсервисы, критически важное киберпространство, критически важная кибернетическая инфраструктура, критически важные киберсервисы);
2) ***виды угроз*** (киберпреступление, кибертерроризм, киберконфликт, кибервойна, кибербезопасность);
3) ***способы действий*** (боевые действия в киберпространстве, кибератака, киберконтратака, оборона и противодействие в киберпространстве, кибервойна, оборонительные возможности в киберпространстве, наступательные возможности в киберпространстве, использование преимуществ в киберпространстве, средства киберсдерживания).

Можно согласиться с российским экспертом А.В. Бедрицким, который полагает, что «перечисление терминов, по которым российские и американские эксперты смогли достичь

[2] Вопрос о том, являются ли отличия между этими категориями чисто терминологическими, дискуссионен. – *Прим. ред.*

согласия, явно указывает на справедливость официальной позиции российской стороны, настаивающей на необходимости рассматривать проблемы международной информационной безопасности в разоруженческом аспекте» [1]. Показательно, что выработанная терминология основана на узком подходе и не включает в себя социо-гуманитарную составляющую информационной безопасности, что, возможно, объясняется 2011-м г. публикации данной работы, то есть до принятия официальных документов, где было закреплено приоритетное внимание к социо-гуманитарному измерению безопасности в цифровой сфере.

В докладе Группы правительственных экспертов ООН от 2010 г. указано, что глобальное информационное пространство становится ареной разрушительных действий и что киберугрозы становятся одним из важнейших вызовов XX1 века [32]. Резолюции Генеральной Ассамблеи ООН подчеркивают национальную ответственность за обеспечение информационной безопасности на уровне национальных государств [26].

Главной угрозой информационной безопасности в военно-политическом плане является ведение информационных войн и информационного противоборства между государствами. В документе «Основы государственной политики РФ в области международной информационной безопасности на период до 2020 года» использование интернет-технологий в качестве «информационного оружия в военно-политических, террористических и преступных целях», а также для «вмешательства во внутренние дела государств» обозначены как угрозы информационной безопасности для России и мира [11]. Страны НАТО российский подход к пониманию киберугроз не разделяют, отказываясь признавать возможность использования информационных технологий, социальных сетей в целях нарушения общественной стабильности и правомерность их рассмотрения как угрозы национальной и международной безопасности, что может стать препятствием на пути к международному сотрудничеству в данной области.

На современном этапе особую опасность в рамках информационно-технологической компоненты информационного противоборства приобретает воздействие на критические информационные инфраструктуры государства. Атаки вируса Stuxnet на ядерные объекты Ирана в 2010 г. показали уязвимость информационных технологий, обеспечивающих работу жизненно важных систем жизни общества и государства. В настоящее время информационные атаки на критические инфраструктуры государства, такие как системы электронного правительства, банковские системы и др., получили широкое распространение как в России, так и за рубежом. Трансграничный характер информационных технологий, их доступность, анонимность пользователей затрудняют решение проблемы. Кроме того, во многих странах большая часть критически важных информационных ресурсов, сетей и систем находится в частной собственности, что обусловливает необходимость частно-государственного партнерства для обеспечения их безопасности.

В условиях постоянного динамического развития информационных технологий происходит совершенствование видов их злонамеренного использования – появляются новые виды информационного оружия, вредоносного программного обеспечения, вирусных атак и пр. По оценке российских экспертов, современные супервирусы настолько сложны, что их создание, скорее всего, под силу только высококвалифицированным командам специалистов, для чего необходимы временные, финансовые и людские ресурсы [5].

К числу успешных примеров использования информационного оружия аналитики также относят использование супервируса-шпиона Flame, собиравшего доступную информацию в различных информационых сетях, в том числе в сетях сотовой связи, а также супервируса-шпиона Red October, который был направлен против научных и государственных информационных систем и был обнаружен в России и других странах СНГ, а также в ряде других государств Латинской Америки и Ближнего Востока.

В современных конфликтах информационное оружие используется как вспомогательное средство, расширяющее возможности вооруженных сил, а также в целях работы с мировым и внутригосударственным общественным мнением. Под информационным оружием понимают средства и методы, применяемые с целью нанесения ущерба информационным ресурсам, процессам и системам, негативного информационного воздействия на оборонные, управленческие, политические, социальные, экономические и другие критически важные инфраструктуры государства, а также массированной психологической обработки населения

с целью дестабилизации общества и государства. Приведем определения, выработанные Шанхайской организацией сотрудничества: «Информационное оружие – информационные технологии, средства и методы, применяемые в целях ведения информационной войны» [16, с. 242]; «Информационная война – противоборство между двумя или более государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам или ресурсам, критически важным и другим структурам, подрыва политической, экономической, социальной систем, массированной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны» [16, с. 242].

В условиях всеобщего доступа к информации, широкого распространения Интернета особое значение имеет работа с общественным мнением как внутри страны, так и на международной арене, что наглядно продемонстрировали события в ходе августовской пятидневной войны в Южной Осетии 2008 г. В этих условиях контроль над информационным пространством выступает как инструмент навязывания противнику своих целей посредством воздействия на его систему ценностей, установки и восприятие мира[3]. В информационно-психологической области, как отмечает российский исследователь Р.В. Болгов, воздействие оказывается на психологическую сферу с помощью методов пропаганды, дезинформации, манипулирования сознанием, которые мало изменились по своей сути со времен Сунь-цзы. Сами эти методы совершенствовались скорее эволюционно, чем революционно. Новизна заключается в использовании старых методов информационного воздействия, но с помощью новых средств (прежде всего, Интернета) [2, с. 78].

В отсутствии признанных на международном уровне понятий «информационное оружие», «информационная война», а также критериев идентификации подобных феноменов, исследователи все чаще обращаются к термину «гибридная война» или «многомерная война» [3], при этом в современных конфликтах элементы информационного и кибероружия используются все чаще. Так, как отмечает эксперт в области международной безопасности, полковник в отставке А.О. Гилев: «Современная война многомерна. Она сочетает информационное, военное, финансовое, экономическое и дипломатическое воздействие на противника в реальном времени. Предполагается, что массированное и координированное использование всех невоенных методов может оказаться достаточным, чтобы запугать и ослабить оппонента, сведя применение Вооруженных сил к минимуму. Для успеха необходимо, во-первых, обеспечить как можно более полную международную изоляцию объекта воздействия, а во-вторых, заручиться возможностью оказывать на него давление изнутри» [3]. Информационное противоборство становится частью межгосударственной конкуренции и в мирное время. Как заявил Президент Российской Федерации В.В. Путин, в 2014 г. было пресечено порядка 74 млн кибератак на официальные сайты российских структур и государственных органов [14].

В настоящее время более 120 стран занимаются разработками информационного и кибероружия, что стало наименее затратным в политическом (и не только) отношении ответом на неспособность поддерживать баланс сил в области обычных вооружений. В большинстве стран разрабатываются концепции ведения информационных войн и предпринимаются попытки их реализации. Между тем, дальнейшее движение по этому пути может расшатать сложившуюся систему международной безопасности и контроля над вооружениями. Как убедительно показал в своей работе сотрудник «РЭНД Корпорейшн» Мартин Либики, традиционные меры сдерживания в информационном пространстве малоэффективны вследствие дешевизны и доступности кибероружия, а также сложности выявления источника угрозы [37].

Можно утверждать, что гонка информационных и кибервооружений уже началась. Эта гонка на национальном и международном уровнях будет отражать текущий баланс сил на международной арене. Военные теоретики высказывают предположение, что информационное пространство становится «пятым полем боя», наряду с землей, морским и воздушным пространствами, космосом [34].

Информатизация порождает новые угрозы и для государств-лидеров, усиливая

[3] Иногда такой инструмент неправомерно отождествляется с так называемой «мягкой силой»: реально эти категории всего лишь пересекаются. – *Прим. ред.*

асимметричную составляющую современных конфликтов, в результате чего развитые в технологическом плане государства оказываются весьма уязвимыми. По мнению ряда исследователей, американская военная мощь и развитие информационного оружия на деле лишь способствовали провоцированию глобальной конфликтности, в том числе, за счет попыток противников США создать ядерное оружие, и ослабили безопасность, для обеспечения которой предназначались [3, с. 12]. Кроме того, неоднозначное влияние ИКТ на международную безопасность проявляется, с одной стороны, в их содействии демократизации (что и является их целью в соответствии с официальной позицией США) и, следовательно, снижению конфликтности. С другой стороны, информационные технологии являются удобным инструментом для создания асимметричных угроз и наращивания политического влияния, результатом чего становится провоцирование новых вооруженных столкновений [3, с. 13].

В результате глобальной информатизации формируется новая среда безопасности и новые вызовы, на которые государства вынуждены реагировать. Многие из них носят внутренний характер, хотя и проистекают из киберпространства, которое по своей природе транснационально. Вместе с тем растет список общих, стоящих перед всеми государствами вызовов, который мог бы стать основой для достижения международных договоренностей.

Информационное пространство по своей природе транснационально, информационные вызовы и угрозы не ограничиваются пределами отдельных государств. Для обеспечения международной информационной безопасности необходимо сотрудничество, опирающееся на нормы международного права при учете особенностей цифровой среды. Поиск путей предотвращения как государствами, так и террористическими и иными преступными организациями злонамеренного использования информационно-коммуникативных технологий, способного привести к нарушению международного мира и безопасности, является в последние годы одним из трендов в дискуссиях политиков, ученых и специалистов в данной области.

CHALLENGES AND THREATS OF THE GLOBAL INFORMATION SOCIETY

***Elena Zinovieva**, PhD (Political Science),*
Associate Professor at the Department of World Politics,
MGIMO-University, 76 Vernadsky Ave., 119454. Moscow.
E-mail: zinovjeva@mail.ru

Summary

The article investigates the challenges and risks to international security arising from the development of the global information society. The basic trends of the global information society development are analyzed, as well as theoretical approaches to the theory of information society. The author also assesses the impact of the global information society development on the world politics. The paper examines the main challenges, risks and threats arising from the development of the global information society, as well as the prospects for international cooperation in the field of international information security.

Key words: *information society, information security, Internet, international security.*

ЛИТЕРАТУРА / REFERENCES

1. *Бедрицкий А.В.* Международные договорённости по киберпространству: возможен ли консенсус? // Проблемы национальной стратегии. 2012. №4. [Электронный ресурс]. URL: http://www.riss.ru/images/pdf/journal/2012/4/10_.pdf
2. *Болгов Р.В.* Информационные технологии в современных военных конфликтах и вооруженных стратегиях. Дисс. на соискание ученой степени канд. полит. наук. –СПбГУ, 2011.
3. *Гилев А.О.* Многомерная война и новая оборонная стратегия // Россия в глобальной политике. № 5. 2014. [Электронный ресурс]. URL: http://www.globalaffairs.ru/number/Mnogomernaya-voina-i-novaya-oboronnaya-strategiya-17101

4. Глава Минсвязи: Число пользователей Интернета в России увеличится на 30 млн человек // РБК, 22.05.2014. [Электронный ресурс]. URL: http://www.rbc.ru/rbcfreenews/20140522014554.shtml
5. *Демидов О., Симоненко М.* Пожар в киберпространстве // Индекс безопасности. 2013. № 1. [Электронный ресурс]. URL: http://www.pircenter.org/media/content/files/10/ 13559127940.pdf
6. Доктрина информационной безопасности РФ. Утверждена 09.09.2000.
7. *Крутских А.В.* К политико-правовым основаниям глобальной информационной безопасности // Международные процессы. – М., 2007. № 1 (5). [Электронный ресурс]. URL:http://www.intertrends.ru/thirteen/003.htm
8. *Кукиер К., Майер-Шёнбергер В.* Большие данные // Россия в глобальной политике. 2013. № 3. [Электронный ресурс].URL: http://www.globalaffairs.ru/number/Bolshie-dannye--16038
9. *Куликова А.* Возможна ли гонка кибервооружений между Россией и США? // ПИР Центр, 28.01.2015. [Электронный ресурс]. URL: http://pircenter.org/media/content/files/13/14243529940.pdf
10. Окинавская Хартия глобального информационного общества. «Группа восьми». – Окинава, 2000. [Электронный ресурс]. URL:http://www.ifap.ru/ofdocs/okinhar.htm
11. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года. Утвержден 01.08.2013. // Совет Безопасности РФ: официальный сайт.
12. *Паршин П.Б.* Глобальное информационное общество и мировая политика // Аналитические доклады ИМИ. – М.: МГИМО-Университет, 2009. № 2 (23).
13. Путин: ФСБ в 2014 году пресекла 74 миллиона кибератак. РИА Новости. 26.03.2015. [Электронный ресурс]. URL: http://ria.ru/defense_safety/20150326/1054622560.html
14. Развитие Интернета в регионах России // Информационный бюллетень Яндекс. Весна 2012. [Электронный ресурс].URL: http://download.yandex.ru/company/ya_regions_report_spring_2012.pdf
15. *Сергеев В.М.* Сравнительное изучение сетевых связей в современном мире (ворота в глобальный мир) // Ежегодник ИМИ. Вып. 3–4. – М.: МГИМО-Университет, 2014.
16. Соглашение между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. 2009 г. // Международная информационная безопасность: дипломатия мира: сборник материалов / под ред. С.А. Комова. – М., 2009.
17. *Стрельцов А.А.* Правовое обеспечение информационной безопасности России: теоретические и методологические основы. – М., 2004. [Электронный ресурс]. URL: http://www.iisi.msu.ru/UserFiles/File/publications/Streltsov.pdf
18. *Уэбстер Ф.* Теории информационного общества. М.: Аспект-Пресс, 2005.
19. *Федоров А.В.* Информационная безопасность в мировом политическом процессе: Учебное пособие. – М.: МГИМО-Университет, 2006.
20. *Черненко Е.В.* Холодная война 2.0 // Россия в глобальной политике. 2013. № 1. [Электронный ресурс]. URL: http://www.globalaffairs.ru/number/Kholodnaya-voina-20-15874
21. Barlow J. A Declaration of the Independence of Cyberspace. – 1996. URL:http://homes.eff.org/~barlow/Declaration-Final.html.
22. *Bell D.* The coming of post-industrial society: A venture of social forecasting. – N.Y.: Basic Books, 1973; *Touraine A.* The Post-Industrial Society. Tomorrow's Social History: Classes, Conflicts and Culture in the Programmed Society. – N.Y.: Random House, 1971.
23. *Castells M.* End of Millennium. Volume 3, The Information Age: Economy, Society and Culture. – Oxford: Blackwell Publishers, 1998.
24. *Castells M.* The New Public Sphere: Global Civil Society, Communication Networks, and Global Governance // The Annals of the American Academy of Political and Social Science. 2008. № 616. URL:http://prtheories.pbworks.com/w/file/fetch/ 45138545/ Castells_2008_The_New_Public_Sphere.pdf
25. *Castells M.* The rise of network society. The Information Age: Economy, Society and Culture Vol. *I. Malden,* MA. – Oxford, UK: Blackwell, 1996.
26. Cyberprotest: new media, citizens and social movements / Ed. by *W. van d Donk, B. Loader, P. Nixon, D. Rucht.* Routlege, 2004.

27. Developments in the Field of Information and Telecommunications in the Context of International Security/, UN document A/RES/63/37. 02.12.2008.
28. Ibid.
29. *Dunn M.* Securing the digital age: the challenges of complexity for critical infrastructure protection and IR theory // International relations and security in the digital age/ Ed by *Eriksson J., Giacomello G.* Routledge, 2007.
30. *Friedman T.* The Lexus and the OliveTree. – N.Y.: Farrar Straus & Giroux, 1999.
31. *Friedman T.* The world is flat: a brief history of the twenty-first century. – N.Y.: Farrar, Straus and Giroux, 2007.
32. General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN document A/65/201, 30 July 2010.
33. Internet World Stats.Usage and population statistics. URL:www.internetworldstats.org
34. *Lewis J., Timlin K.* Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization, UNIDIR, 2011.
35. *Libicki M.* Cyberdeterrence and Cyberwar. Santa Monica, CA: RAND Corporation, 2009.
36. *Molander R.* Strategic Information Warfare: A New Face of War / *R. Molander, A. Riddile, P. Wilson*. CA: Rand Corporation, 1996.
37. *Morgenthau H.* Politics among nations: the struggle for peace and power. 1973.
38. *Neuneck G.* Civilian and military cyberthreats: shifting identities an attribution. // The Cyber Index. International Security Trends and Realities. UNIDIR, 2013. P. 115 // URL: http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf
39. *Poster M.* The second media age. Blackwell, 1995.
40. *Rauscher K.F., Yaschenko V.* Russia–US Bilateral on Cyber Security: Critical Terminology Foundations. – N.Y., USA: EastWest Institute. 2011.
41. *Reardon R., Choucri N.* The Role of Cyberspace in International Relations: A View of the Literature. Paper prepared for the 2012 ISA Annual Convention. San Diego, CA April 1, 2012. URL: http://ecir.mit.edu/images/stories/Reardon%20and%20Choucri_ISA_ 2012.pdf/
42. Top Sites. Alexa Rank. The top 500 sites on the web. URL:http://www.alexa.com/topsites