

АНАЛИЗ ВНЕШНЕПОЛИТИЧЕСКИХ ИНИЦИАТИВ РОССИИ В ОБЛАСТИ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Е.С. Зиновьева

Московский государственный институт международных отношений (университет)
МИД России. Россия, 119454, Москва, пр. Вернадского, 76.

Развитие информационных и коммуникационных технологий (ИКТ) играет важнейшую роль для повышения качества жизни человека, экономического и социально-политического прогресса как каждой страны в отдельности, так и всего человечества в целом. Однако оно чревато новыми информационными вызовами и угрозами международной и национальной безопасности. Межгосударственное противоборство, перешедшее в информационную сферу, порождает конфликты, крайней формой проявления которых являются информационные войны. В статье изучены особенности глобального информационного общества, оказывающие определяющее влияние и на характер международной безопасности в информационную эпоху, и на международное сотрудничество в данной области. Также приводится анализ позиции и интересов России в этой сфере, российских внешнеполитических инициатив по вопросам международной информационной безопасности, с которыми наша страна постоянно выступает с 1998 г. По инициативе России проблематика международной информационной безопасности рассматривалась в рамках ОБСЕ, ШОС, ОДКБ, Международного союза электросвязи (МСЭ), в ходе Всемирной встречи на высшем уровне по вопросам информационного общества (ВВУИО), в рамках СНГ и Регионального содружества в области связи (РСС). Работа также ведётся «на полях» таких форумов, как «Группа восьми», «Группа двадцати», БРИКС.

Сегодня более 130 государств развивают программы ведения кибервойн, что создаёт серьёзные угрозы информационной стабильности, ибо отследить источник информационной атаки сложно, а последствия её могут быть разрушительными и стать причиной ответного удара, в том числе с использованием обычных вооружений. В этой ситуации подход России, выступающей за выработку правил поведения государств и демилитаризацию информационного пространства с целью обеспечения его безопасности, представляется актуальным.

Ключевые слова: Интернет, международная информационная безопасность, информационная стабильность, правила поведения государств в информационном пространстве, внешняя политика России, угрозы, российские инициативы.

Развитие информационных и коммуникационных технологий (ИКТ) играет важнейшую роль в повышении качества жизни человека, экономического и социально-политического развития как каждой страны в отдельности, так и человечества в целом. Однако развитие ИКТ чревато новыми информационными вызовами и угрозами международной и национальной безопасности. Межгосударственное противоборство, перешедшее в информационную сферу, порождает конфликты, крайней формой проявления которых являются информационные войны.

В последнее время существенно увеличилось количество деструктивных информационных атак, совершаемых с использованием современных информационных технологий, которые становятся всё сложнее. Прогнозируется, что в ближайшей перспективе объектами их воздействия будут не только информационные ресурсы в Интернете, но и критически важные объекты инфраструктуры государств, обеспечивающие функционирование промышленности, транспорта, энергетики и другие сферы жизнедеятельности.

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 учёте особенностей цифровой среды. Особенности Интернета как глобальной информационной системы оказывают ключевое влияние на международную информационную безопасность. Интернет представляет собой сложную и неоднородную макросистему, объединяющую очень большое число различных информационных сетей. Современный Интернет состоит из технической инфраструктуры, включающей в себя серверы, маршрутизаторы, кабели, 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» (WorldWideWeb, 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. Связную работу Интернета как единой информационной системы обеспечивает система доменных имён и корневых серверов.

Исследователи «Проекта управления Интернетом» при Сиракузском университете (Internet governance project) выделяют следующие особен-

ности Интернета, которые следует принимать во внимание в ходе анализа управления им:

1. Открытость стандартов. Интернет основывается на открытых технических стандартах, которые может бесплатно использовать каждый. В ряде случаев в стандартах Интернет-протоколов используются запатентованные технологии, но они, как правило, доступны по разумной цене.

2. Рыночные механизмы. Сети, составляющие Интернет и соединяемые протоколами, принадлежат различным организациям, в большинстве случаев представителям частного бизнеса. Большая часть инвестиций исходит от частного сектора. Услуги и соединение координируются в основном на рыночной, контрактной основе;

3. Интеллектуальные средства и контрольные функции сосредоточены на периферии Сети. Функция Сети – передача информации, сами протоколы технологически нейтральны.

4. Глобальный характер: Интернет не локализован ни в одном национальном государстве, соединение устанавливается вне зависимости от национальных границ [4].

Определение Интернета, как и любой другой технологии, будет неполным без характеристики последних тенденций в развитии Сети.

1. Основное количество вновь подключающихся пользователей проживает в странах Азии и Ближнего Востока. По экспертным оценкам, эти регионы сохраняют свой потенциал для Интернет-технологий и в обозримом будущем. Как следствие, второй по распространённости язык в Интернете – китайский [1], и у него есть все шансы обойти английский, особенно после внедрения многоязычных доменных имён (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. Идёт формирование 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 неограниченный период времени.

3. Широкое распространение получают блоги, социальные и peer-to-peer сети, вследствие чего пользователи уже не являются пассивными получателями информации, а её активными создателями, зачастую создавая серьёзную кон-

курению ведущим медиа-компаниям. В 2009 г. впервые число пользователей социальных сетей превысило число пользователей электронной почты, причём социальные сети намного более популярны среди женщин, чем среди мужчин. В настоящее время число пользователей социальной сети Facebook превышает 1 млрд, причём наибольший прирост 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 19-е место в мире по объёму трафика (для сравнения, «Facebook» занимает 1-е место, а китайская социальная сеть «QQ» – 8-е) [3].

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. Всё больше цифровых ресурсов отдельных пользователей и организаций хранится и обрабатывается на «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.

Т. Фридман в книге «Лексус и оливковое дерево», написанной в 1999 г., подчёркивает взаимосвязь между развитием Интернета и процесса глобализации [7]. Позднее, в 2005 г., в книге «Плоский мир» он утверждает, что Интернет и другие информационные технологии сделали нас «соседями», убивают географию, расстояния и язык [8]. По его мнению, всё то, что сегодня понимается под глобализацией, а именно: свободный обмен товарами, капиталами, рабочей силой, невзирая на расстояния и государственные границы, не было бы возможным без обмена информацией, знаниями, идеями.

Соглашаясь с доводами Т. Фридмана, нельзя не отметить, что развитие Интернета отнюдь не влечёт 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.

В условиях быстрого развития Интернета, доступности информации, дешевизны доступа

к соответствующим технологиям обостряется проблема информационной безопасности. Появляются новые вызовы и угрозы, такие как информационная преступность, информационный терроризм, а также межгосударственное противоборство в информационной сфере. Трансграничный характер Интернета обусловил необходимость поиска ответов на те вызовы, которые ставит информационное общество на международном уровне.

Международная информационная безопасность трактуется, прежде всего, исходя из характера угроз. Традиционно выделялась «триада угроз» международной информационной безопасности — использование ИКТ в террористических, преступных и военно-политических целях (под военно-политическими целями понимается использование ИКТ в межгосударственных конфликтах). В частности, подобный подход к определению угроз был закреплён в ряде резолюций ГА ООН, посвящённых проблематике информационной безопасности.

Россия в 2013 г. в документе «Основы государственной политики в области международной информационной безопасности на период до 2020 г.» [9] добавила к триаде угроз опасность вмешательства во внутренние дела суверенного государства посредством ИКТ, нарушение общественной стабильности, разжигание межнациональной розни. По сути, это стало реакцией России на события «арабской весны», когда социальные сети и блоги активно использовались для координации протестного движения.

Относительно терминологии нет единства мнений — ведутся дискуссии между государствами, придерживающимися различных толкований понятия «международная информационная безопасность». Россия выступает за широкий подход к определению содержания этого понятия, включая в него как технические аспекты (безопасность информационных сетей и систем), так и обширный круг политико-идеологических аспектов (манипулирование информацией, пропаганда посредством глобальных информационных сетей, информационное воздействие). Страны Запада, прежде всего США, придерживаются узкого подхода, ограничиваясь техническими аспектами, и используют иную терминологию — «кибербезопасность».

Значимость национальных интересов России в области обеспечения информационной безопасности и управления Интернетом особо подчёркивает тот факт, что они упоминаются в целом ряде официальных документов последних лет, среди которых «Стратегия национальной безопасности Российской Федерации до 2020 г.» [8], «Стратегия развития информационного общества Российской Федерации» [3], «Концепция внешней политики Российской Федерации» [4], «Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 г.» [9]

■ Интернет - Политика

и др. В «Стратегии национальной безопасности Российской Федерации до 2020 г.» [8] информационная безопасность рассматривается в качестве одной из важнейших составляющих национальной безопасности страны.

На сегодняшний день Россия является одним из наиболее динамичных и устойчиво растущих рынков ИКТ в мире. Вместе с тем, как показывают результаты исследований, российский сектор Интернета (ру-нет) сталкивается со значительным числом киберугроз, как внутренних, так и внешних. Это также актуализирует необходимость международного сотрудничества по обеспечению информационной безопасности, за что и выступает Россия.

Россия исходит из потребности выработки определённых правил поведения государств в информационном пространстве. Это предполагает заключение международных договорённостей, на основании которых государства отказались бы от использования, передачи и применения средств информационного воздействия, то есть осуществления любых возможных агрессивных действий в информационном пространстве. Кроме того, обеспечение международной информационной безопасности предполагает противодействие международной информационной преступности и терроризму.

Россия активно участвует в международных переговорах по обеспечению информационной безопасности. Это является практическим воплощением официальной позиции нашей страны, изложенной как в «Стратегии развития информационного общества Российской Федерации» [3], так и в «Концепции внешней политики Российской Федерации» [4]. В соответствии с этими документами, перед российской дипломатией ставится задача обеспечить эффективное вхождение страны в глобальное информационное пространство.

Анализ документов и выступлений официальных лиц позволяет сделать вывод, что Россия выступает за демилитаризацию информационного пространства, так как гонка вооружений в информационной сфере способна расшатать сложившиеся договорённости о разоружении и международной безопасности. Согласно «Основам государственной политики в области международной информационной безопасности на период до 2020 г.» [9]. Россия ставит целью государственной политики в области международной информационной безопасности содействие установлению международного правового режима, направленного на создание условий для формирования системы международной информационной безопасности; достижению

этой цели, среди прочего, будет способствовать создание условий, обеспечивающих снижение риска использования ИКТ для осуществления враждебных действий и актов агрессии, направленных на дискредитацию суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности. В «Концепции внешней политики Российской Федерации» [4] указано, что Россия будет добиваться выработки под эгидой ООН правил поведения в области обеспечения международной информационной безопасности.

С 1998 г. Россия инициативно выступает за развитие и углубление международного сотрудничества по обеспечению информационной безопасности как на глобальном, так и на региональном уровне, а также в рамках двусторонних отношений. Договорённости о сотрудничестве по международной информационной безопасности были достигнуты с рядом государств, в том числе со странами ШОС, Белоруссией, Кубой. В 2013 г. был заключён ряд важных договоров с США, направленных на формирование мер укрепления доверия в глобальном информационном пространстве. По инициативе России проблемы международной информационной безопасности рассматривались на высоком политическом уровне и многосторонней основе, в рамках ОБСЕ, ШОС, ОДКБ, Международного союза электросвязи (МСЭ), в ходе Всемирной встречи на высшем уровне по вопросам информационного общества (ВВУИО), в рамках СНГ и Регионального содружества в области связи (РСС). Работа также ведётся «на полях» таких форумов, как «Группа восьми», «Группа двадцати», БРИКС. В официальных документах этих международных форумов и организаций были закреплены положения о наличии угроз для международной информационной безопасности и о необходимости международного сотрудничества в данной области.

Сегодня более 130 государств развивают программы ведения кибервойн, что создаёт серьёзные угрозы информационной стабильности: отследить источник информационной атаки сложно, последствия её могут быть разрушительными и стать причиной ответного удара, в том числе с использованием обычных вооружений. В этой ситуации подход России, выступающей за выработку правил поведения государств в информационном пространстве с целью обеспечения безопасности, представляется актуальным и соответствующим международной ситуации.

Список литературы

1. Internet World Stats Usage and Population Statistics. Режим доступа: www.internetworldstats.org
2. Top Sites. Alexa Rank. The Top 500 Sites on the Web. Режим доступа: <http://www.alexa.com/topsites>

3. Стратегия развития информационного общества в Российской Федерации. 2008. Утв. Президентом 7 февраля. Режим доступа: <http://www.mid.ru/ns-osndoc.nsf/0e9272befa34209743256c630042d1aa/453f799b9fe0637cc32573f3002b2558?OpenDocument>
4. Концепция внешней политики Российской Федерации. 2013. Утв. Президентом 12 февраля. Режим доступа: <http://mid.ru/bdomp/ns-osndoc.nsf/e2f289bea62097f9c325787a0034c255/c32577ca0017434944257b160051bf7f!OpenDocument>
5. Mathiason J. 2004. Internet Governance: The State of Play // Internet Governance Project. Режим доступа: <http://dcc.syr.edu/miscarticles/MainReport-final.pdf>
6. Friedman T. 1999. The Lexus and the Olive Tree. N.Y.: Farrar Straus & Giroux. 394 p.
7. Friedman T. 2007. The World Is Flat: a Brief History of the Twenty-First Century. N.Y.: Farrar, Straus and Giroux. 660 p.
8. Стратегия национальной безопасности России до 2020 года. 2009. Утв. Президентом 12 мая указом № 537. Режим доступа: <http://www.mid.ru/bdomp/ns-osndoc.nsf/e2f289bea62097f9c325787a0034c255/8abb3c17eb3d2626c32575b500320ae4!OpenDocument>
9. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года. 2013. Утв. Президентом 24 июля. Режим доступа: <http://www.scrf.gov.ru/documents/6/114.html>

Об авторе

Зиновьева Елена Сергеевна – к.полит.н., доцент кафедры мировых политических процессов МГИМО(У) МИД России. E-mail: zinovjeva@mail.ru.

Статья подготовлена в рамках работ по гранту РГНФ 14-57-00005 «Международное сотрудничество по обеспечению информационной безопасности».

ANALYSIS OF RUSSIAN FEDERATION FOREIGN POLICY IN THE FIELD OF INTERNATIONAL INFORMATION SECURITY

E. Zinovi'eva

Moscow State Institute of International Relations (University), 76 Prospect Vernadskogo, Moscow, 119454, Russia

Abstract: *Information and communication technologies (ICT) play an essential role in the improvement of the quality of life, economic and socio-political of individual countries and humanity in general.*

However, ICT development is fraught with new challenges and threats to international and national security. Interstate rivalry in the information sphere generates conflicts, an extreme form of which is an information war.

Since 1998, the Russian initiative supports the international cooperation on information security at the global and regional level as well as within the framework of the bilateral relations.

The article analyzes the characteristics of the global information society, which has a decisive influence on the international security in the information age, as well as international cooperation in this field. The analysis of Russian foreign policy initiatives in the field of international information security is also presented.

Today more than 130 countries develop cyber capabilities, both defensive and offensive, that pose serious threats to the international stability. It's difficult to trace the source of information attacks and its consequences can be devastating and cause retaliation, including the use of conventional weapons. In this situation Russian approach, advocating for the development of the rules of conduct of States and demilitarization of information space in order to ensure its safety, seems urgent and relevant with the international situation.

Key words: Internet, International Information Security, Russian Foreign Policy.

References

1. Internet World Stats. Usage and Population Statistics. Available at: www.internetworldstats.org
-

■ Интернет - Политика

2. Top Sites. Alexa Rank. The Top 500 Sites on the Web. Available at: <http://www.alexa.com/topsites>
3. Strategy of Information Society Development in the Russian Federation. 2008. Approved by the President on 7 February. Available at: <http://www.mid.ru/ns-osndoc.nsf/0e9272befa34209743256c630042d1aa/453f799b9fe0637cc32573f3002b2558?OpenDocument> (In Russian)
4. The Foreign Policy Concept of the Russian Federation. 2013. Approved by the President 12 February Available at: <http://mid.ru/bdomp/ns-osndoc.nsf/e2f289bea62097f9c325787a0034c255/c32577ca0017434944257b160051bf7f?OpenDocument> (In Russian)
5. Mathiason J. 2004. Internet Governance: The State of Play. Internet Governance Project. Available at: <http://dcc.syr.edu/miscarticles/MainReport-final.pdf>
6. Friedman T. 1999. The Lexus and the Olive Tree. N.Y.: Farrar Straus & Giroux. 394 p.
7. Friedman T. 2007. The World Is Flat: a brief history of the twenty-first century. N.Y.: Farrar, Straus and Giroux. 660 p.
8. National Security Strategy of Russian Federation. 2009. Approved by the President 12 May. Presidential decree no 537. Available at: http://www.mid.ru/bdomp/ns-osndoc.nsf/e2f289bea62097f9c325787a0034c255/8abb3c17eb3d2626c32575b500_320ae4?OpenDocument (In Russian)
9. Basics of the State Policy of Russian Federation in the Field of International Information Security for the Period up to 2020. 2013. Approved by the President 24 July. Available at: <http://www.scrf.gov.ru/documents/6/114.html> (In Russian)

About the author

Elena S. Zinovi'eva – PhD in Political Science, Associate Professor of the Department of World Political Processes, of the MGIMO – University of the RF MIA. E-mail: zinovjeva@mail.ru.