Развитие информационного общества: проблемы безопасности

Е.С. Зиновьева

Тенденции развития глобального информационного общества во многом обусловлены проблемой международной информационной безопасности. В глобальной информационной сфере складываются линии разделения и направления политических конфликтов, государства разрабатывают планы ведения информационных войн и информационного противоборства. Транснациональная же природа информационного общества формирует ситуацию взаимозависимости, что придает импульс сотрудничеству по обеспечению информационной безопасности.

Глобальное информационное пространство – высокотехнологичная область, в которой находят отражение многие значимые тенденции мировой политики. Характеристики глобальной информационной сферы, в свою очередь, также трансформируют природу и содержание мирополитических процессов. В 1990-е гг. была распространена точка зрения, согласно которой развитие Интернета формирует киберпространство, не поддающееся контролю со стороны государств. Но уже в 2000-е гг. становится очевидным, что политика, в том числе международная, оказывает определяющее воздействие на развитие глобальной информационной сферы. Наметилось формирование политического пространства Интернета, во многом представляющего собой отражение «реальной» политической карты мира. Линии контроля и разделения в глобальной информационной сфере формируются за счет ограничения доступа к информации в ряде стран, широкого распространения информационных войн в бизнесе и политике.

Интернет является ключевой инфраструктурой, вокруг которой формируется глобальное информационное общество. В 2010 г. число пользователей интернета превысило 1.9 млрд. На сегодняшний день охват Интернета глобален, при этом наибольшее число пользователей проживает в Азии (41% от общего числа жителей, всего 650 млн.), на втором месте Европа (24% от количества населения, всего 390 млн.), затем Северная Америка (16% от общего числа, всего 247 млн.). Менее всего пользователей в Австралии и Океании (1,3% от общего числа, всего 20 млн.). В России 2010 г. Интернетом пользовалось 37% взрослого населения страны – то есть около 43 млн. человек, из них около 17 млн. проживали в Москве и Санкт-Петербурге. В целом уровень проникновения Интернета в РФ достаточно низкий – 37%, однако в крупных городах он превышает 60%[1]. Статистические данные показывают, насколько велик вес Интернета как средства коммуникации в современном обществе.

Для понимания природы глобального информационного общества и выявления перспективных направлений его развития важно охарактеризовать последние тенденции в развитии информационно-коммуникационных технологий и Интернета.

Зиновьева Елена Сергеевна – к.полит.н., преподаватель кафедры мировых политических процессов МГИМО(У) МИД России. Статья подготовлена при выполнении работ по гранту РГНФ 11-03-00069 по теме «Международно-политические проблемы инновационного взаимодействия в России и за рубежом: проблемы взаимодействия». E-mail: elena.zinovjeva@gmail.com

1. Основное количество вновь подключающихся пользователей проживает в странах Азии и Ближнего Востока, по экспертным оценкам эти регионы сохранят свой потенциал для интернет-технологий и в обозримом будущем. Как следствие, второй по распространенности язык в Интернете – китайский[2], и у него есть все шансы обойти английский, особенно после внедрения многоязычных доменных имен (многоязычные доменные имена - имена, представленные символами национальных алфавитов, а не только латинского). Россия также стремится занять достойное место в Интернет- пространстве и упрочить позиции русского языка. В 2010 г. был создан домен на кириллице «.рф». Таким образом, в будущем мы станем свидетелями действительно многоязычного Интернета.

2. Идет формирование «повсеместной сети». Большая часть подключений осуществляется не с помощью стационарных компьютеров (как это было предусмотрено создателями сети), а с помощью мобильных телефонов и иных типов устройств.

3. Широкое распространение получают блоги, социальные и peer-to-peer сети, вследствие чего пользователи уже не являются исключительно получателями информации, но и активными ее создателями, зачастую конкурируя с ведущими медиа-компаниями. В 2009 г. число пользователей социальных сетей превысило число пользователей электронной почты, причем, социальные сети намного более популярны среди женщин, чем мужчин.

4. Наметилась тенденция к конвергенции телекоммуникаций или появлению унифицированных коммуникаций. Постепенно происходит объединение Интернета и других телекоммуникационных технологий (радио, телевидения, телефона) на основе сетей, основанных на пакетной передаче данных (то есть глобальной сети Интернет).

5. Широкое распространение получает «облачная» обработка данных. Все больше цифровых ресурсов отдельных пользователей и организаций хранится и обрабатывается на «серверных фермах», 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 над транснациональными информационными потоками.

Определения сущностных характеристик информационного общества, предлагаемые различными учеными, существенно различаются. Так, М. Кастельс понимает под информационным обществом социум, построенный по сетевому признаку, где ключевое значение имеет принадлежность к той или иной сети крупных транснациональных компаний или СМИ[3]. Г. Шиллер вкладывает в понятие информационного общества иной смысл. Он считает, что в информационном обществе ключевое значение имеют капиталистические отношения, ибо информация становится товаром, а крупные транснациональные корпорации получают возможность эксплуатировать слаборазвитые в экономическом отношении государства[4]. Теоретическое осмысление и систематизация различных концепций информационного общества представлено в работе Ф. Уэбстера «Теории информационного общества»[5].

Интернет оказывает влияние на политические, экономические, социальные характеристики современного общества. Благодаря Интернету информация фактически становится общедоступной в любом месте и в любое время. По мнению ряда исследователей, присущие Интернету открытость, децентрализованный характер, сетевая организация, способствуют демократизации, становлению глобального гражданского общества, усилению взаимозависимости. И хотя по мере роста коммерческой значимости сети, политические и экономические интересы во все большей степени начинают определять направления эволюции Интернета, базовые характеристики, изначально присущие технологии, на сегодняшний день являются определяющими в рамках информационного общества.

Т. Фридман в написанной в 1999 г. книге «Лексус и оливковое дерево», акцентировал взаимную связь между развитием Интернета и процессами глобализации современного мира[6]. В 2005 г., уже в книге «Плоский мир», он утверждает, что Интернет и другие информационные технологии сделали людей «соседями», «убивая географию, расстояния и язык»[7]. Согласно Фридману, все то, что сегодня понимается под глобализацией – свободный обмен товарами, капиталами, рабочей силой, невзирая на расстояния и государственные границы, – не было бы возможным без обмена информацией, знаниями, идеями.

Соглашаясь с доводами Т. Фридмана, нельзя не отметить, что развитие Интернета не разрешает проблему конфликтности, присущей международной системе. Ответом на информационную глобализацию является сегментация глобальной информационной сферы. Государственные, географические разграничения дополняют новые информационные границы. Такие авторитарные государства, как Китай, Мьянма, Бирма, Пакистан, ограничивают информационные потоки с помощью крупных интернет-компаний, таких как «Yahoo» и «Google», которые стремятся закрепиться на перспективных рынках развивающихся государств и поэтому передают органам государственной власти конфиденциальную личную информацию пользователей их услуг, блокируют доступ к определенным сайтам.

Международная информационная безопасность. Одно из негативных последствий бурного развития Интернета и других информационно-коммуникационных технологий – возникновение новых форм международных конфликтов, включая информационные войны, сетевые войны,

хакерские атаки и т.п. Заместитель директора Департамента новых вызовов и угроз МИД России А.В. Крутских замечает в этой связи: «Основная озабоченность в сфере обеспечения международной информационной безопасности связана с возможностью применения информационно-коммуникационных технологий в целях, несовместимых с задачами обеспечения международной стабильности и безопасности»[8].

Доктрина информационной безопасности России дает следующее определение этого феномена: «Под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства»[9].

По мнению А.В. Федорова, «в результате распространения информационно-коммуникационных технологий изменяется характер социума, следовательно, изменяется характер возникающих в нем противоречий и их разрешения»[10]. Все большее число государств вовлекаются в создание программ информационных средств воздействия, а также ведения информационных войн. Террористические и преступные группировки также берут на вооружение средства информационного воздействия. В целом, кибербезопасность следует рассматривать в контексте так называемой «триады» угроз международной информационной безопасности – террористической, военной и преступной.

На сегодняшний день значительное число государств разрабатывает программы создания информационных средств воздействия, ведения информационных войн. Создаются специальные структуры, в чьи задачи входит не только защита национального сегмента информационной сферы и быстрое реагирование на информационные вызовы и угрозы, но и ведение скрытых и явных информационных войн (напр., Cybercom США, Cyber Operations Group Великобритании). Террористические и преступные группировки также берут на вооружение средства информационного воздействия. В целом, информационную безопасность следует рассматривать в контексте «триады» угроз международной информационной безопасности: террористической, военной и преступной. Информационная преступность и информационный терроризм зачастую выступают в роли «прикрытия» интересов и агрессивной политики государств в информационной сфере. Вместе с тем, угрозы информационной безопасности далеко не всегда являются результатом злонамеренной деятельности, следует отметить риски системных сбоев, а также возможную негативную роль случайного «человеческого фактора».

Информационные технологии оказывают двойственное влияние на международную безопасность, что проявляется в том, что с одной стороны, они способствуют демократизации, а, следовательно (в соответствии с теорией демократического мира), снижению конфликтности. С другой стороны, информационные технологии являются питательной средой для сетевых форм преступности и терроризма, удобным способом создавать асимметричные угрозы и наращивать политическое влияние, что провоцирует новые вооруженные столкновения[11].

Выделяют два основных аспекта информационной безопасности: информационно-технический и информационно-психологический. Обеспечение первого из них включает в себя защиту, контроль и соблюдение законности и правопорядка в телекоммуникационной сфере (защита от несанкционированного доступа, хакерских взломов компьютерных сетей и сайтов, логических бомб, компьютерных вирусов и вредоносных программ, несанкционированного использования частот, радиоэлектронных атак и пр.). Обеспечение же информационно-психологической безопасности предполагает защиту психологического состояния общества и государства от негативного информационного воздействия.

Особую опасность в рамках информационно-технологической компоненты информационного противоборства приобретает воздействие на критические информационные инфраструктуры государства. Нарушение информационной инфраструктуры АЭС или вывод из строя систем теплоснабжения на севере России, нарушение работы транспортных систем или систем вооружений может привести к более разрушительным последствиям, чем применение традиционного оружия.

Воздействие на критические информационные инфраструктуры будет производиться именно через открытее сети, такие, как Интернет. После террористических атак 11 сентября 2001 г. в США и странах Европейского союза защита критических информационных инфраструктур стала одним их приоритетных направлений обеспечения безопасности. На международном уровне исследовательские программы, принятие модельных законов, а также другие действия по гармонизации законодательств начинают приниматься в рамках таких организаций как ОЭСР, «Группа восьми», НАТО, ООН, Всемирный банк и др.

Защита критических информационных инфраструктур становится важнейшим фактором национальной и международной безопасности. Как правило, под критическими инфраструктурами понимаются системы, нормальное функционирование которых жизненно важно для общества и государства. Критические инфраструктуры государств во все большей степени зависят от нормальной работы информационных технологий, вследствие чего термин «критические информационные инфраструктуры» получил широкое распространение. Степень развития информационного общества, и, следовательно, зависимость от информационных инфраструктур существенно разнится между странами. Так же, как и официально определяемые списки критических инфраструктур.

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

На сегодняшний день можно назвать лишь незначительное число атак на критические информационные инфраструктуры. Вероятно, это связано с тем, что информационная сфера транснациональна, критические информационные инфраструктуры государств связаны между собой, зачастую носят международный характер (в качестве примера можно привести международные финансы). В этих условиях государства не заинтересованы в том, чтобы нарушать работу транснациональных сетей, от которых они зависят в значительной степени.

Не менее важна социально-психологическая составляющая международной информационной безопасности. В условиях всеобщего доступа к информации, широкого распространения Интернета, особое значение имеет работа с общественным мнением как внутри страны, так и на международной арене. Это наглядно продемонстрировали события в ходе августовской пятидневной войны в Южной Осетии 2008 г. В этих условиях контроль над информационным пространством выступает как инструмент «мягкой силы», то есть способности навязывать противнику свои цели посредством воздействия на его систему ценностей, установки, восприятие.

Новые тенденции в области средств ведения и форм протекания международных конфликтов позволяют говорить о революции в военном деле, основанной на применении высокоточного оружия. При этом высокоточное, наукоемкое оружие включает в себя и информационную компоненту. А.В Бедрицкий отмечает: «Сегодня основная роль информационных систем в военной сфере заключается не столько в повышении точности поражения цели, сколько в том, что с их помощью можно реорганизовать структуру вооруженных сил, сделать их более гибкими и эффективными, повысить скорость реагирования на поле боя, а также выработать новые тактические приемы»[12].

Описанные выше тенденции усиливают ассиметричный характер средств и возможностей участников современных конфликтов. Так, Китай еще в 2001 г. заявил о том, что в условиях существенного отрыва США в области развития науки и технологий не представляется возможным достижение паритета, и в этих условиях КНР будет ориентироваться на информационные средства воздействия. Информационные технологии широко используются террористами в их деятельности как в целях повышения эффективности организации между ячейками в рамках сетевой структуры, так и для широкого распространения информации о терактах, так и как одна из новых форм оружия, информационное оружие.

Авторитетный российский ученый, д.воен.н. проф. В.И. Слипченко, занимающийся анализом развития систем вооружений и революции в военном деле, полагает: следующим поколением войн, седьмым по счету, будут информационные войны, ведущиеся информационным оружием[13]. Вероятнее всего, полем боя в новых информационных войнах станет именно киберпространство. Вместе с тем, описанные тенденции могут быть отнесены к долгосрочным, на обозримую перспективу роль обычной военной силы будет сохраняться.

Перспективы международного сотрудничества по обеспечению информационной безопасности. Проблема международной информационной безопасности вышла на международную повестку дня в 1990-е гг. и с тех пор не утрачивает актуальности. Международные переговоры по проблемам информационной безопасности ведутся как на двусторонней основе, так и в рамках глобальных и региональных международных организаций – ООН, ОБСЕ, НАТО, ОДКБ, ШОС и др. Инициатором формирования глобального правового режима, не допускающего использования информационных технологий в целях, несовместимых с международной стабильностью, стала Россия.

Использование информационных технологий в военно-политических целях лишь в ограниченной степени попадает в сферу действия норм международного права. Все более актуальной становится адаптация международного права к особенностям информационной сферы. Еще в 1998 г. Россия выступила с инициативой о постановке на международном уровне вопроса об обеспечении международной информационной безопасности. Начиная с 1998 г., резолюция «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» принималась Генеральной Ассамблеей ООН ежегодно. Россия инициирует международные исследования угроз в сфере информационной безопасности и возможных совместных коллективных мер по их устранению, выступает за создание международно-правового режима, ограничивающего возможности создания и применения информационного оружия. Россия участвует в обсуждении проблем информационной безопасности на региональных уровнях, в рамках ШОС, ОБСЕ, ОДКБ.

Следует отметить умножение числа международных инициатив по информационной безопасности в последние годы. В 2010 г. был подготовлен доклад Генерального секретаря ООН по проблемам информационной безопасности. Необходимость отражения киберугроз также

была обозначена в новой Стратегической концепции НАТО 2010 г. В июне 2011 г. вступило в силу Соглашение между правительствами государств – членов ШОС в области обеспечения международной информационной безопасности. На неофициальном саммите ОДКБ в августе 2011 г. главы государств-членов обсудили вопросы информационной безопасности и контроля над Интернетом, предложения по укреплению «информационного суверенитета».

Деятельность международных организаций не ограничивается созданием площадок для дискуссий и принятием международно-правовых актов, также создаются специализированные центры, принимаются и реализуются программы действий. В 2009 г. был создан Центр оценки и мониторинга киберугроз НАТО в Эстонии. В рамках ОДКБ реализуется утвержденная президентами Программа совместных действий по формированию системы информационной безопасности. Программа охватывает такие направления, как:

– сотрудничество в политической сфере;

– совместные научные и исследовательские разработки и обмен информацией о достижениях в этой области;

– подготовка кадров;

– унификация законодательной и нормативно-правовой базы;

– совместное обеспечение безопасности жизненно важных объектов;

– проведение совместных мероприятий, направленных на борьбу с преступлениями в сфере информационных технологий[14].

Более того, с 2009 г. в рамках ОДКБ проводятся специализированные учения под названием «ПРОКСИ» («Противодействие криминалу в сфере информации»), направленные на отработку опыта совместного противодействия информационной преступности.

Информационное общество транснационально, формирует ситуацию взаимозависимости, что придает новый импульс международному сотрудничеству в данной области. В сентябре 2011 г. на встрече высоких представителей в Екатеринбурге Россией была представлена концепция Конвенции об обеспечении международной информационной безопасности. В концепции охарактеризованы основные угрозы международному миру и безопасности в информационной сфере, а также закреплена «триада» угроз военно-политического, террористического и криминального характера в сфере международной информационной безопасности. В основу противодействия этим угрозам заложена взаимоувязанная система мер, опирающаяся на общепризнанные принципы и нормы международного права, а также на меры укрепления доверия в этой области[15].

В 2011 г. постоянные представители Китая, России, Таджикистана и Узбекистана в ООН направили генеральному секретарю ООН совместное письмо с просьбой распространить Международный кодекс по обеспечению безопасности в сфере информации в качестве официального документа ООН на 66-й сессии Генеральной Ассамблеи. В кодексе определены права и обязанности государств в информационном пространстве. Документ предполагает добровольное подписание государствами и взятие на себя обязательств не использовать информационные технологии для проведения враждебных действий или агрессии, а также распространения информационного оружия и технологий. Кодекс также призывает к борьбе с преступной и террористической деятельностью в сфере информационных технологий, полному соблюдению прав и свобод в информационном пространстве и созданию международной системы многостороннего, прозрачного и демократического управления интернетом[16].

В настоящее время открываются новые возможности формирования глобального режима международной информационной безопасности. Долгое время США удерживали лидерство в области развития информационных технологий, сознательно ограничивая возможности формирования глобального правового режима информационной безопасности. Однако изменение характера угроз информационной безопасности привело к тому, что наиболее развитая в информационном плане держава оказалась крайне уязвимой. Как показывает Р.В. Болгов, американская военная мощь, созданная для укрепления национальной безопасности, и информационно-технологичные вооружения как составляющие этой мощи, на деле способствовали провоцированию конфликтности и только ослабили безопасность, для обеспечения которой они предназначались[17].

В настоящее время, несмотря на сложность и новизну рассматриваемой проблематики, не только развивающиеся, но и развитые страны поддерживают инициативу международно-правового регулирования глобальной информационной сферы. Существует разница в подходах к определению угроз информационной безопасности между Россией и рядом развитых стран. Сущностное противоречие в подходах проявляется на уровне терминологии: если Россия инициирует обсуждение проблемы «информационной безопасности», включающей в себя как технические, так и социально-психологические аспекты, то США и ряд стран Европы полагают, что на международном уровне обсуждению подлежит лишь «кибербезопасность», то есть информационно-техническая проблематика.

По мнению стран, придерживающихся последней позиции, социально-психологическое измерение информатизации включает в себя очень широкий круг вопросов, трудно поддающихся определению, и следовательно, согласование подходов в данной области на международном уровне труднодостижимо. Вместе с тем, в последние годы на экспертном уровне ведется работа, направленная на сближение названных позиций, на поиск компромисса[18].

Российские исследователи проводят параллели между международно-правовым регулированием в области освоения космического простран-

ства и развития информационного общества[19]. В обоих случаях развитие новых технологий формирует взаимозависимость и порождает вызовы и угрозы гражданского и военного характера. Разработка правовой базы, регулирующей поведение государств в космическом пространстве в целях обеспечения международной безопасности, шла поэтапно, параллельно разрабатывались и общие принципы поведения и проблемы ограничения отдельных действий государств в данной сфере (напр., запрещение ядерных испытаний в космосе). Для регулирования чувствительных, спорных направлений деятельности, которые сложно было вписать в рамки строго обязательных международно-правовых документов, были найдены приемлемые формы деклараций и принципов. Как представляется опыт международного сотрудничества по обеспечению безопасности в иных высокотехнологичных областях, таких как космос, может быть продуктивно использован в отношении глобальной информационной сфере.

Zinovjeva E.S. Evolution of the Global Information Society: Security Aspects.

Summary: *Trends of the evolution of global information society depend on the information security. New lines of political conflicts and divides emerge in the global information sphere as a result of aggressive policy of states, which create plans of information wars and conflicts. However transnational nature of the information society creates interdependence and thus incentives for international cooperation in the field of information security.*

Ключевые слова

Информационное общество, информационная безопасность, международное сотрудничество.

Keywords

Information society, information security, international cooperation.

Примечания

1. Бюллетень «Интернет в России. Весна 2010». // «Фонд развития интернета», 2010. [Электронный ресурс]. - Режим доступа: http://bd.fom.ru/report/cat/smi/smi_int/int290610_pressr
2. Internet World Stats. Usage and population statistics. [Электронный ресурс]. – Режим доступа: www.internetworldstats.org
3. Castells M. The rise of network society. The Information Age: Economy, Society and Culture Vol. I. 2nd ed. Cambridge, MA; Oxford, UK: Blackwell, 2000.
4. Schiller H. Information Inequality: The Deepening Social Crisis in America, London: Routledge 1995.
5. Уэбстер Ф. Теории информационного общества. – М.: Аспект-Пресс, 2005.
6. Friedman T. The Lexus and the Olive Tree. – N.Y.: Farrar Straus & Giroux,, 1999 – 394 p.
7. Friedman T. The world is flat: a brief history of the twenty-first century. – N.Y.: Farrar, Straus and Giroux, 2007. – 660 p.
8. Крутских А.В. К политико-правовым основаниям глобальной информационной безопасности. // Международные процессы. – 2007. – № 1(5). – С.28-37. - Режим доступа: http://www.intertrends.ru/thirteen/003.htm
9. Доктрина информационной безопасности РФ. Утверждена 9.09.2000. [Электронный ресурс]. — Режим доступа: http://www.rg.ru/oficial/doc/min_and_vedom/mim_bezop/doctr.shtm
10. Федоров А.В. Информационная безопасность в мировом политическом процессе. Учебное пособие. М.:МГИМО, 2006. С. 76.
11. Болгов Р.В. информационные технологии в современных вооруженных конфликтах и военных стратегиях (политические аспекты). Автореферат диссертации … кандидата политических наук: 23.00.04. Спб, 2010. – Стр. 13.
12. Бедрицкий А.В. Реализация концепции информационной войны военно-политическим руководством США на современном этапе : Автореферат диссертации… кандидата политических наук : 23.00.04 Москва, 2007. – С. 7
13. Слипченко В.И. Война будущего (прогностический анализ). [Электронный ресурс]. – Режим доступа: http://www.scribd.com/doc/26599/B-Слипченко-Война-будущего-прогностический-анализ
14. Кожевников А.В. О коллективных мерах государств-членов ОДКБ в сфере обеспечения информационной безопасности. // Международный терроризм в информационную эпоху: реалии кибертерроризма и кибероружия, терроризм и средства массовой информации. Сборник материалов международной конференции. М., 2010. – Режим доступа: http://catu.su/index.php?option=com_content&view=article&id=155%3A2011-11-18-13-13-16&catid=38%3Aslideshow&Itemid=91
15. К вопросу о представлении концепции Конвенции об обеспечении международной информационной безопасности. // Официальный сайт МИД России. [Электронный ресурс]. – Режим доступа: http://www.mid.ru/bdomp/ns-osndoc.nsf/e2f289bea62097f9c325787a0034c255/bb6011086c26ec3dc325792500360170!OpenDocument
16. Россия, Китай, Таджикистан и Узбекистан представили кодекс информационной безопасности. // Иносми. [Электронный ресурс]. – Режим доступа: http://inosmi.ru/russia/20110913/174603156.html
17. Болгов Р.В. информационные технологии в современных вооруженных конфликтах и военных стратегиях (политические аспекты). Автореферат диссертации … кандидата политических наук: 23.00.04. Спб, 2010. – Стр. 12.
18. Rauscher K., Yashenko V. Russia – US bilateral. Lying foundations on critical terminology East Institute: NY, 2011.
19. См., напр.: Крутских А.В. К политико правовым основаниям международной информационной безопасности. // Международные процессы. – 2007. № 13. – Режим доступа: www.intertrends.ru/thirteen/003.htm; Федоров А.В. Информационная безопасность в мировом политическом процессе. М.: МГИМО, 2006. С. 212.