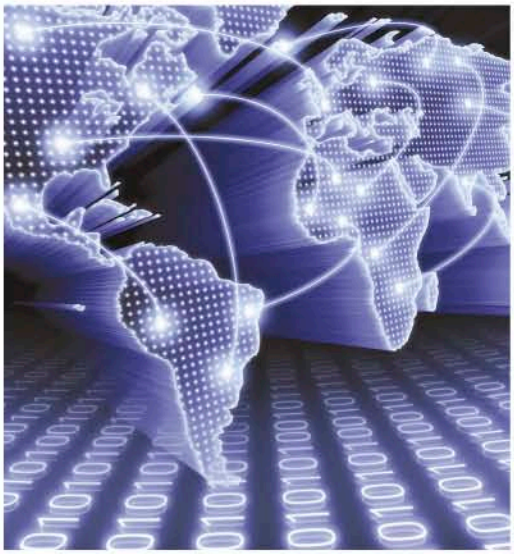
РСМД

Российский совет
по международным
делам



РАБОЧАЯ ТЕТРАДЬ

РОССИЯ
И ВЫЗОВЫ ЦИФРОВОЙ СРЕДЫ

№ XV | 2014

Российский совет по международным делам

Москва 2014

УДК 004.056(470+571)
ББК 32.973.2(2Рос)-018.2
О35

Российский совет по международным делам

Главный редактор:
докт. ист. наук, член-корр. РАН **И.С. Иванов**

Авторский коллектив:
докт. юрид. наук **В.С. Овчинский**; **Е.С. Ларина**; канд. полит. наук **С.А. Кулик**

Выпускающие редакторы:
канд. полит. наук **И.Н. Тимофеев**; канд. полит. наук **Т.А. Махмутов**;
А.Л. Тесля

Россия и вызовы цифровой среды: рабочая тетр. / [В.С. Овчинский и др.]; [гл. ред. И.С. Иванов]; Российский совет по междунар. делам (РСМД). – М.: Спецкнига, 2014. – 40 с. – Авт. указаны на обороте тит. л. – ISBN 978-5-91891-367-3.

Рабочая тетрадь подготовлена в рамках проекта РСМД «Информационная безопасность, противодействие киберугрозам и использование Интернета в целях защиты национальных интересов России на международной арене». Рассматриваемые авторами статей вопросы присутствия России в виртуальном пространстве предполагают определение исходной точки для развития дискуссии и поиска эффективной стратегии для российских участников глобальных интернет-процессов. При этом специальное внимание в материалах уделяется использованию сетевых инструментов для повышения качества реализации внешней политики.

Высказанные в рабочей тетради мнения отражают исключительно личные взгляды и исследовательские позиции авторов и могут не совпадать с точкой зрения Некоммерческого партнерства «Российский совет по международным делам».

ПОЛНЫЙ ТЕКСТ РАБОЧЕЙ ТЕТРАДИ ОПУБЛИКОВАН НА ИНТЕРНЕТ-ПОРТАЛЕ РСМД. ВЫ МОЖЕТЕ СКАЧАТЬ ЕЕ И ОСТАВИТЬ СВОЙ КОММЕНТАРИЙ К МАТЕРИАЛУ ПО ПРЯМОЙ ССЫЛКЕ – RussianCouncil.ru/paper15

СОДЕРЖАНИЕ

ПРЕДИСЛОВИЕ

Последние два десятилетия характеризуются устойчивым ростом Всемирной паутины – сети Интернет. Можно заметить, что виртуальный мир все чаще определяет реально происходящие события. Грань между виртуальным и реальным становится все менее четкой.

Если на первых этапах развития Интернета трудно было даже представить, что он станет неотъемлемой частью нашей жизни, то сегодня Интернетом обусловлены самые разные явления и процессы. Мы свободно говорим об электронной торговле, телемедицине, новых средствах коммуникации, включая видеозвонки, онлайн-образование и т.п. Сетевой характер стали приобретать элементы государственного управления, внутриполитической и международной жизни. Получили развитие электронное правительство, электронное голосование по общественно значимым вопросам, цифровая дипломатия. Свое виртуальное представительство – веб-сайты, интернет-порталы – открыло большинство органов власти. Особое значение приобрела активность в виртуальных социальных сетях, направленная на прямое и оперативное формирование общественного мнения о происходящих событиях. Министерства иностранных дел целого ряда государств взяли на вооружение работу на популярных социальных сервисах, таких как *Facebook* и *Twitter*. Ежегодно разнообразие интернет-инструментов увеличивается.

Растет и число возможных интернет-угроз, как для участников и пользователей Всемирной паутины, так и для всей сетевой архитектуры. Принципиальными становятся формирование приоритетов работы в виртуальной среде, выработка стратегии использования сетевых инструментов. Все ведущие государства мира рассматривают эти задачи в качестве приоритетных. И Россия здесь не исключение. Учитывая глобальный характер Интернета, ключевым становится выработка подходов к сетевому позиционированию страны, адекватному использованию сетевых возможностей для защиты и продвижения интересов государства. При этом специального внимания заслуживают вопросы физической защиты объектов, обеспечивающих работу Интернета, и виртуальной защиты критически важной инфраструктуры государств.

На международных форумах и в организациях ООН продолжается интенсивное обсуждение возможностей регулирования Интернета. Вопросы безопасности и степень вмешательства государства в сетевые процессы, а также рост числа негосу-

дарственных участников в интернет-коммуникациях выступают в качестве основных тем в таких дискуссиях. Наибольшие споры вызывают стремление и возможности отдельных государств осуществлять контроль над информационным и медиапространством. Российская Федерация не без оснований предполагает, что это существенным образом влияет на всю архитектуру международной стабильности и поэтому требует взвешенных решений, поддержанных на международном уровне.

Данной публикацией Российский совет по международным делам (РСМД) приглашает специалистов по международным отношениям и информационно-коммуникационным технологиям к обсуждению перспектив и возможностей России для эффективного участия в управлении Интернетом.

В.С. Овчинский, Е.С. Ларина

МИРОВАЯ ЦИФРОВАЯ СРЕДА: ВОЗМОЖНОСТИ И РИСКИ ДЛЯ РОССИИ

Введение

Информационная сфера существует столько же, сколько существует человечество. Менялись лишь средства коммуникации, способы хранения и предоставления информации, уровень ее доступности. Исторической тенденцией развития этой сферы был неизменный рост доступности информационных ресурсов, как для граждан, так и для государств, как для общественных организаций, так и для бизнеса. Одновременно каналы передачи и доступа к информации становились все более разнообразными и оперативными. Наконец, разнообразие и широта информационных каналов, охват ими все большего числа людей постоянно повышают связность мира. Если в доинтернетную эпоху два любых жителя Земли были знакомы через шесть посредников, то сейчас эта цифра уменьшилась уже до четырех и имеет тенденцию к дальнейшему снижению[1].

Киберпространство как таковое появилось в ходе первой промышленной революции с массовым распространением машин и механизмов. В каждой машине был управляющий блок, посредством которого человек приводил в действие силы, во много раз превышающие его физические возможности. «Киберпространство» представляет собой метафору, характеризующую пространство распространения сигналов в любых управляющих системах. Впервые это понятие было введено американским фантастом У. Гибсоном в романе «Нейромант», а затем уже получило распространение среди военных и специалистов информационных технологий.

В течение последних 200 лет киберпространство непрерывно расширялось, а возможность осуществления управления различного рода машинами, механизмами на расстоянии постоянно увеличивалась. Качественный скачок произошел с появлением Интернета и массовым его применением в промышленной, социальной, коммунальной и иных сферах. С этого момента киберпространство практически стало отождествляться с сетью Интернет, другими сетями и телекоммуникациями.

[1] **Теория шести рукопожатий** – теория, согласно которой любые два человека на Земле разделены в среднем лишь пятью уровнями общих знакомых (и, соответственно, шестью уровнями связей). URL: http://www.ru.wikipedia.org/wiki/Теория_шести_рукопожатий

Очевидно, что и информационная сфера, и киберпространство получили принципиально новое качество с появлением Интернета, базирующегося на информационных технологиях и электронно-вычислительной технике. В основе любых вычислений лежат операции с цифрами. Поэтому буквально в последние годы и в официальных выступлениях, и в публикациях, и в терминологии различных профессиональных сообществ, включая политиков, военных, стратегистов и т.п., и в повседневном языке все чаще используется термин «цифровая среда».

Картография цифровой среды

Цифровая среда включает в себя все многообразие информационных технологий и киберпространство. Соответственно, информационная безопасность прямо относится к цифровой среде, но является лишь одним ее аспектом. Точно так же и киберпространство в строгом смысле этого слова представляет собой ту часть цифровой среды, где происходит управление различного рода объектами физического мира посредством использования Интернета, других сетей и телекоммуникационных каналов.

Цифровая среда имеет собственные:

- инфраструктуру. Она включает в себя, во-первых, телекоммуникационные и интернет-линии (оптоволоконные кабели и т.п.), во-вторых, вычислительные комплексы различной размерности – от суперкомпьютеров до смартфонов и планшетных компьютеров – и, в-третьих, вычислительные управляющие встроенные блоки в различного рода объекты физического мира, начиная от производственных линий и заканчивая кроссовками и майками;
- структуру. Она состоит, во-первых, из сетевых программных протоколов, обеспечивающих передачу информации по различным сетям, включая Интернет, корпоративные сети, одноранговые сети (типа Tor) и т.п., во-вторых, программы и программные платформы, осуществляющие хранение, переработку и предоставление информации – от баз данных до привычных всем операционных систем типа Windows, Linux и т.п. – и, наконец, в-третьих, программы-интерфейсы, обеспечивающие восприятие информации конечными пользователями (интерфейсы сайтов, блогов, порталов, приложений, различного рода программ и т.п.);
- ультраструктуру. Она представляет собой инфосферу, где содержатся воспринимаемые человеком прямые и скрытые

смыслы, выраженные в текстах, таблицах, видео- и аудиоконтенте. Ультраструктура включает в себя, во-первых, общедоступные сетевые ресурсы типа сайтов, блогов, порталов, социальных сетей и т.п., во-вторых, защищенные, доступные только для определенных категорий пользователей информационные ресурсы государственной и корпоративной принадлежности, в-третьих, общедоступные ресурсы с платным контентом.

За почти 25-летнюю историю развития общедоступных коммуникационных сетей, с 1991 г., когда к закрытой сети получили возможность подключаться все желающие, сложилось два принципиально различных их типа:

– Интернет, а также внутренние государственные и корпоративные сети, недоступные для сторонних пользователей. Эти сети построены по иерархическому принципу. В сетях существует несколько уровней иерархии, которые аккумулируют и передают информацию. Соответственно, права и возможности регулирования информации на каждом уровне зависят от его положения в иерархии: чем выше уровень, тем больше возможностей и прав.

– так называемые пиринговые или одноранговые сети[2]. Наиболее популярные из них в настоящее время – коммуникационная сеть Tor и платежная сеть Биткойн. В одноранговых сетях информация передается между компьютерами пользователей, которые имеют абсолютно равные права и возможности в передаче информации. В силу этого одноранговые сети работают, как правило, намного более медленно, чем Интернет.

Указанные типы сетей функционируют независимо друг от друга. Соответственно, ресурсы одной сети не обнаруживаются и не находятся поисковыми системами другой сети. При этом в каждой из сетей предусмотрены специальные порталы, которые облегчают пользователям использование ресурсов в другой сети.

Интернет имеет следующую картографию:

• web 1. Это наиболее старый, сложившийся сегмент сети. Он включает в себя правительственные, корпоративные, общественные, персональные порталы, сайты, блоги, онлайн-СМИ. Ресурсы этого сегмента Сети легкодоступны при помощи поисковых систем (типа Google, Yandex и пр.);

• web 2. Это так называемый социальный веб, или веб социальных сетей и платформ. Здесь расположены такие ресурсы, как В Контакте, Facebook, Twitter и пр. Контент в этом

[2] Одноранговая, децентрализованная или пиринговая (от англ. peer-to-peer, P2P – равный к равному) сеть – это оверлейная компьютерная сеть, основанная на равноправии участников.
URL: http://www.ru.wikipedia.org/wiki/ Одноранговая_сеть

сегменте Интернета создается в основном самими пользователями, поэтому он получил название социального веба. Из-за политики собственников платформ и социальных сетей, а также из-за требований приватности они лишь частично видимы для поисковых систем. В этом сегменте ускоренными темпами растет доля видео- и фотоконтента;

• web 3. Этот сегмент Интернета появился в последние два–три года и растет наиболее быстрыми темпами. Это так называемый «веб мобильных приложений». Интерфейсы приложений размещаются на экранах планшетных компьютеров, смартфонов. Соответственно, пользователи работают с приложениями без обращения к поисковым системам, просто устанавливая связь между своим устройством и Интернетом;

• невидимый Интернет. Невидимый Интернет это ресурсы, которые не обнаруживаются поисковыми машинами, а также порталы, сайты и т.д., доступ к которым предполагает либо платный характер, либо наличие специального разрешения на использование ресурсов. По имеющимся данным[3], в невидимом Интернете находится порядка 90% всего ценного научно-технического, технологического, финансово-экономического и государственного открытого контента. Объемы невидимого Интернета постоянно растут. Он развивается более быстрыми темпами, чем web 1 и web 2. Главными причинами опережающих темпов являются, с одной стороны, стремление к архивации всех доступных данных корпоративными пользователями, а с другой желание обладателей ресурсов вывести их из общедоступного пользования в платный сегмент, т.е. монетизировать;

• Интернет вещей. Представляет собой соединенные через Интернет с управляющими центрами встроенные информационные блоки самых различных объектов физического мира, в том числе производственной, социальной, коммунальной инфраструктуры. Так, например, к нему относятся подсоединенные к Всемирной сети технологические линии, системы управления водо- и теплоснабжением и т.п. Буквально в последние год-два обязательным требованием по умолчанию стало подключение к Интернету всех типов домашнего оборудования, бытовой техники, вплоть до холодильников, стиральных машин и т.п.;

• бодинет. Со стремительным развитием микроэлектроники появилась возможность встраивать элементы, передающие информацию в предметы гардероба (кроссовки, майки и т.п.), а также широко использовать микроэлектронику в новом по-

[3] Pierluigi Paganini, Richard Amores. The Deep Dark Web. 2012.

колении медицинской техники, реализующей различного рода имплантаты – от чипов, контролирующих сахар в крови, до искусственного сердца и т.п. Кроме того, тенденцией последних месяцев стало создание распределенного компьютера, который предполагает, что отдельные его элементы распределяются по человеческому телу – фактически человек носит на себе компьютер и взаимодействует с ним круглые сутки[4].

Большую часть одноранговых сетей относят к так называемому «темному вебу» (dark web). Своим названием этот сегмент Сети обязан широкому использованию своих ресурсов различного рода преступными, незаконными группами и группировками. Основными сегментами этого веба являются сеть Tor, созданная в 2002 г. военно-морской разведкой США, и платежная сеть Биткойн. В настоящее время сети используются преимущественно для противоправной деятельности, киберпреступности, торговли наркотиками, оружием и т.п., а также для осуществления целенаправленных акций по подрыву государственного суверенитета.

Особый сегмент сети, частично располагающийся в сети Интернет, частично – в специально созданных одноранговых сетях, составляют так называемые «сети денег». Общемировой тенденцией является сокращение наличного платежного оборота и переход к электронным деньгам во всех их видах. Сеть денег включает в себя специализированные телекоммуникационные расчетные сети, связывающие крупнейшие банки типа SWIFT, а также платежные системы, использующие Интернет, типа PayPal, Яндекс. Деньги и т.п. Отдельным быстро развивающимся сегментом денежных сетей являются специализированные платежные системы, базирующиеся на одноранговых сетях и зашифрованных сообщениях. Наиболее известная из этих систем – это платежная система Биткойн.

Таким образом, цифровая среда имеет сложную картографию, где отдельные сегменты развиваются по собственным, независимым от общих закономерностей трендам. При этом целый ряд основополагающих тенденций являются общими для всех сегментов цифровой среды.

Первой основополагающей тенденцией цифровой среды является информационный взрыв. В последнее время объем информации удваивается каждые два года[5]. По данным компании Cisco, объем сгенерированных данных в 2012 г. соста-

---

[4] Подробнее см.: Ларина Е.С. Встречайте – bodynet! URL: http://www.therunet.com/articles/1877-vstrechayte-bodynet

[5] IDC iView. Big Data, Bigger Digital Shadows, and Biggest Growth in the Far East. URL: http://www.emc.com/leadership/digital-universe/2012iview/big-data-2020.htm

вил 2,8 зеттабайта и увеличится до 40 зеттабайт к 2020 г.[6] Примерно треть передаваемых данных составляют автоматически сгенерированные данные, т.е. управляющие сигналы и информация, характеризующие работу машин, оборудования, устройств, присоединенных к Интернету. На 40% ежегодно растет объем корпоративной информации, передаваемой и хранящейся в сети Интернет.

Число пользователей Интернета в мире к концу 2013 г. составило 2,7 млрд человек, или 39% населения Земли, а к 2016 г. эта доля составит 65–75% населения, по данным Центра новостей ООН[7]. Как ожидается, количество корпоративных пользователей Интернета во всем мире увеличится с 1,6 млрд человек в 2011 г. до 2,3 млрд человек в 2016 г.

Если в 2012 г. более 90% пользователей выходили в Сеть с компьютеров всех типов и лишь 10% – с мобильных устройств, то к 2016 г. доля планшетных компьютеров, смартфонов и других гаджетов увеличится как минимум до 45–50%[8].

Россия входит в число ведущих стран по числу пользователей Интернетом. В настоящее время более 55% населения взаимодействует с Интернетом[9]. В крупных городах им охвачено более 75% населения. Происходящее из года в год снижение стоимости широкополосного доступа в Интернет, переход на новые стандарты мобильной связи, обеспечение доступа в Интернет жителям ранее не охваченных им районов страны открывают принципиально новые возможности для экономического, общественного и социального развития.

Прежде всего появляются возможности для создания общегосударственной и корпоративных систем непрерывного дистанционного образования и целевого формирования компетенций по наиболее востребованным, в том числе ранее не существовавшим профессиям и специальностям. Не меньшие возможности открываются перед интернет-медициной, которая в последние несколько лет получила широчайшее распространение в США, Западной Европе, ряде других стран. При этом следует отметить, что в России еще в конце 1990-х – начале 2000-х годов в системе РЖД была создана охватывающая всю территорию страны система интернет-медицины, которая

---

[6] Cisco Visual Networking Index: Global Data Traffic Forecast Update, 2013–2020. URL: http://www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/white-paper-listing.html

[7] В мире наблюдается стремительный рост числа подписчиков на Интернет и мобильную связь // Центр новостей ООН. URL: http://www.un.org/russian/news/story.asp?NewsID=20390#.U00YSvl_uSo;
Отчет Международного союза электросвязи «Измерение информационного общества». 2013. URL: http://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2013/MIS2013-exec-sum_R.pdf

[8] Доклад «Мобильный интернет в России и мире: платформы, потребление, тенденции», представленный Nielsen и Mail.Ru Group. URL: http://www.corp.mail.ru/blog/mobileinternet

[9] Интернет в России: динамика проникновения. Осень 2013, ФОМ. URL: http://www.fom.ru/SMI-i-internet/11288

с учетом новых технологических возможностей может быть использована как в общегосударственном масштабе, так и в масштабе отдельных регионов либо крупных корпораций.

Огромные возможности имеются у российской интернет-коммерции (компаний – резидентов РФ, ведущих коммерческую деятельность в Интернете). По своим объемам она занимает 13-е место в мире[10]. Но по темпам роста она первенствует в Европе. Ключевым вопросом для устойчивого роста интернет-торговли является опережающее развитие безналичного платежного оборота в виде электронных платежей по кредитным картам и т.п. Развитию российской интернет-коммерции будут способствовать также соответствующие международному законодательству меры по недопущению демпинга со стороны внешних рынков электронной коммерции. Подобные меры в настоящее время действуют в Германии, Великобритании, других странах.

Защита «цифрового суверенитета»

Исторически Интернет формировался как свободная среда информационного взаимодействия при неформальном, но реализованном через жесткие технологические программные и организационные способы контроле со стороны Соединенных Штатов Америки – страны-создателя Всемирной паутины. В результате к настоящему времени сложилось парадоксальное положение. В Интернет в значительной степени переместились торговля, финансовые операции, политическая и социальная активность, т.е. ключевые сферы жизнедеятельности каждого государства. Между тем в Интернете, в отличие от физической реальности, не признаны поствестфальские принципы международного права. Безусловно, обеспечение «цифрового суверенитета», совместное международное управление Интернетом и распространение принципов поствестфальской международной системы на Интернет с учетом его особенностей являются важными направлениями внешнеполитической активности России и все большего числа стран, придерживающихся сходных взглядов на принципы международно-правового регулирования Интернета.

Второй важнейшей тенденцией изменения цифровой среды становится формирование Интернета вещей. Интернет вещей – это самые разнообразные технологические, произ-

[10] Россия заняла 13 строчку в мировом рейтинге онлайн-торговли. URL: http://www.cnews.ru/top/2013/11/19/rossiya_zanyala_13_strochku_v_mirovom_reytinge_onlayntorgovli_550401?goback=.gde_135696_member_5808972659395956737

водственные, инфраструктурные устройства, приборы, приспособления и т.п., имеющие блоки контроля, передачи информации и управления, соединенные с Интернетом. В настоящее время к Интернету уже подключено более 17 млрд устройств[11].

Согласно сделанному IDS прогнозу, к Интернету вещей к 2020 г. будет подключено 212 млрд устройств, а денежная емкость этого рынка составит 8,9 трлн долларов. Причем в Интернете вещей образца 2020 г. окажется 30,1 млрд автономных устройств, от автомобилей до пылесосов[12].

Развитие Интернета вещей открывает поистине безграничные перспективы и возможности для российской и мировой экономики. Анализ данных, поступающих от соединенных с Интернетом инфраструктурных объектов, позволяет, как показывает мировой опыт, на 20–30% сократить время, проводимое на перегруженных автомобильных трассах, более чем на 15% сократить непроизводительные расходы воды и электроэнергии в жилых и производственных зданиях и т.п.[13] Как свидетельствует опыт Финляндии и Норвегии, использование технологии «умных домов» и «умных кварталов», предусматривающей в том числе подсоединение к Интернету системы как поквартирного, так и централизованного тепло- и энергоснабжения, позволяет на 12–17% уменьшить расходы на отопление при сохранении неизменной температуры в жилых помещениях[14]. Понятно, что в условиях нашей страны использование Интернета вещей в подобных сферах даст еще более впечатляющий эффект. Этот эффект может быть связан, во-первых, с природно-климатическими особенностями нашей страны, во-вторых, со значительным отставанием реализации программ экономии различных, в том числе коммунальных ресурсов и, в-третьих, с достаточным и все возрастающим количеством мегаполисов и агломераций, где он проявляется наиболее сильно и масштабно.

Как правило, угрозы, связанные с Интернетом вещей, сводят к различным видам киберпреступности и даже к кибертерроризму. Понятно, что в условиях, когда вся инфраструктура населенных центров, отдельных жилых кварталов, домов и просто жизнедеятельности каждого человека полностью завя-

---

[11] The Internet of Everything: Business Models and Scenarios. Gartner, 2013. URL: http://www.gartner.com/newsroom/id/2621015

[12] Worldwide Internet of Things (IoT) 2013–2020 Forecast: Billions of Things, Trillions of Dollars. IDC, 2013. URL: http://www.idc.com/getdoc.jsp?containerId=243661

[13] Worldwide Internet of Things (IoT) 2013–2020 Forecast: Billions of Things, Trillions of Dollars IDC, 2013. URL: http://www.idc.com/getdoc.jsp?containerId=243661

[14] The Internet of Everything: Business Models and Scenarios. Gartner, 2013. URL: http:// www.my.gartner.com/portal/server.pt?open=512&objID=202&mode=2&PageID=5553&showOriginalFeature=y&resId=2610121&fnl=search&srcId=1–3478922244

зана на Интернет вещей, злонамеренное вторжение в Интернет вещей может привести к трудно предсказуемым последствиям. Поэтому первостепенной задачей государств с высоким уровнем интернетизации населения и доходов, позволяющих приобретать предметы со встроенным Интернетом, становится налаживание теснейшего международного сотрудничества по борьбе с киберпреступностью и кибертерроризмом. Причем уже сегодня ясно, что это сотрудничество не должно ограничиваться принятием соответствующих юридических актов, но и должно предполагать каждодневный обмен информацией и эффективным инструментарием борьбы против киберпреступности и кибертерроризма. Более того, заслуживает внимания предложение о создании объединенных добровольных международных сил по противодействию трансграничным киберпреступным и кибертеррористическим группировкам. Россия, располагающая первоклассными специалистами и имеющая целый ряд компаний-резидентов[15], являющихся лидерами в сфере индивидуальной и корпоративной информационной безопасности, несомненно, может сыграть в этой работе заметную роль.

Существует еще одна в должной мере неосознаваемая угроза цифровому суверенитету России, связанная с Интернетом вещей. В настоящее время поисковые системы и платформы социальных сетей, такие как Facebook, Twitter и др., позволяют анализировать поведение пользователей, объединяемых в самые различные группы, их предпочтения, активность, связи и т.п. С появлением Интернета вещей такой мониторинг в режиме онлайн может вестись уже не в отношении интернет-активности, а в отношении реальной жизнедеятельности населения, функционирования предприятий, организации работы городских и иных структур. Дело в том, что в рамках Интернета вещей информация передается в компании-производители изделий, соединенные с Интернетом, либо в компании-поставщики микропроцессоров. Соответственно, именно в этих компаниях – наряду с индивидуальными, корпоративными или государственными пользователями систем, оснащенных Интернетом вещей, – оказывается полная информация о реальном мире в режиме онлайн. Именно поэтому буквально в последние месяцы ведущие интернет-компании, например Google, начали заключать сделки ценой от сотен до миллиардов долларов по приобретению компаний, связанных с Интернетом вещей. Этой угрозы можно избежать двумя способами. Радикально:

[15] С деятельностью ряда из них можно ознакомиться на сайте SecurityLab. URL: http://www.securitylab.ru

развив собственную микроэлектронную промышленность, производящую чипы для приборов, оборудования и систем, подсоединенных к Интернету вещей. Паллиативно: установив в качестве обязательного условия для продажи на территории России предметов, оборудования и устройств, подключенных к Интернету, наличие на территории России и подпадающих под ее юрисдикцию центров обработки данных (ЦОД) соответствующей компании.

Буквально на наших глазах рождается нательный, носимый Интернет, или, как его еще называют, бодинет. Этот фрагмент Сети складывается из трех сегментов. Прежде всего появились уже первые предвестники эры распределенных компьютеров типа очков Google Glass. Вторым сегментом являются предметы гардероба, т.е. повседневная одежда, обувь и т.п., соединенная с Интернетом и контролирующая, как правило, состояние здоровья или иных параметров обладателя гардероба. Наконец, наиболее активно в перспективе будет развиваться сегмент, связанный с электронными компонентами микроустройств и микроприспособлений, непосредственно имплантированных в тело человека. Так, на сегодняшний день уже около миллиона американцев имеют медицинские имплантаты, подсоединенные к Интернету и в основном связанные с кардиоконтролем, а также с контролем уровня сахара в крови. Ежегодно цена на такого рода имплантаты падает не на проценты, а в разы. Также по экспоненте увеличивается количество такого рода имплантатов, в значительной мере порожденных достижениями биотехнологий и микроматериаловедения[16]. Есть основания полагать, что в ближайшие 5–7 лет встроенные в человеческое тело имплантаты, соединенные с Интернетом, из экзотики превратятся в обыденность практически во всех развитых странах мира.

При общем отставании в лечебном, в том числе в коммерческом использовании такого рода имплантатов российские исследователи имеют целый ряд впечатляющих разработок и в целом входят в число мировых лидеров в сфере медицинских кибертехнологий. Соответственно, при должной организации взаимодействия частного бизнеса и государства в этой сфере отечественный высокотехнологичный бизнес не только может сохранить за собой значительную долю внутреннего рынка, но и имеет хорошие шансы выдержать конкуренцию в отдельных сегментах глобального рынка высоких медицинских интернет-технологий.

[16] Nanomedicine – Healthcare in the 21st Century. Cleveland clinic, 2013.

Широкое распространение бодинета порождает принципиально новые типы угроз, связанные с возможностью осуществления киберпреступлений, вплоть до нанесения тяжелых телесных повреждений и убийств, а также целевого точечного кибертерроризма. В Соединенных Штатах данная угроза рассматривается как актуальная, на государственном уровне и на уровне частных компаний разрабатываются конкретные меры по противодействию ей. Принимая во внимание признанную во всем мире высочайшую квалификацию российских специалистов в сфере тестирования на несанкционированное проникновение (этичные хакеры), есть отличный шанс превратить угрозу в возможность для российского бизнеса и опосредованно для Российского государства. Для реализации этой возможности надо в кратчайшие сроки выступить с российской частно-государственной инициативой на международной арене по созданию единого пула производителей медицинских имплантатов, микроэлектронной техники и компаний в сфере информационной безопасности и тестирования несанкционированного проникновения. Такой пул может в перспективе стать надежным щитом для массовой киберпреступности, связанной со злонамеренным вмешательством в работу имплантатов, соединенных с Интернетом.

Цифровая среда и третья производственная революция

Ключевым процессом, меняющим производственный базис, системы экономических отношений, сложившееся международное разделение труда, воздействующим на мировые финансы и политические системы, является разворачивающаяся третья производственная революция. В ее основе лежит тотальное вторжение цифровых технологий в основы производственной деятельности. Еще с начала нулевых годов информационные технологии активно применялись в бизнесе, прежде всего в виде так называемой бизнес-аналитики и иных информационных бизнес-решений. Однако до некоторого времени информационные технологии имели отношение лишь к управленческим процессам.

В последние несколько лет ситуация коренным образом изменилась в связи с массовым внедрением робототехники, автоматизированных линий и экспансии в самые различные производственные сферы 3D-печати.

Уже сейчас в США действует или готовится к пуску в ближайшие годы более 9 тыс. полностью автоматизированных

производств. В настоящее время безусловным лидером по производству высокотехнологичных промышленных роботов являются Соединенные Штаты Америки. В этом году на предприятия США поставлено чуть менее 20 тыс. единиц высокотехнологичных антропоморфных роботов.

Ради справедливости надо сказать, что США не являются лидером по уже установленным промышленным роботам. Первое место уверенно держит Япония. Второе место занимает Китай. И лишь на третьем месте – Соединенные Штаты. Лидирующую пятерку замыкают Южная Корея и Германия[17]. При этом, по оценкам специалистов, китайские роботы менее технологичны и применяются в основном на элементарных сборочных работах, связанных с выпуском традиционных устройств и бытовой техники.

В целом, по оценкам различных источников, наиболее массовое применение робототехники в ближайшие годы будет иметь место в США, Южной Корее и Японии. Уже сейчас начат массовый выпуск роботов, применение которых более экономично, чем использование не только квалифицированных, но и низкоквалифицированных конвейерных рабочих. Все без исключения автоматические и роботизированные линии и отдельные промышленные роботы завязаны не только на корпоративные сети, но и на Интернет.

Наряду с робототехникой ключевым направлением третьей производственной революции является 3D-печать. В основе 3D-печати лежит технология под названием Additive Manufacturing, т.е. аддитивное (точнее «поэтапное») изготовление. 3D-принтеры не наносят на бумагу краску, а «выращивают» объект из пластмассы, металла или других материалов.

Если на первом этапе 3D-принтеры использовались в основном в дизайне, то в настоящее время 3D-технологии берутся на вооружение в самых различных сферах – от изготовления мебели и одежды до высокотехнологичных отраслей промышленности. В текущем году произошел прорыв в области промышленного использования 3D-печати крупнейшими корпорациями. Линии 3D-печати в настоящее время строят Boeing, Samsung, Siemens, Canon, General Electric и т.п. В результате к концу 2013 г. мировой рынок продажи 3D-принтеров оценивался от 3 до 3,5 млрд долларов и в среднем удваивается в течение полутора лет, т.е. растет по экспоненте.

Бесспорным лидером как в производстве 3D-принтеров, так и в их использовании являются Соединенные Штаты. На них

[17] Хороший год для роботов. URL: http://www.computerra.ru/90864/horoshiy-god-dlya-robotov

приходится почти 40% мирового производства 3D-принтеров. Около 10% – доля Японии. Практически столько же приходится на Германию и Китай. Пятерку лидеров с 6% замыкает Великобритания. Россия в сфере промышленного применения 3D-принтеров занимает десятое место[18].

3D-печать, так же как робототехника, полностью завязана на информационные технологии. Подавляющая часть 3D-фабрик подключена к Интернету и использует удаленные системы хранения информации, а также вычислений, необходимых для бесперебойной работы принтеров.

Третья производственная революция меняет лицо индустрии. Процесс этот высокодинамичный. В этой связи у России имеются большие шансы максимально использовать возможности технологий третьей производственной революции. Массовое применение подобных технологий в США, Европе и Китае зачастую сдерживается фактором неизбежного снижения капитализации уже имеющихся производственных мощностей. Эти мощности находятся в работоспособном состоянии, имеют малые сроки эксплуатации, под них отлажена логистика, системы маркетинга и продаж. В то же время в Российской Федерации производственный потенциал характеризуется высоким уровнем износа, наличием значительного числа машин, оборудования, технологических линий с запредельными сроками эксплуатации. Соответственно, для российской промышленности нет препятствий для внедрения наиболее прогрессивных технологий. Кроме того, технологии третьей производственной революции полностью погружены в цифровую среду и предполагают высокий уровень профессиональной подготовки программистов, разработчиков и эксплуатантов оборудования. Как раз по этим специальностям Россия весьма конкурентоспособна на мировой арене и имеет достаточное число специалистов в области информационных наук, включая математиков, когнитивных лингвистов, разработчиков, программистов и т.п. Что касается эксплуатантов, то в России имеются отлаженные методы их подготовки и переподготовки.

Наиболее явной угрозой со стороны третьей производственной революции для России является то, что две прошлые революции в сфере информационных наук – микроэлементную революцию и интернет-революцию – Россия пропустила и в итоге откатилась в сфере науки и технологий с передовых позиций в ранг стран догоняющего развития. По сути, угроза состоит в том, чтобы не пропустить третью производственную револю-

[18] World 3D Printing (Additive Manufacturing). Date Published: Dec-2013 Fredonia group. URL: http://www.freedoniagroup.com/brochure/31xx/3123smwe.pdf

цию. Преодоление этой угрозы связано, с одной стороны, с совместными усилиями государства и бизнеса, а с другой стороны, с максимально широким международным сотрудничеством. Оно может выражаться в самых различных формах и включать в себя не только приглашение профессоров, ведущих технологов, конструкторов и т.п., но и в целевой покупке небольших передовых венчурных фирм-производителей робототехники, промышленных 3D-принтеров и т.п. Таких фирм, обладающих передовыми технологиями, за рубежом значительное количество. Они испытывают большую нехватку капитала. У них ограничены возможности для маркетинга и формирования рынков сбыта своей продукции в условиях острой конкуренции на североамериканском, европейском и азиатском рынках. В этой связи есть большое поле, чтобы использовать не только российский, но и зарубежный научно-технический потенциал для того, чтобы уже на ранних этапах третьей производственной революции Россия могла занять лидирующее место.

Отличительной чертой нашего времени является включение в цифровую среду практически всех направлений науки и техники, в том числе и науки о живом. В последние 10 лет стремительно нарастают процессы своего рода соединения кластера информационных наук и технологий с науками о жизни и биотехнологиями. Уже сформировалась биоинформатика и ее многочисленные практические применения. В общем они получили названия генно-информационной инженерии и производственных биотехнологий и т.п. Наиболее ярким проявлением производственных биотехнологий является индустрия индивидуализированных лекарств, на которые делают ставку и фармацевтические гиганты, и новые, молодые, быстроразвивающиеся в этой сфере компании. Сюда же относятся различные виды регенеративной медицины. Широко используются возможности 3D-печати для производства донорских органов. Сегодня это уже не фантастика, а прошедшая клинические испытания обыденность, которую взяли на вооружение, например, медицинские учреждения Франции, Германии, Соединенных Штатов и т.п.

Особым направлением является синтетическая биология. Она позволяет производить новые виды бактерий и живых организмов прямо из компьютера, используя специальные растворы и программные коды, транслируемые компьютером в питательную среду.

Ежегодно не на проценты, а в разы удешевляется оборудование для так называемого компьютерного обследование генома. Если еще 5–7 лет назад такие исследования стоили де-

сятки тысяч долларов, а оборудование – миллионы долларов, то в настоящее время работы ведут сотни компаний по всему миру, а цена оборудования снизилась на порядки. Технология компьютерного исследования генома открывает поистине необозримые возможности для генной инженерии и принципиально новых видов медицины.

Возможности России в сфере биоинформатики и биотехнологий определяются значительными и по некоторым сегментам прорывными разработками, имеющими долгую историю. Нельзя не отметить, что вплоть до 1991 г. советская микробиология и биоинженерия занимали лидирующие позиции в мире. По оценкам американских экспертов, например М. Секоры, основателя проекта «Сократос»[19], благодаря существованию специализированного российского комитета – Главмикробиопрома – с большой сетью подведомственных научно-исследовательских и производственных центров и учебных институтов Советский Союз заметно опережал все другие страны мира во многих направлениях биотехнологий и генной инженерии. Однако затем, в условиях международных мер по ликвидации биологического оружия, а также деградации высокотехнологичных отраслей отечественной промышленности, особенно в 1990-е годы, значительная доля потенциала оказалась утерянной. Хотя при должной мобилизации сил Россия может, базируясь на имеющихся разработках и достижениях, действующих научных школах, диаспоре российских биотехнологов, работающих за рубежом, наверстать упущенное.

Неконтролируемое развитие биоинформатики и генной инженерии по своим разрушительным последствиям потенциально может превзойти ущерб от применения атомного оружия. При этом если для ядерного оружия отработаны политические, правовые и технологические инструменты контроля его распространения и недопущения попадания подобного оружия в руки террористических групп, то подобный инструментарий для биотехнологий отсутствует. По оценкам многих экспертов, в ближайшие три–пять лет это будет представлять самую большую угрозу как для России, так и для мирового сообщества в целом. Эта угроза резко возрастает в ситуации, когда уже сегодняшние достижения в биоинформатике позволяют создавать кибербиооружие направленного действия, т.е. поражающее группы людей с определенными генетическими маркерами. В этой связи первоочередной задачей является выдвижение,

[19] Подробнее об этом см.: Ervin Ackman. President Reagan's Program to Secure U.S. Leadership Indefinitely: Project Socrates. URL: http://www.amazon.com/President-Reagans-Program-Leadership-Indefinitely-ebook/dp/B00G1RJWXW

а главное, реализация многосторонних инициатив по организации международного сотрудничества как на государственном уровне, так и на уровне общественных организаций и фондов, подкрепленных ресурсами ведущих университетов и корпораций по превентивному предупреждению разработки кибервооружений либо биотехнологии двойного назначения. Острота проблемы такова, что серьезный эффект могут дать не только меры, осуществляемые после подписания соответствующих многосторонних соглашений и выработки правового режима борьбы с кибербиотерроризмом, но и меры, осуществляемые в рамках законодательства отдельных стран, проводимые на основе прямых связей между научными, технологическими и коммерческими структурами различных стран.

Набирающей не только из года в год, но и из месяца в месяц тенденцией преобразования цифровой среды является появление, развитие и проникновение в самые различные сферы бизнеса, политики и повседневной жизни компьютерных экспертных систем. За последние два-три года Соединенным Штатам и частично Великобритании удалось осуществить подлинный прорыв в области создания экспертных систем. Эти экспертные системы реализуют принципы программирования, вдохновленные примером биологических систем, имитирующих сеть нейронов. Наиболее известной экспертной системой стал знаменитый компьютер Watson корпорации IBM, победивший во вполне человеческой игре «Своя игра». После победы на игровом поле Watson показал высокие результаты как экспертная система в медицинской онкологии, фармацевтике, полицейских расследованиях, биржевом деле. По оценкам различных экспертов[20], в ближайшие 7–12 лет он может вытеснить до 70% работников, занимающихся рутинным умственным трудом в самых различных сферах деятельности. Экспертные системы дают их обладателям и пользователям огромную интеллектуальную мощь, ставя себе на службу богатства человеческого знания, помноженного на мощь вычислительных алгоритмов. При этом надо отметить, что IBM уже не является монополистом. Об активной работе в этом направлении объявили Google, Facebook, Amazon.com и др.

В России существует мощная школа программистов, компьютерных лингвистов, математиков, работающих в сфере экспертных систем. Создание первых работающих экспертных систем

[20] Подробнее об этом см.: Brynjolfsson E., McAfee A. Race Against The Machine: How the Digital Revolution is Accelerating Innovation, Driving Productivity, and Irreversibly Transforming Employment and the Economy. URL: http://www.amazon.com/Race-Against-Machine-Accelerating-Productivity-ebook/dp/B005WTR4ZI/ref=sr_1_3?s=digital-text&ie=UTF8&qid=1396004715&sr=1–3&keywords=machine+against

в СССР датируется еще концом 1980-х годов. Известно, что значительная часть специалистов по ядру экспертных систем – алгоритмам обработки естественного языка – покинули СССР, а затем Россию и работают на ведущие зарубежные компании.

С учетом того, что российская математическая и лингвистическая школы остаются одними из ведущих в мире, а профессионалы в этой сфере являются востребованными в ведущих транснациональных компаниях и государственных ведомствах, у России есть потенциальные возможности наверстать явно имеющееся на сегодняшний день отставание в сфере создания работоспособных экспертных систем, широко применяемых в самых различных сферах жизнедеятельности. Однако для того, чтобы потенциальную возможность превратить в реальность и в обозримо короткие сроки создать экспертные системы, необходимы целевые государственные программы в этой сфере. Причем для осуществления подобных программ решающую роль играют не только и не столько деньги, сколько возможность объединить в коллектив распределенных по разным компаниям, учебным заведениям, в том числе за рубежом, специалистов и создать для них комфортные условия и нацелить на реализацию проекта.

При этом необходимо отметить, что сохранение, а тем более углубление отставания России в сфере интеллектуальных экспертных систем может быть смело отнесено к числу важнейших национальных угроз. Без внедрения мощных и доступных экспертных систем, способных взаимодействовать с конечным пользователем на естественном, т.е. на человеческом языке и имеющих мощнейшее вычислительное ядро, в ближайшие 5–7 лет у страны могут возникнуть проблемы буквально во всех сферах. Прежде всего отсутствие таких систем может негативно сказаться на поддержании необходимого уровня обороноспособности страны, проработанности сложных политических решений и привести к системному ослаблению конкурентоспособности российского бизнеса.

Цифровая среда и экспансия больших данных

Едва ли не определяющим фактором динамики цифровой среды на ближайшее время станет повсеместная экспансия больших данных. Сам по себе термин «большие данные» появился пять лет назад после публикации специального выпуска журнала Nature в 2008 г.[21] С тех пор направление больших

[21] Выпуск журнала Nature, посвященный большим данным. URL: http://www.nature.com/nature/journal/v455/n7209/index.html

данных стало ведущим в сфере информационных технологий. Парадокс состоит в том, что строгого определения больших данных до сих пор не существует. Однако всем, кто занят большими данными, интуитивно понятно, что большие данные подразумевают:

- во-первых, огромные массивы разнородной информации о процессах, явлениях, событиях, различного рода объектах и т.п., пополняемые непрерывно в режиме онлайн. Согласно имеющейся статистике, 60% этой информации носит неструктурированный, в основном текстовой характер и 40% составляет структурированная, или табличная, информация[22];
- во-вторых, специально спроектированные программные платформы, где большие данные любого объема могут храниться в удобном для вычислений виде;
- в-третьих, наличие различного рода математического, прежде всего статистического инструментария для обработки больших данных и получения результатов в виде, понятном для человека.

На крупнейшей конференции по большим данным[23] было озвучено, что не более 0,6% всей имеющейся сейчас информации накапливается, хранится и перерабатывается, т.е. подпадает под категорию больших данных. Там же были приведены цифры, что потенциально в качестве больших данных может использоваться 23% всей хранимой в настоящее время информации. То есть фактически сейчас из всей этой информации используется как большие данные, т.е. обрабатывается и анализируется, чуть больше 3%. Между тем последние достижения в области создания платформ накопления, хранения и обработки объемов данных всех форматов позволяют увеличить потенциальные большие данные с 23% до примерно 40% всей передаваемой в сетях информации.

Еще в 2011 г. McKinsey Global Institute объявил[24] большие данные «следующим рубежом для инноваций, конкуренции и производительности». Уже сегодня большие данные дают заметный эффект в бизнесе. Например, выяснилось, что в транснациональных компаниях, входящих в список Fortune 500, где, казалось бы, до мелочей отлажены все процедуры и процессы, внедрение технологий больших данных на 5–7% увеличило эффективность использования ресурсов – труда, основных про-

[22] Survey Analysis: Big Data Adoption in 2013 Shows Substance Behind the Hype, Gartner. URL: https://www.gartner.com/doc/2589121/survey-analysis-big-data-adoption

[23] Predictive Analytics World. London, October 23–24, 2013. URL: http://www.predictiveanalyticsworld.com

[24] Big data: The next frontier for innovation, competition, and productivity. URL: http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation

изводственных фондов, энергии и т.п. – и на 7–9% увеличило объемы продаж. Для среднего бизнеса показатели оказались в полтора-два раза выше. Причем следует отметить, что данные получены в условиях, когда мировая экономика испытывает на себе последствия глубочайшего финансово-экономического кризиса и экономический рост измеряется в лучшем случае 1–2%[25].

В 2011–2013 гг. в Великобритании и США осуществляются государственные инициативы, связанные с косвенным стимулированием населения к принятию рациональных, по мнению правительств, решений на основе объединения технологий больших данных и поведенческой экономики и политики[26].

На чем же базируется эффективность больших данных? Технологии больших данных, и прежде всего методы статистического анализа, компьютерного распознавания образов и т.п., применяемые на огромных, постоянно пополняемых массивах данных, позволяют:

- проводить самые различные и сколь угодно подробные классификации той или иной совокупности людей, компаний, иных объектов по самым разнообразным признакам. Такие классификации обеспечивают точное понимание взаимосвязи тех или иных характеристик любого объекта – от человека до компании или организации – с теми или иными его действиями;
- осуществлять многомерный статистический и иной математический анализ. Этот анализ позволяет находить корреляции между самыми различными параметрами, характеристиками, событиями и т.п. Корреляции не отвечают на вопрос «почему?». Они показывают вероятность, с которой при изменении одного фактора изменяется и другой. В каком-то смысле большие данные представляют собой альтернативный традиционной науке метод. Наука на основе теоретических моделей отвечает на вопрос «почему?», а затем, получив ответ, делает рекомендации, как действовать. В случае корреляции стадия поиска причины ликвидируется, а действие происходит в тех случаях, когда факторы тесно взаимосвязаны и на один из факторов легко или возможно осуществить целенаправленное воздействие;
- прогнозировать. На основе классификаций и аналитических выкладок осуществляется прогнозирование. Суть прогнозирования состоит в том, чтобы на основе корреляции опреде-

[25] Cisco Connected World Technology Report. URL: http://www.cisco.com/c/en/us/solutions/enterprise/connected-world-technology-report/index.html

[26] Подробнее об этом см.: Sunstein C.R. Why Nudge?: The Politics of Libertarian Paternalism. Yale University Press, 2014. URL: http://www.amazon.com/Why-Nudge-Politics-Libertarian-Paternalism/dp/0300197861/ref=pd_sim_b_17?ie=UTF8&refRID=043MRV8BETG3ZVZ55RZA

лить наиболее легкий способ воздействия для того, чтобы один набор факторов, характеризующих тот или иной объект, лицо, компанию, событие и т.п., был преобразован в другой.

Большие данные в первую очередь были использованы в маркетинге, инвестиционном бизнесе, в продажах и т.п. То есть фактически там, где речь идет о косвенном, незаметном управлении поведением. Другой сферой применения больших данных стали процессы, описываемые множеством параметров, где за счет изменения режима можно получить экономию того или иного ресурса. В этой связи за пределами маркетинга и продаж самыми активными пользователями больших данных стали государственные учреждения и энергетический сектор экономики.

В ходе опросов топ-менеджеры крупнейших корпораций говорят о том, что они используют большие данные, но фактически они применяют стандартные платформы бизнес-аналитики, которые не позволяют осуществлять многомерные классификации и качественное прогнозирование, удовлетворяясь, как правило, аналитической функцией. Кроме того, у подавляющего числа российских компаний просто нет огромных массовых данных, пополняемых в режиме онлайн. Также у нас в стране, по сути, отсутствуют коммерческие брокеры больших данных, активно действующие прежде всего в США и Японии. Речь идет о компаниях, покупающих, собирающих, хранящих и продающих обезличенные большие данные.

В то же время у России есть все необходимые предпосылки для совершения подлинного рывка в сфере больших данных. Поскольку ключевые программные решения для платформ хранения и обработки больших данных относятся к открытому и свободному софту и принимая во внимание мощнейший российский потенциал в сфере статистики, математики и программирования, у России есть все возможности максимально задействовать потенциал технологий больших данных во всех сферах: от государственного управления до обеспечения текущей человеческой жизнедеятельности. Не говоря уже о бизнесе.

Для этого необходимо, чтобы государство через имеющиеся у него венчурные организации, такие как Фонд развития интернет-инициатив, «Сколково», «Роснано», целенаправленно финансировало разработчиков платформ больших данных, ориентированных на конкретные сферы – от обороноспособности до малого бизнеса. Для сравнения: в США в прошлом году только через государственные каналы было профинансировано около 80 стартапов в области больших данных, а всего в конкурсе на лучший международный стартап в области боль-

ших данных из США участвовало более 300 стартапов[27]. В России на сегодняшний день, как отмечают эксперты, существует менее 10 стратапов в сфере больших данных, хоть в какой-то степени соответствующих международному уровню[28].

Если в течение ближайших 2–3 лет ситуация в сфере разработки национальных платформ и сервисов по работе с большими данными, ориентированными на разные сегменты жизни государства, различные сферы экономики, на бизнес всех размеров – от транснациональных компаний до малого бизнеса, коренным образом не изменится, то для нашей страны возникнет целый ряд угроз.

Едва ли не самой наглядной из них станет утрата российским бизнесом достигнутого уровня конкурентоспособности. Ориентировка на зарубежные платформы в данной ситуации не спасает положения, поскольку, как показывают события последнего года, использование зарубежных сервисов, программных решений и т.п. чревато утечками данных, включая прямой промышленный шпионаж.

Гораздо более серьезной является потенциальная угроза применения в отношении нашей страны и социума технологий больших данных в соединении с инструментальной реализацией достижений поведенческих наук. Как указывалось выше, в настоящее время подобные технологии апробируются в Великобритании и США. Надо понимать, что большие данные родились в значительной мере в секторе маркетинга и продаж и были ориентированы на целенаправленное управление групповым поведением. Соответственно, продвинутые решения на основе соединения больших данных и поведенческих технологий открывают поистине безграничные возможности для необнаруживаемого эффективного дистанционного управления поведением больших групп населения. Это управление может осуществляться в самых различных сферах, начиная от подталкивания к потреблению тех или иных товаров и услуг и заканчивая дистанционным манипулированием электоральным поведением. Большие данные являются типичной технологией двойного назначения, и в этой связи важно не только иметь эффективные российские решения, но и своевременно выступить с инициативами в международных организациях по законодательному запрещению трансграничного применения инструментальных решений, базирующихся на соединении достижений технологий больших данных и поведенческих наук.

[27] Приведены данные авторов статьи.
[28] Приведены данные авторов статьи.

* * *

Цифровая среда динамично, пластично и не всегда прогнозируемо меняется. Эти изменения происходят в момент развертывания третьей производственной революции. Более того, цифровая среда трансформируется в условиях нарастающей неопределенности глобальных финансово-экономических, политических, военных и социальных процессов. Все эти обстоятельства накладываются на постоянно растущую сложность человеческой цивилизации и усиление сетевой взаимозависимости всех ее компонентов – начиная от государств и заканчивая отдельными группами людей. В этих условиях любые конфликты вне зависимости от их природы и исходных порождающих факторов чреваты непредсказуемой динамикой развития, склонностью к лавинно нарастающей эскалации и сокращающимися возможностями для своевременного урегулирования. В подобных условиях, как никогда ранее в истории, важна философия, а главное – практика международного многостороннего сотрудничества. Она должна обеспечивать предупреждение возникновения новых очагов конфронтации, а также пресекать попытки получения какой-либо из частей единого, но разнообразного, состоящего из множества действующих независимых субъектов мира односторонних преимуществ.

С.А. Кулик

СЕТЕВЫЕ ИНСТРУМЕНТЫ И ВНЕШНЯЯ ПОЛИТИКА: К ПОВЕСТКЕ ОБСУЖДЕНИЯ

Быстрое развитие сетевых инструментов (информационно-коммуникационные технологии (ИКТ), социальные сети, блогосфера) все заметнее отражается на ходе глобальных и региональных процессов и тем самым влияет на ранжирование проблемных повесток международного сообщества и государств. Это обусловливает растущее воздействие на государственные службы, вовлеченные во внешние дела.

Тема «Сетевые инструменты и внешняя политика» в довольно живом темпе усложняется и выходит за рамки устоявшихся шаблонов в размышлениях политиков и экспертов. Впереди скорее всего новые вопросы и неожиданности. Вместе с тем она уже увеличивает нагрузку на внешнеполитические ведомства, расширяет поле их деятельности. Это заставляет по меньшей мере поскорее и внимательнее задуматься над этой темой в приоритетах российской международной деятельности и над целесообразностью постепенной и адекватной перенастройки последней, не исключая организационные вопросы. Государственным структурам стоит четко поставить перед собой задачу оживить экспертное сообщество и активизировать взаимодействие с ним.

Нужно объединять интеллектуальные ресурсы на междисциплинарной основе («технари», правоведы, специалисты по «мягкой силе» и др.). Сейчас они заметно разрознены. Без понятного прописывания значения сетевых инструментов (СИ) хотя бы для политики «мягкой силы» «государственное задание» больше ориентирует их на технологические вопросы безопасности ИКТ, защиту от внешнего воздействия или регулирование Интернета. При всей важности этих вопросов за ними можно не увидеть «леса» проблем и вызовов, нарастающих на международной сцене и для России, и для других ведущих государств. К тому же нелишне учитывать, что над дисциплинарными состыковками серьезно и весьма последовательно работают наши крупные зарубежные партнеры.

При разборе возможностей, возникающих с приобретением СИ, очевидное предпочтение (не только у России) отдается их использованию для нужд «мягкой силы», для повышения эффективности «обратной связи» госструктур с общественностью и иными внешними адресатами. В общем, для игры на информационном пространстве во благо укрепления позиций

и репутации государства за его рубежами. В довольно упрощенном видении речь идет о весе сетевых инструментов для внешней политики, об их употреблении на этом направлении ведомствами, занимающимися международными проблемами.

Но помимо новых горизонтов возможностей СИ открыли перед этими службами очевидные вызовы и предлагают очередные задачи. С развитием ИКТ еще в конце прошлого века руководство многих стран озаботилось проблемой нахождения сетевых рычагов в руках террористов и оргпреступности, выведения из строя объектов критически важной инфраструктуры. Эти вопросы стали выноситься за пределы национальных границ, на двусторонние и авторитетные международные форумы самого высокого уровня (например, обсуждение на «Группе восьми»).

Позднее в повестках переговорных механизмов на верхние позиции стали подниматься перспективы нынешнего режима регулирования Интернета (с центральными серверами на территории США) и его изменения. Ряд стран, включая Россию, выражают недовольство тем, что Всемирная паутина выпадает из сферы полномочий ООН и ее специализированной структуры – Международного союза электросвязи, а существующий статус-кво не учитывает интересы всех участников на равноправной основе. Намерениям изменить такую ситуацию противятся многие ведущие государства, и не только западные. Без взаимопонимания возникает опасность «балканизации Интернета» (с техническим обособлением отдельных его секторов и установлением в них собственных норм регулирования), что весьма активно просчитывается на специализированных площадках.

Эти вопросы закрепились и набирают вес в глобальной повестке. По некоторым из них (то же регулирование Интернета) нас по-прежнему ожидают сложные дискуссии и переговорная борьба.

В самое последнее время «корзина» заданий для внешнеполитических служб пополняется. Не менее важно, что при этом руководство ведущих стран и международных структур стало подгонять переговоры по теме сетевых инструментов в расширяющемся списке их форматов.

Степень зависимости от глобальной инфраструктуры СИ заставляет руководство вплотную и побыстрее приступить к сотрудничеству во избежание множества нежелательных последствий быстрого развития ИКТ. Возникла также потребность попытаться вместе выявить еще не просчитанные будущие угрозы.

Если взять на заметку доклад Всемирного экономического форума «Глобальные риски – 2014»[29], опубликованный в январе 2014 г., то по составленным рейтингам рисков с 2007 г. получается, что на международном уровне в верхние строчки опасностей буквально взлетели вызовы, обусловленные развитием и распространением высоких технологий, ИКТ. Более того, они, включая кибератаки, кражу данных, подрыв функционирования критически важных объектов инфраструктуры, начинают теснить даже традиционные угрозы геополитического характера. Одна из проблем заключается в том, что противодействие последним опирается на более или менее действенный опыт и механизмы регулирования, а вот в отношении опасностей в киберпространстве мы имеем явный дефицит и опыта, и понимания, и управленческих технологий.

Лишь совсем недавно, к примеру, у политических лидеров стало заметным понимание того, что ИКТ не только помогают социальному и экономическому развитию государств. Существенно участившиеся сбои и различные преступления в использовании СИ чреваты замедлением экономического роста, ослаблением финансовой стабильности. Потому данная проблематика все громче стучится в двери переговорных кабинетов «Группы двадцати», причем с возможностью ее отдельной постановки.

Возникает риск «цифровой дезинтеграции» – усиления национальных защитных мер против киберпреступлений без укрепления глобального взаимодействия, что чревато падением статуса СИ в качестве надежного средства финансово-экономического «общения» и ведения бизнеса с сопутствующими социальными и иными издержками.

Пока угрозы из сетевого пространства, как правило, лишь незримо пронизывают многие документы международных форумов, той же «двадцатки». Это в разной мере характерно для базовых внешнеполитических документов ведущих государств. Достаточно внимательнее прочитать вторую часть Концепции внешней политики Российской Федерации (от 12 февраля 2013 г.) «Современный мир и внешняя политика Российской Федерации». Однако ряд отмеченных там вызовов, в том числе транснационального масштаба, заметно исходит в том числе от СИ. Не стоит удивляться тому, что в этих документах сетевые проблемы станут очерчиваться подробнее и с отдельными ориентировками для внешнеполитических ведомств.

---

[29] Доклад Всемирного экономического форума «Глобальные риски – 2014». URL: http://www.reports.weforum.org/global-risks-2014

Более предметные официальные материалы уже предлагают внешнеполитическим ведомствам и более понятные установки. Например, принятые 24 июля 2013 г. «Основы государственной политики Российской Федерации в области международной информационной безопасности»[30] дают ориентиры для работы с внешними партнерами по сетевой проблематике.

Существенная динамика наблюдается в ООН, занятой не только добавлением новых вопросов, но и аналитической работой, направленной на поиск согласованных подходов. На последнем направлении просматриваются плодотворные усилия Группы правительственных экспертов ООН с нашим участием[31].

Группе удалось наметить выход из тупика разногласий по поводу, казалось бы, простого вопроса: один «клуб» государств предпочитает термин «кибербезопасность» (все страны Запада и многие другие ведущие игроки, такие как Бразилия, Индия), а второй – «международная информационная безопасность» (МИБ) (Россия, страны Организации Договора о коллективной безопасности и Шанхайской организации сотрудничества). При относительной размытости в предлагаемых определениях этот вопрос блокировал продуктивное обсуждение самого предмета анализа, провоцировал участников переговоров и экспертных дискуссий на обмен взаимными подозрениями и претензиями. Их логика такова. Россия хочет поставить высокие национальные барьеры для информационных потоков. А все западные страны в интерпретациях своего определения ориентируются преимущественно на сохранение статус-кво в регулировании Интернета. Это свидетельствовало об отсутствии особого желания выйти за границы обсуждения режимов работы Интернета и заняться другими направлениями в формировании международного кодекса поведения в сфере безопасности использования сетевых инструментов.

Компромиссные предложения группы получили развитие и, главное, в существенной степени закреплены в знаковом документе от 17 июня 2013 г. – Совместном заявлении президентов России и США «о новой области сотрудничества в укреплении доверия»[32]. Действительно новой – охватывающей ИКТ. В нем речь идет об «угрозах безопасности в сфере использования

[30] Основы государственной политики Российской Федерации в области международной информационной безопасности. URL: http://www.scrf.gov.ru/documents/6/114.html

[31] О высокой оценке этих усилий Россией см.: Сообщение МИД России для СМИ от 08.11.2013 г. «О принятии в ходе заседания Первого комитета на 68-й сессии Генеральной Ассамблеи ООН российской резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». URL: http://www.mid.ru/brp_4.nsf/0/9C738EC38849040244257C1D004302B7

[32] Совместное заявление президентов России и США «о новой области сотрудничества в укреплении доверия». URL: http://www.kremlin.ru/ref_notes/1479

ИКТ и самим ИКТ» и о «борьбе» с ними. Преодолев дилемму «кибербезопасности» и МИБ, лидеры обоих «клубов» наконец обозначили более понятное видение объектов сотрудничества. Благодаря этому удалось четче прописать некоторые задачи. Среди них – «более эффективная защита критически важных информационных систем», «урегулирование опасных ситуаций, вызываемых событиями, которые могут создавать угрозы безопасности в сфере использования ИКТ и самим ИКТ». Другими словами, постановка задач наконец стала шире традиционного набора вопросов вокруг информационных потоков и судеб регулирования Интернета.

С появлением этой инициативы стало легче договариваться в международных структурах. Таким же знаковым и прецедентным событием, уже на региональном уровне, стало принятие в декабре 2013 г. «Первоначального перечня мер укрепления доверия в рамках ОБСЕ с целью снижения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий». Он тоже обращен к безопасности «по использованию ИКТ и самих ИКТ»[33].

Речь идет не только об уже проделанной значительной работе, но и о предстоящих серьезных усилиях по выполнению этих документов внешнеполитическими ведомствами вместе с их коллегами. По линии ОБСЕ – найти к октябрю 2014 г. согласие в более детальном понимании терминологии и, соответственно, предмета дальнейших переговоров для расширения перечня мер доверия. Причем на сей раз требуется согласие нескольких десятков государств с весьма различными позициями и из разных «клубов по интересам». Пока же главное – члены такой непростой структуры, как Организация по безопасности и сотрудничеству в Европе, обозначили понимание того, что все они оказались в одной лодке в океане угроз, связанных с ИКТ.

Оба события представляются существенным успехом российской дипломатии. А в ближайшие месяцы ее ожидает более плотный график специализированных форумов и «саммитов» по сетевым инструментам с высоким официальным представительством. Предстоят серьезные баталии и по регулированию Интернета в преддверии полномочной конференции Международного союза электросвязи в октябре–ноябре 2014 г.

Нужно взять на карандаш вероятные «сюрпризы», из-за которых тема сетевых инструментов вторгается в кабинеты, где ведутся разговоры о весьма отдаленных от нее предметах. Из

[33] OSCE. Permanent Council Decision No 1106. «Initial set of OSCE confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies». 3 December 2013. URL: http://www.osce.org/pc/109168

недавних примеров – переговоры между США и Евросоюзом о создании трансатлантического партнерства в торговле и инвестициях. Связанный с разоблачениями Э. Сноудена скандал по поводу открытости сетевого пространства для американских спецслужб дал повод европейским переговорщикам ужесточить требования по целому ряду торгово-экономических и правовых вопросов, что поставило перед Вашингтоном много дополнительных проблем и увязок. Да и в целом такого рода «сбои» в этом пространстве увеличили нагрузку на внешнеполитические ведомства обеих сторон по выправлению трансатлантических отношений. Не исключено, что такого рода неожиданности может получить и Россия.

Эти разоблачения еще сильнее стимулируют интерес ООН к теме СИ, подняв их на новые высоты. Организация активнее и плотнее подключается к разрешению разных проблем – от регулирования Интернета до воздействия сетевых инструментов на обеспечение прав граждан и социально-экономическое развитие. Это в свою очередь не может не затрагивать планы российского МИД. К тому же в Концепции внешней политики Российской Федерации упоминание МИБ сделано именно на треке этой организации: Россия «будет добиваться под эгидой ООН правил поведения в области обеспечения международной информационной безопасности» (п. 32 (и))[34].

Список примеров можно продолжать. Но ограничимся двумя соображениями. Во-первых, существенно возрастает роль проблематики СИ во внешней политике, в расширении внешнеполитической повестки России и наших партнеров и вероятном изменении ее приоритетов; данные темы все чаще проникают в различные переговорные досье. Во-вторых, этот очевидный и динамичный процесс приводит в определенное замешательство ведомства, занимающиеся международными делами. Все еще присутствует (далеко не только в России) недопонимание реальных вызовов развития ИКТ, что препятствует более четкому формулированию вытекающих из них задач. При этом растет озабоченность очередными «сюрпризами» для соответствующих служб.

В отличие от темы «Сетевые инструменты **во** внешней политике», проблематика «Сетевые инструменты **для** внешней политики» заметно яснее изложена в официальных документах и аналитических разработках ряда ведущих государств (прежде всего США, Канады, ведущих стран Европейского союза, Китая), а главное, опирается на существенно больший практиче-

[34] Концепции внешней политики Российской Федерации. URL: http://www.mid.ru/brp_4.nsf/0/6D84DDEDEDBF7DA644257B160051BF7F

ский опыт. Она также доминирует в экспертных рассуждениях, официальных базовых установках и заявлениях российских властей, но с очевидным дефицитом прописанного видения использования СИ.

Так, целый ряд задач на треке «мягкой силы» поставлен в Концепции внешней политики Российской Федерации, прежде всего в положениях, касающихся его напрямую, – «Международное гуманитарное сотрудничество и права человека» и «Информационное сопровождение внешнеполитической деятельности». Но лишь с кратким упоминанием того, что в таком сопровождении «будут использоваться возможности новых информационно-коммуникационных технологий».

В общем, этот базовый, а также другие официальные материалы (например, Россотрудничества) предлагают список задач, успешное выполнение которых, включая критерий «затраты–эффективность», во многом зависит от масштабности подключения сетевых инструментов (о чем свидетельствует опыт, например, США, Великобритании и Австралии). Остается прописать роль последних в отдельных установочных документах или документах более широкого порядка по информационной составляющей для внешней политики.

В июле 2012 г. на совещании в российском МИД президент России отметил, что «традиционные, привычные методы международной работы освоены нашей дипломатией достаточно хорошо, если не в совершенстве, но по части использования новых технологий, например, так называемой “мягкой силы”, безусловно, есть над чем подумать»[35]. Это замечание в определенной мере оживило наше экспертное сообщество, в том числе занимающееся по части СИ. Но это было заметно лишь на первых порах.

Отметим, что по-прежнему наблюдается достаточно вольное обращение с терминами касательно сетевых технологий для внешней политики. С различным пониманием каждого из них.

Можно встретить широкий спектр понятий: «цифровая дипломатия», «сетевая дипломатия», «дипломатия Web 2.0» (в последние месяцы появилась «дипломатия 3.0»), «Твиттер-дипломатия» и т.д. и т.п. Этот разнобой вполне объясним – не только в России, но и во многих других странах отсутствует их официальная расшифровка. В некотором смысле это напоминает споры о «кибербезопасности» и МИБ. Например, под заголовками «Твиттер-дипломатия» рассматриваются вопросы, имеющие весьма опосредованное отношение к данному

[35] Совещание послов и постоянных представителей России. 9 июля 2012 г., Москва. URL: http://www.kremlin.ru/news/15902

конкретному инструменту. Размываются субъекты и объекты анализа.

Выступая 21 января 2014 г. в Москве на пресс-конференции по итогам деятельности российской дипломатии в 2013 г., глава МИД России С. Лавров впервые заметил, что «уместно говорить и об информационной дипломатии»[36]. Ранее представители министерства предложили подумать об «инновационной дипломатии», подразумевая работу в большей мере на информационном поле. Например, заместитель директора Департамента информации и печати МИД России Е.А. Пантелеев еще в конце 2012 г. поделился своим достаточно детальным видением «инновационной дипломатии»[37].

По всей видимости, назрела потребность в формулировании более конкретного комплекса задач по проблеме «Сетевые инструменты для внешней политики». Она имеет свое измерение, отличное от темы «Сетевые инструменты во внешней политике», – со своими особенностями и содержанием. Определенные сигналы из МИД России экспертному сообществу прозвучали и полезно заняться совместной работой, в том числе по вертикали «снизу вверх». В ней стоит повнимательнее оценивать плюсы и минусы из опыта некоторых лидеров по части такой дипломатии – прежде всего США и Великобритании.

Автор данного материала выпустил доклад о подходах Соединенных Штатов к предмету, который там принято официально именовать «электронной дипломатией» (ediplomacy)[38]. Данный термин к тому же встречается в названиях некоторых структур и направлений деятельности Государственного департамента. Правда, он понимается относительно в достаточно обобщенном виде: использование Всемирной паутины и новых ИКТ для содействия в реализации внешнеполитических целей. Заметим, что этот термин принят и Евросоюзом.

Поэтому обратимся к опыту Великобритании, МИД которой воспользовался американскими наработками, одобрив в конце 2012 г. «Цифровую стратегию»[39]. В отличие от США в документе упоминается «цифровая дипломатия» (но без расшифровки).

В этой связи в последнее время можно наблюдать следующую картину. В целой «колоде» определений, к которым при-

---

[36] Пресс-конференция министра иностранных дел России С.В. Лаврова по итогам деятельности российской дипломатии в 2013 году. URL: http://www.mid.ru/bdomp/brp_4.nsf/2fee282eb6df40e643256999005e6e8c/b748284d938d69b144257c67003ac3cb!OpenDocument

[37] Пантелеев Е. Внешняя политика и инновационная дипломатия // Международная жизнь. 2012. № 12.

[38] См. подробнее: Кулик С.А. Электронная дипломатия. Начало / Институт современного развития, февраль 2013. URL: http://www.insor-russia.ru/files/EDiplomacy.pdf

[39] The Foreign and Commonwealth Office Digital Strategy.
URL: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/39629/AB_12–11–14_Digital_strategy.pdf

бегают эксперты, «цифровая дипломатия» вместе с «электронной» постепенно вытесняет другие. Попутно заметим также, что используемый термин «кибердипломатия» все чаще привязывается к теме «Сетевые инструменты во внешней политике», к вопросам, затронутым в первой части материала.

По задачам и направлениям «стратегии» МИД Великобритании ограничивается преимущественно ссылками на отдельные примеры работы посольств и центрального аппарата – по повышению отдачи от «цифровых технологий в различных областях внешнеполитической работы». В их списке мы находим: «слежение за развитием событий и предсказание их дальнейшего хода»; «формулирование внешней политики»; «реализация внешней политики»; «оказание воздействия на объекты и их идентификация»; «общение (с аудиторией) и повышение (ее) интереса к внешней политике».

Весьма скудный набор примеров, причем далеко не по всему списку, свидетельствует о вполне естественной неготовности МИД широко открывать дверь на свою «кухню» (шире она открыта лишь у США). Даже сама по себе проблематика воздействия на общественное мнение, включающая непрямые методы и рычаги, со своими «ноу-хау», крайне чувствительная. Не говоря уже о «формулировании внешней политики». Поэтому неудивительно, что значительная часть документа и списка примеров посвящена в отдельном блоке использованию СИ для облегчения поддержки и тем самым улучшения восприятия страны получателями виз, а также своими гражданами, отправляющимися за рубеж.

Вместе с тем в документе довольно зримо просматриваются два важных посыла, ранее открыто и официально взятых на вооружение Госдепартаментом США. Во-первых, признается, что «масштабы использования цифровых технологий вышли за рамки команд, занятых только коммуникациями вовне, и по нарастающей напрямую охватывают команды, вовлеченные в политическую работу. Многие из последних стали непосредственно отвечать за применение цифровых технологий для достижения политических результатов, а другие команды занимаются должным обеспечением функционирования цифровых каналов»[40].

Для лучшего понимания того, что вкладывается в этот посыл, полезно обратиться к работе и документам Государственного департамента США и их экспертному анализу. Предпочтение ограничиваться в основном социальными сетями при анализе использования СИ во внешнеполитической работе

[40] The Foreign and Commonwealth Office Digital Strategy. P. 6. URL: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/39629/AB_12–11–14_Digital_strategy.pdf

создает ограниченное представление о «цифровой дипломатии». В стороне остаются другие важные объекты и субъекты использования сетевых инструментов – и вовне, и внутри государственного механизма и внешнеполитических ведомств.

Если исходить из повышения эффективности такой дипломатии для внешней политики, то речь идет в том числе об улучшении согласованности и оперативности механизма принятия и выполнения решений. Сетевые инструменты предоставляют для этого новые возможности. Возможности для накопления, оптимизации отбора и распространения по ведомствам и в самих ведомствах оценок и предложений, управления огромными потоками собственной информации и т.д. Поэтому при оценке их полезности для внешнеполитических нужд не стоит забывать о должных усилиях по перенастройке внутреннего механизма. Но здесь внешние эксперты неизбежно сталкиваются с вполне объяснимыми ограничителями, связанными с закрытостью этого механизма, в том числе в ведущих демократических странах.

Внешнеполитическая сфера – слишком чувствительная и рисковая, чтобы быть вполне открытой для стороннего анализа. Особенно по проблеме «правильного» использования дипломатами сетевой инфраструктуры для служебных нужд и для внешних коммуникаций. Но стоит обратить внимание на то, что вопросы, касающиеся сетевых инструментов внутри внешнеполитического механизма, уже обозначены заместителем директора Департамента информации и печати МИД России Е.А. Пантелеевым в его видении «инновационной дипломатии».

Во-вторых, впечатление о намерениях повысить значение СИ для использования не только «вовне», но и «внутри» самого механизма разработки и принятия внешнеполитических решений подкрепляется заявленными планами продвижения по иерархической лестнице ответственных за применение сетевых технологий, расширения программ подготовки персонала и др. Такой настрой подтвердил один из отвечающих за выполнение стратегии в МИД Великобритании А. Бай в кратком годовом отчете, размещенном в его блоге в декабре 2013 г. Хотя по поводу «формулирования» и «реализации» внешней политики упоминаются лишь «мероприятия» в рамках ежегодной встречи послов, на которых обсуждалась тема использования сетевых инструментов для «содействия внешнеполитической работе»[41].

В этой связи отметим, что внешнеполитическими ведомствами многих государств для усиления «сетевой мощи» активно

[41] Bye A. Foreign Office Digital Strategy: one year on // Digital Diplomacy – the FCO's digital work. December 20, 2013. URL: http://blogs.fco.gov.uk/digitaldiplomacy/2013/12/20/foreign-office-digital-strategy-one-year-on

привлекаются (в том числе на профильную госслужбу) представители частного сектора, занимающиеся технологиями, пиар-кампаниями и иными связанными с ней специальностями. Налажено взаимодействие с крупными частными сетевыми структурами. Расширяется сотрудничество с НКО в использовании СИ для внешних нужд государства. Не случайно, что тот же МИД Великобритании в этом русле развил свою стратегию более приземленным документом «Руководство для сотрудников по политике в сфере социальных медиа» (июнь 2013 г.)[42].

У нас же на этом «фронте» пока затишье. Несмотря на известную российскую специфику, рано или поздно из этого состояния придется выходить – как по линии частно-государственного партнерства, так и по реальному, а не декларативному расширению участия НКО в политике «мягкой силы» с их потенциалом для эффективной работы в сетевом пространстве.

При внимательном изучении опыта тех же США и Великобритании, как признанных экспертами лидеров в освоении СИ для внешней политики, полезно увидеть и оценить побольше «подводных камней». Они в значительной степени касаются использования официальными лицами и дипломатами открытых инструментов, а также рисков, обусловленных теми «приграничными зонами» общения с помощью СИ внутри механизма и вовне.

В оценках внешнеполитических ведомств обеих стран сами западные эксперты в основном едины в том, что те предпочитают весьма осторожно работать на внешних платформах и особо не рисковать. Даже небольшие ошибки здесь чреваты самыми серьезными последствиями. Многие работники находятся в среде, в которой представление о целесообразности жесткого контроля за каналами и содержанием информации и донесений доминирует над настроениями расширить пространство для использования преимуществ новых технологий.

Еще «хуже» обстоят дела у их союзников. Например, по данным на середину 2013 г., в масштабах подключения открытых каналов (Twitter, Facebook, блоги) послы США и Великобритании во многие разы опережали канадских коллег. Такой же разрыв наблюдался по линии посольств и в соотношении числа читателей на один Твиттер-аккаунт. Объяснение – в «чрезмерном централизованном и ограничительном контроле за коммуникациями». Необходимо предварительное, требующее относительно долгого времени одобрение Оттавы на публичное выступление в социальных сетях[43].

---

[42] См.: Paris R. The Digital Diplomacy Revolution: Why is Canada Lagging Behind? / Canadian Defense and Foreign Affairs Institute, June 2013. P. 3.
URL: http://www.cdfai.org/PDF/The%20Digital%20Diplomacy%20Revolution.pdf

[43] Ibid. P. 6.

Возник еще один вопрос: как достигнуть должного баланса между разрешением сотрудникам создавать собственные страницы в Twitter или Facebook для контактов с общественностью и разрешением на обмен между ними профессиональными мнениями и оценками по тем же каналам? В свою очередь Госдепартамент США сталкивается с очевидно жестким выбором между должным контролем за точностью передаваемых аудитории сообщений и предоставлением своим сотрудникам более широкого маневра во внешнем общении на более понятном и менее официозном языке.

Внутренние «фильтры» позволяют повысить гарантии того, что сотрудники, использующие сетевые инструменты, будут четко следовать официальной позиции. С другой стороны, потребность в быстром реагировании на события чревата тем, что они могут выдавать политические оценки без одобрения вышестоящего начальства. Последнее может иметь деструктивные последствия, которые будет сложно нейтрализовать. В целом необходимость оперативного реагирования на события является одним из доминирующих предметов экспертного анализа того, чтó для этого следует правильно изменить в механизмах взаимодействия с внешней аудиторией по каналам СИ.

Перед нами встает востребованная задача разобраться с тем, что такое «новые технологии» для внешнеполитической работы, какие ориентиры полезны с учетом зарубежного опыта и отечественной специфики и ресурсов, как и в каких масштабах внедрять ИКТ «внутри системы» ввиду требований безопасности и рисков, какие нужны организационные меры и изменения в том, что принято называть «документооборотом», и др. Но нужно подчеркнуть, что на этом направлении в ведущих странах, включая США и Великобританию, основную роль в поддержке инноваций и расширения возможностей СИ для внешней политики играет государство. Оно является также инициатором привлечения частного сектора, НКО и гражданского общества к решению задач рассматриваемого направления внешнеполитической работы.

Полезно также беспристрастно взвесить сильные и слабые стороны сетевого потенциала государства и подумать о формировании более ясных и понятных установок развития сетевых инструментов для нужд внешней политики. При этом следует исходить из того, что предпочтение, отдаваемое установке разной высоты барьеров в глобальном общении, вряд ли даст желаемые результаты. Перспективнее будет заняться проблемами и решениями касательно взаимодействия с рядовыми и глобальными узлами СИ в российских интересах.

Российский совет по международным делам

РОССИЯ И ВЫЗОВЫ ЦИФРОВОЙ СРЕДЫ

Издательство «Спецкнига»
Тел. (495) 744–61–79
www.specialbook.net

Верстка – Л.В. Гречнева

На обложке использовано фото с сайта
www.heywire.com.

Формат 70x100 1/16. Печать офсетная.
Усл. печ. л. 2,5. Тираж 500 экз.