ПЕРСПЕКТИВНЫЕ ТЕНДЕНЦИИ ФОРМИРОВАНИЯ МЕЖДУНАРОДНОГО РЕЖИМА ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Е.С. Зиновьева

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

В статье рассматриваются основные тенденции формирования международного режима по обеспечению информационной безопасности. Международное сотрудничество в этой сфере на глобальном уровне наталкивается на противоречия в государственных интересах. Основными субъектами информационной безопасности являются США, Россия, Китай, а также страны ЕС (Великобритания, Франция и Германия). Основное противостояние развертывается между США с одной стороны и Россией и Китаем, с другой. Страны ЕС занимают срединную позицию, тяготеющую к США. В статье доказывается, что международное сотрудничество по обеспечению информационной безопасности будет отражать общую логику развития международного взаимодействия, для которого характерны новые модели кооперации при участии государств и негосударственных акторов, получившие название многосторонних партнерств или многоуровневого сотрудничества. Логика формирования международного режима по обеспечению информационной безопасности ближе всего к логике формирования международного режима нераспространения. В интересах России поддерживать тенденцию к регионализации режима информационной безопасности. Россия может сформировать режим информационной безопасности на постсоветском пространстве на основе ОДКБ и потенциально в рамках ШОС на более широком евразийском пространстве. Регионализация режимов информационной безопасности создает для России возможность более эффективно контролировать формирующийся режим информационной безопасности на постсоветском пространстве и снимает угрозу потенциальных «цветных революций», инспирируемых по информационным каналам (в том числе с использованием социальных сетей и новых медиа).

Ключевые слова: информационная безопасность, тенденции, международный режим, регионализация.

Позиции участников переговорного процесса и перспективы достижения глобального консенсуса по обеспечению информационной безопасности

Международное сотрудничество по обеспечению информационной безопасности на глобальном уровне наталкивается на противоречия в государственных интересах. От позиций государств, как наиболее влиятельных акторов мировой политики, зависит перспектива формирования глобального режима по обеспечению информационной безопасности. Как отмечают исследователи, зачастую отсутствие институционально или формально закрепленного режима отражает интересы отдельных государств, стремящихся сохранить лидерство в какой-либо области. Схожей стратегией может быть поддержка формирования множества разрозненных организаций и институтов, регламентирующих взаимодействие в отдельной области международных отношений, так как это позволяет выбирать различные нормы и правила взаимодействия, зафиксированные в этих соглашениях, в зависимости от ситуативных интересов[1]. Как представляется схожая ситуация сложилась в сфере обеспечения международной информационной безопасности и управления Интернетом, где сформировалось множество функциональных и ряд региональных режимов.

Российские и зарубежные эксперты в качестве ключевых субъектов международного сотрудничества в области информационной безопасности называют следующие страны – США, Россия, Китай, а также страны ЕС (Великобритания, Франция и Германия) [9], отмечая, что они обладают наибольшим потенциалом в данной области. Более того, они также выступают в качестве наиболее активных участников переговорного процесса по МИБ. Ниже проанализированы их позиции по вопросу информационной безопасности.

В российской научной литературе по вопросам информационной безопасности зачастую акцентируется внимание на противоречиях, которые существуют между США и Россией в данной области, которые рассматриваются как ключевое препятствие на пути к международному сотрудничеству. Причиной противоречий является различие в возможностях и, как следствие, интересах в информационной сфере. США являются лидерами в сфере информационно-коммуникационных технологий и не заинтересованы в ограничении своей «свободы рук». Россия же стремится ограничить возможные риски, связанные с информационным пространством, укрепляя, таким образом, национальную и международную безопасность. Кроме того, Россия добивается закрепления принципа невмешательства в информационное пространство – согласно проекту Конвенции об обеспечении международной информационной безопасности, представленной на рассмотрение ООН Россией «Каждое государство вправе устанавливать суверенные нормы и управлять в соответствии с национальными законами своим информационным пространством»[2]. И хотя в документе указывается, что государства должны защищать свободу слова в Интернете и «не вправе ограничивать доступ граждан к информационному пространству», делается важная оговорка: правительства могут вводить ограничения «в целях защиты национальной и общественной безопасности»[3]. В ходе переговоров США вплоть до недавнего времени делали основной акцент исключительно на технологических аспектах защиты информационных сетей, борьбы с терроризмом и преступностью и выступали за исключение из международных документов указаний на военно-политическую составляющую проблемы.

Вместе с тем, зарубежные эксперты с большей озабоченностью отмечают обострение противоречий между США и Китаем в сфере обеспечения информационной безопасности [12]. Эти два государства предлагают два различных видения проблемы обеспечения информационной безопасности. Если Китай, как и Россия, выступает за государственное регулирование информационной сферы и обеспечение информационной безопасности на основании международных договоров, то США предпочитают частную модель регулирования и уклоняются от признания военно-политической составляющей информационной безопасности, делая акцент на террористической и преступной компонентах. 8 мая 2015 гг. Россия и Китай подписали соглашение между правительствами двух стран о сотрудничестве в области обеспечения международной информационной безопасности. В документе зафиксировано общее понимание угроз в информационной безопасности - использование ИКТ в террористических целях, для вмешательства во внутренние дела государств, подрыва суверенитета, политической и экономической стабильности, разжигания межнациональной и межконфессиональной вражды, совершения правонарушений и преступлений[4]. Столь же тес-

[1] Так называемая стратегия "forum shopping" (см. [7])

[2] Конвенция об обеспечении международной информационной безопасности (концепция). // МИД России. Официальный сайт. 22.09.2011. URL: http://www.mid.ru/bdomp/ns-osndoc.nsf/e2f289bea62097f9c325787a0034c255/542df9e13d28e06ec3257925003542c4!OpenDocument (проверено 22.08.2016 г.)

[3] Там же.

[4] Сообщение для СМИ. О подписании Соглашения между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности // МИД России. Официальный сайт. 8.05.2015. URL: http://www.mid.ru/brp_4.nsf/newsline/2C7A7D0752AAB2B843257E3F003F2204 (проверено 22.08.2016 г.)

ные отношения в сфере кибербезопасности связывают Россию лишь с партнерами по ОДКБ. По мнению западных экспертов, данное соглашение можно трактовать как стремление государств подорвать лидирующие позиции США в сфере управления Интернетом и Интернет-индустрии[5]. Отметим, что Россия и Китай выдвигают схожие инициативы по информационной безопасности на целом ряде площадок – ООН, БРИКС, ШОС. Вместе с тем, позиция Китая по сравнению с российской отличается большей выжидательностью [4], несмотря на то, что противоречия носят не только политический, но и экономический характер – именно США обвиняют в изоляции китайских ИТ-компании, в частности Huawei, от глобальных рынков[6].

Как правило, подход стран ЕС, которые также выступают в роли влиятельных игроков в глобальном информационном пространстве, трактуется как схожий с подходом США, в силу, прежде всего, союзнических обязательств по НАТО, а также значительной взаимозависимости в экономических аспектах развития Интернет-индустрии. Традиционно, страны ЕС выказывали озабоченность, прежде всего, относительно защиты от информационных угроз для экономики.

Вместе с тем, как показали международные переговоры в ходе NetMundial, а также Группы правительственных экспертов ООН по международной информационной безопасности 2014 – 2015 гг. европейские страны, прежде всего, Германия и Франция тяготеют к более независимой политике в отношении информационной безопасности, в частности, в сфере управления Интернетом они поддерживают интернационализацию контроля над этой технологией. Эксперты связывают подобное изменение позиций ряда европейских стран с разоблачениями Э. Сноудена, указавшего на факт использования США своих преимуществ в информационной сфере в целях получения политических и экономических и политических целей в ущерб интересам стран ЕС[7].

Для развивающихся стран в ходе международных переговоров, как правило, приоритетными являются вопросы информационного развития и сокращения «цифрового разрыва», помощи в создании «цифровых потенциалов».

На сегодняшний день США являются государством-лидером в области развития ИКТ и, следовательно, не заинтересованы в принятии на себя международных обязательств в данной сфере. Вплоть до недавнего времени США отказывались обсуждать на международном уровне проблематику военно-политического использования информационно-коммуникационных технологий, а также вопросы демилитаризации информационного пространства. Однако позиция США по данному вопросу изменилась с приходом к власти Б. Обамы, который провозгласил развитие Интернета и информационной сферы одним из своих приоритетов. А.В. Бедрицкий систематизировал ключевые интересы, лежащие в основе позиции США по проблеме информационной безопасности следующим образом:

1. «Военное использование киберпространства целесообразно и будет иметь важное значение. Соединённые Штаты не намерены связывать себя какими-либо ограничениями на развёртывание, испытания и использование военных возможностей в этой сфере в целом. В дальнейшем в интересах защиты критически важных инфраструктур характеристики конкретных кибернетических угроз будут детализироваться и по ним могут быть подписаны международные соглашения. Однако вопрос о том, насколько такие соглашения будут ограничивать наступательный потенциал США и, соответственно, будет ли целесообразным международное обсуждение этих вопросов, должен решаться в ходе всесторонних исследований и моделирования.

2. Соединённые Штаты будут настаивать на том, чтобы эти соглашения не исключали возможности осуществлять возмездие (сдерживание) в случае проведения против них кибернетических атак другими странами. Они также будут последовательно выступать за право предупреждать кибернетические атаки, поскольку считают такие действия активной защитой своих инфраструктур.

3. Поскольку в случае проведения кибератаки достаточно трудно выявить страну-агрессора, Соединённые Штаты, возможно, будут заинтересованы в подписании многостороннего соглашения, определяющего пропорциональность ответа на кибератаку, исходя из её масштаба, продолжительности и потенциальной угрозы для гражданских объектов. Это, естественно, потребует выработки в той или иной мере режима верификации» [1].

Показательно, что в киберстратегии Министерства обороны США от 2015 г. в качестве основных угроз безопасности США указаны агрессивные действия России и Китая в киберпространстве, отмечены также угрозы, исходящие от Ирана и КНДР, а также негосударственных акторов – кибертеррористов (прежде всего, ИГИЛ) и киберпреступников. Еще в 2011 г. киберпространство было объявлено полем боя, то в 2015 году был определен порог ущерба ки-

[5] См. напр.: Risen T. China, Russia Seek New Internet World Order // US News and World Report. 14.05.2015. URL: http://www.usnews.com/news/articles/2015/05/14/china-russia-seek-new-internet-world-order

[6] Huawei. The company that spooked the world // The Economist. 4.08.2012. URL: http://www.economist.com/node/21559929 (проверено 22.08.2016 г.)

[7] Сноуден: АНБ следит за учреждениями и гражданами Евросоюза // Интерфакс. 08.03.2014. URL: http://www.interfax.ru/world/363552 (проверено 22.08.2016 г.)

бератак, в ответ на которые будут предприняты ответные меры, в том числе с использованием обычных вооружений[8].

Изменение позиций США по вопросу обеспечения информационной безопасности стало следствием изменения баланса сил вследствие стремительного развития киберпотенциала Китая. В исследовательском сообществе США ведутся дискуссии о формах возможных кибер-столкновений с Китаем[9], в аналитических отчетах отмечается значительное число кибератак со стороны китайских хакеров на критические инфраструктуры США[10].

Как показывает опыт развития международных режимов в других высокотехнологичных областях, один актор не может навязывать другим нормы, принципы и правила поведения в долгосрочной перспективе. Динамичный характер развития Интернета и подвижность социо-экономической среды указывают на то, что США, хотя и выступали в роли гегемона на начальном этапе развития режима постепенно утрачивают подобные позиции, т.к. их роль в рамках режима все чаще ставится под вопрос другими государствами. Изначальные позиции гегемона ставятся под вопрос вмешательством национальных и международных акторов, ростом их потенциала, ассиметричными угрозами и, кроме того, динамической природой Интернета [4].

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 российский исследователь, сотрудник СПбГУ Р.В.Болгов, американская военная мощь, созданная для укрепления национальной безопасности, и информационно-технологичные вооружения как составляющие этой мощи на деле способствовали провоцированию конфликтности (в т.ч. за счет попыток противников США создать ядерное оружие) и только ослабили безопасность, для обеспечения которой они предназначались [2].

Несмотря на то, что ряд противоречий отошел на второй план (США согласились с некоторыми из российских предложений, признав наличие военно-политических угроз в области информационной безопасности, а также необходимость правового регулирования данной области) наметились новые проблемы: так, западные страны выступают не за полную демилитаризацию информационного пространства, что соответствует российским интересам, но за международно-правовое регулирование кибер-конфликтов, с целью ограничить возможность использования информационного оружия в отношении особенно уязвимых критических инфраструктур, имеющих ключевое значение для безопасности населения, таких, например, как информационные системы, обеспечивающие работу госпиталей, и пр. Позицию стран НАТО, прежде всего США, по вопросу международно-правового регулирования военно-политического аспекта информационной безопасности отражает опубликованное 19 марта 2013 года Таллиннское руководство. Данный документ, подготовленный группой экспертов Центра совместной кибероборонь НАТО в Таллинне, посвящен вопросам применения международного права к конфликтам в информационной сфере, прежде всего, в ее технологическом измерении [14].

Согласно официальной позиции России, данное руководство допускает возможность милитаризации информационного пространства, в то время как Россия подчеркивает необходимость полного запрета информационного оружия. Таким образом, данный документ можно рассматривать как «пробный шар» на пути легитимизации кибервойн, которые рассматриваются как допустимое средство разрешения межгосударственых противоречий, но закрепляется их место в правовом поле.

Вместе с тем, как утверждает О. Демидов, российский и западный подходы не обязательно противоречат друг другу. Россия выступает за подчинение поведения государств в информационном пространстве специальному своду универсальных и юридически обязывающих норм. Разница между двумя подходами заключается в том, что они рассматриваются через призму разных установок и задач. Если Россия и ее союзники видят свою миссию в том, чтобы не допустить межгосударственных киберконфликтов и вывести такие явления за рамки приемлемых действий на международной арене, то Таллиннское руководство – документ, не несущий такой задачи.

Сближение и гармонизация двух подходов – задача на отдаленную перспективу что обусловлено, прежде всего, дефицитом доверия между ключевыми участниками переговоров. Заклю-

[8] The Department of Defense Cyber Strategy. Washington, April, 2015. URL: http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (проверено 22.08.2016 г.)

[9] Cyber war and competition in the China-US relationship //Remarks delivered at the China Institutes of Contemporary International Relations. – 2010. – T. 13. URL: http://dspace.africaportal.org/jspui/bitstream/123456789/28852/1/Cyber%20war%20and%20competition%20in%20the%20China-US%20relationship.pdf?1 (проверено 22.08.2016 г.)

[10] Half of Critical Infrastructure Providers Have Experienced Perceived Politically Motivated Cyber Attacks. Press Release: Symantec. 2010. URL: http://finance.yahoo.com/news/Half-ofCritical-iw-478930509.html?x=0&.v=1 (проверено 22.08.2016 г.)

чение двусторонних соглашений по информационной безопасности может сформировать необходимую для продолжения переговоров атмосферу доверия.

Определенным препятствием для многостороннего переговорного процесса в данной области является то, что для многих государств проблематика военно-политического использования ИКТ является чувствительной и они не всегда готовы открыто обсуждать ее. Весьма спорным также является вопрос включения вопросов регулирования контента информационных сетей в сферу обсуждения в ходе международных переговоров. Россия настаивает на использовании терминов «информационная безопасность», «информационное пространство», предполагающих более широкий подход к определению референтного объекта безопасности, – в этом случае объектом безопасности являются не только сетевое оборудование и программное обеспечении, но и более широкие, социально-гуманитарные аспекты развития информационного общества. США же настаивают на использовании термина «кибербезопасность», что предполагает обеспечение исключительно безопасности компьютерных сетей. Однако и в данной области есть определенное развитие: Дискуссии в ходе деятельности ГПЭ и обсуждения проектов вышеназванных резолюций позволили выработать некий вариант нейтральной терминологии. В тексте резолюций рассматриваемая проблематика формулируется вне рамок западной лексики кибербезопасности и, по большей части, не в терминах «обеспечения МИБ». Поиски участниками ГПЭ взаимоприемлемых формулировок с целью нахождения компромисса привели к тому, что тексты резолюций обращены к проблематике «ИКТ в контексте международной безопасности», «злонамеренного использования ИКТ» и др. Таким образом, вынося спорные терминологические вопросы за скобки, удается выработать хрупкий компромисс.

В рамках складывающегося режима обеспечения международной информационной безопасности общие интересы государств и бизнеса заключаются в том, чтобы установить хрупкую атмосферу доверия и укрепить он-лайн отношения, и это достигается при помощи принципов, норм, правил и процедур принятия решений для защиты конфиденциальности, целостности и доступности, достоверности, приватности информации. И принятие правил поведения государств в данной сфере может быть важным шагом на пути к развитию международного сотрудничества. Отметим, что еще в 2011 г. Россия предложила свод правил поведения в сфере ИКТ на рассмотрение ООН как проект Конвенции об обеспечении международной информационной безопасности. В документе делается особый акцент на суверенитете в информационной сфере и невмешательстве во внутренние дела[11]. Схожий свод правил вносился на рассмотрение ООН и по линии ШОС в 2011 и в 2015 гг. Однако, США и ЕС долгое время не были готовы обсуждать подобные правила поведения, рассматривая их как попытку ограничить свободу в интернете и ввести цензуру в сети. В настоящее время страны Запада поддерживают инициативу введения правил, однако полагают, что правила не должны быть обязывающими и не должны привести к разделению Интернета на национальные сегменты. Отметим, что страны ЕС в последние годы все более открыто высказываются в поддержку идеи правил поведения, однако не поlдерживая идею «цифрового суверенитета». Более того, данная инициатива нашла поддержку у Индии, которая, как отмечает сотрудник ПИР-центра О.В. Демидов, «опасается кибер-угроз со стороны Китая» [3, с. 136].

Однако, несмотря на то, что сегодня все ключевые участники переговорного процесса согласны с необходимостью выработки правил поведения, позиции относительно содержания правил, сферы их действия, а также обязательств из них проистекающих существенно различаются. Таким образом, международные переговоры по формированию глобального режима управления Интернетом находятся на стадии определения повестки дня, и важно, что Россия выступает в роли инициатора обсуждения многих проблем, так как это дает важные преимущества в переговорном процессе.

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.

Несмотря на активизацию переговоров по вопросам информационной безопасности, трудно ожидать, что стороны в ближайшее время придут к консенсусу. Можно согласится с А.В. Бедрицким, по мнению которого «гораздо более вероятно, что Соединённые Штаты будут пытаться всячески продвигать свою модель кибернетической безопасности» [2]. Если проводить аналогии с режимами в других высокотехнологичных областях, ситуация может измениться вследствие международного кризиса, который коренным образом изменит представления государств о собственной уязвимости, подтолкнув к пониманию необходимости международного сотрудничества.

Перспективы развития международного режима в сфере управления интернетом

Проблема управления интернетом в ходе переговорного процесса всё чаще увязывается с вопросами международной информационной

[11] Конвенция об обеспечении международной информационной безопасности (концепция). // МИД России. Официальный сайт. 22.09.2011. URL: http://www.mid.ru/bdomp/ns-osndoc.nsf/e2f289bea62097f9c325787a0034c255/542df9e13d28e06ec3257925003542c4!OpenDocument (проверено 22.08.2016 г.)

безопасности. От того, на каких принципах будет организовано управление сетью Интернет, которая выступает в качестве системообразующей инфраструктуры глобального информационного общества, будут зависеть политические и экономические характеристики глобального информационного пространства, что не может не влиять на международную информационную безопасность.

В настоящее время сложился государственно-частный режим управления интернетом, в рамках которого функции технической координации пространства имен и адресов интернета возложены на ICANN, некоммерческую организацию, зарегистрированную в США и формально подчиняющуюся законам США. В настоящее время все большее количество государств оспаривают роль ICANN в управлении Интернетом, видя в ней инструмент влияния США.

Отметим, что режим управления интернетом исторически формировался при существенном влиянии экспертного сообщества (т.н. «интернет-сообщества») исследователей и инженеров, однако в настоящее время государства стремятся играть в управлении интернетом более существенную роль. С позиций теории международных режимов период доминирующего влияния организаций «интернет-сообщества» был периодом обучения, формирования базовых принципов регулирования, поскольку США и их союзники не были уверены в том, каким образом следует осуществлять управление этой новой технологией, поэтому они предоставили свободу действий экспертам. Как заявляет Э. Хаас: «В условиях неопределенности, когда вся власть сосредоточена в руках одного государства, и когда эпистемические сообщества успешно консолидировали влияние в доминирующем государстве, тогда действия этого государства могут быть модифицированы в соответствии с убеждениями представителей эпистемического сообщества. Режим все равно будет формироваться под контролем гегемона, однако его содержание будет отражать взгляды эпистемического сообщества» [10]. Подобные режимы, как правило, называют режимами «смешанного происхождения».

М. Франда в своей книге «Управление интернетом: формирование международного режима» анализирует процесс развития международного режима на основании предложенных О. Янгом стадий, которые каждый режим проходят в ходе формирования: определение повестки дня; международные переговоры; операционализация достигнутых соглашений. М. Франда показывает, что формирование международного режима управления Интернетом действительно происходит в соответствии со стадиями, выделенными О. Янгом. Наибольшее внимание М. Франда уделяет первой стадии, процессам определения международной повестки дня в области управления интернетом. Он анализирует ту роль, которую эпистемические сообщества и даже отдельные лица играли на ранних этапах формирования режима, и приходит к выводу, что именно частные лица и некоммерческие организации, обладающие на тот период монополией на определенные виды информации, во многом определяли международную повестку дня в области управления интернетом.

Однако по мере того, как количество пользователей новой технологии возрастала, на правительство США начинали оказывать давление представители бизнес-сообщества, которые требовали более формализованных процедур защиты их интересов в интернет-пространстве, в частности, защиты торговых марок. Кроме того, возрастала экономическая, политическая, культурная, социальная и др. значимость сети, и, следовательно, государства во все большей степени осознавали потенциал технологии и стремились принимать участие в управлении интернетом. Однако это не входило в планы правительства США. Желая стимулировать развитие сети, повысить прозрачность и эффективность механизмов управления, а также избежать передачи управления интернетом к одной из существовавших на тот период межправительственных организаций, США решили передать функции управления Интернетом к частной некоммерческой организации, сохранив при этом контрольные полномочия по отношению к ее деятельности. Создание ICANN в 1998 г. было оформлено Соглашением о взаимопонимании между ICANN и Департаментом торговли США (MoU, Memorandum of Understanding) и ознаменовало переход ко второй стадии развития режима управления интернетом.

Сложившийся в рамках ICANN государственно-частный режим управления интернетом не только не соответствует интересам большинства государственных акторов (в том числе и РФ), которые видят в нем институционализацию доминирования США в информационном пространстве, но не устраивает также организации гражданского общества, которые выступают за большую подотчетность и демократическую легитимность организации. ICANN на протяжении всей своей истории с момента создания подвергалась существенной критике, причем главным объектом являются ее «особые отношения» с Департаментом торговли США, который сохраняет за собой контрольные функции по отношению к данной организации.

Официально ICANN отрицает свою ведущую роль в процессе управления Интернетом еще и потому что пытается избежать того, чтобы ее рассматривали в качестве организации, претендующей на расширение своих полномочий. Однако очевидно, что эти протесты не смогли убедить ни одну из заинтересованных сторон, и организации не удалось предотвратить формирование негативно настроенного по отношению к ней общественного мнения.

Таким образом, ICANN не удалось стать той организацией, в рамках которой обсуждались бы

проблемы управления интернетом на межгосударственном уровне. Однако остальным организациям «интернет-сообщества» пока удается сохранять свои позиции в процессах управления. Стремление правительств принимать участие в процессах управления интернетом, как по символическим, так и по практическим причинам

Остановимся более подробно на прогнозах развития режима управления интернетом в целом и ICANN в частности, предлагаемых различными исследователями и аналитиками. Большая часть исследователей соглашается с тем, что ВВУИО и работа Форума по вопросам управления Интернетом ознаменовали начало нового этапа в данном процессе, который будет характеризоваться утерей США своего влияния и усилением позиций правительств других государств. Следовательно, так или иначе, произойдет усиление межправительственной компоненты режима управления интернетом.

Возможны два варианта: либо ICANN сохранит свое влияние (возможно, при этом ей придется значительно модифицировать свою структуру и состав), либо же функции технической координации инфраструктуры интернета перейдут к межправительственной организации. Сложности, с которыми уже сегодня сталкивается организация в ходе своей деятельности, отсутствие поддержки со стороны правительств, проблемы с легитимностью могут быть предвестниками радикального изменения существующего режима управления интернетом.

Очевидно, что США не могут игнорировать обеспокоенность мирового сообщества в отношении их односторонней политики в сфере регулирования интернета. Со стороны Вашингтона может быть сделана следующая уступка – предоставление ICANN независимости от Департамента торговли, что позволит им избежать наиболее нежелательно варианта – интернационализации управления интернетом и перехода функций ICANN к МСЭ. Однако, предоставив ICANN формальную независимость и увеличив возможности Правительственного совещательного комитета (Governmental Advisory Committee, GAC), США тем не менее сохранят контроль над инфраструктурой интернета благодаря своему рыночному влиянию (большая часть крупных компаний, работающих в Интернет-пространстве, имеет американскую принадлежность), экономическому потенциалу (американские корпорации управляют доменными именами общего уровня, на которых зарегистрирована значительная часть доменов), а также управлению корневыми серверами, большая часть из которых так и останется на территории США.

Если организация продолжит свое существование, возможны различные варианты повышения легитимности и эффективности ее работы. В частности, аналитиками, работающими в рамках Проекта по вопросам управления интернетом (Internet governance project) , предлагается модель реформ, включающих в себя ограничение полномочий ICANN, и передачу контрольных функций по отношению к организации на международный уровень (что подразумевает разрыв контрактных отношений с США); усиление возможностей влияния отдельных пользователей Сети на процесс принятия решений и частичную передачу функции ICANN к МСЭ, что должно стимулировать конкуренцию и повысить эффективность управления.

Сторонники точки зрения, согласно которой ICANN в будущем прекратит свое существование, по-разному видят будущее развитие режима управления интернетом. В частности, высказываются предположения, что управление интернетом будет передано межправительственной организации с глобальным охватом действий, возможно, МСЭ. Рассматривается также и такой вариант, что в результате развития глобального рынка электронной коммерции, проблемы экономической конкуренции выйдут на передний план в процессах управления интернетом и ICANN может стать намного менее влиятельной организацией в данной области по сравнению, например, с ВТО.

Складываются благоприятные условия, чтобы передать контроль управления интернетом к МСЭ. Высока вероятность того, что в ходе саммита по вопросам развития информационного общества под эгидой ООН, запланированного на 2020 г., США уступят свои лидирующие позиции в сфере управления Интернетом. Этому способствует не только кризисное положение экономики США, растущая уязвимость в сфере информационной безопасности, но и сложившиеся международная ситуация в данной области.

Подводя итог, можно сказать, что интернационализация управления интернетом в той или иной форме неизбежна. Однако очевидно, что США, которые рассматривают утрату контроля над Интернет-пространством как одну из угроз национальной безопасности страны, сделают все возможное, чтобы сохранить контрактные отношения с ICANN и свое влияние в рамках режима управления интернетом.

ICANN – частная некоммерческая организация, решения которой имеют значительные экономические, политические и общественные последствия и именно ее статус стал источником проблем, препятствующих ее эффективному выполнению своих функций. На примере ICANN можно проследить, насколько тесно переплетены между собой технические и политические аспекты в интернет-пространстве, зачастую их невозможно разделить. Ещё в 1999 г. авторитетный юрист в области интернет-права Л. Лессиг отметил тот факт, что политическое и техническое регулирование интернета неотделимы друг от друга. «Киберпространство требует нового понимания того, каким образом осуществляется регулирование и что регулирует жизнь здесь... В реальном мире мы регулирование осуще-

ствляется при помощи законов, а в киберпространстве – при помощи программного кода. В киберпространстве программное обеспечение – это закон» [11, с. 17].

Л. Лессиг также предостерегал, что по мере того как современное общество во все большей степени попадает зависимость от интернета, возрастает и опасность того, что общественные отношения будут регулироваться программным кодом, а не законодательными нормами [10, с. 17]. Подобный подход представляется некоторым преувеличением, однако нельзя не согласиться с тем фактом, что любое техническое решение всегда имеет политические последствия, так как оно способствует продвижению определенных интересов и усиливает позицию тех или иных групп как на международной арене, так и внутри государства.

Основные направления адаптации международного права к информационной сфере

Как отмечает директор и основатель «Дипло Фоундейшн» Й. Курбалиа, можно выделить два подхода к тому, каким образом существующие правовые нормы применимы к информационному пространству.

1.) «Реальное» право — подход, в рамках которого Интернет рассматривается как явление, аналогичное предшествующим ему технологиям коммуникации (прошедшим в своем развитии долгий путь от сигнальных костров до телефона). Хотя Интернет быстрее и масштабнее, он по-прежнему является способом дистанционного общения между отдельными людьми. Следовательно, любые существующие правовые нормы могут применяться и по отношению к Интернету.

2.) «Киберправо» исходит из предположения, что Интернет породил новые виды социальных взаимоотношений, осуществляющихся в киберпространстве. Следовательно, для их регулирования возникает необходимость формулировать новые «киберзаконы». Доводом в поддержку этого подхода является тот факт, что невероятная скорость и объем межнационального общения, которое ведется с помощью Интернета, препятствует применению существующих правовых норм [6, с. 85].

Как полагает Й. Курбалиа, в обоих подходах содержится зерно истины, но «реальное» право доминирует и в теории, и на практике. Согласно наиболее распространенному мнению, большая часть существующего законодательства может применяться по отношению к Интернету. Однако в ряде случаев существующие в реальном мире правовые нормы придется видоизменить для того, чтобы иметь возможность применить их к киберпространству. Для иных, более узких, проблем необходима разработка абсолютно новых законов [6, с. 85].

Вместе с тем, в современных условиях проблема адаптации международного права к информационной сфере является крайне политизированной, что связано с межгосударственными противоречиями, обозначенными в предыдущем параграфе. Несмотря на специфические характеристики ИКТ, вытекающие из Устава ООН общепризнанные принципы международного права jus cogens и соответствующие нормы международного права, а именно невмешательство во внутренние дела государств и неприменение силы и угрозы силой остаются незыблемыми как в традиционном, физическом, так и в новом, цифровом пространстве.

Остановимся более подробно на вопросах применения существующего корпуса международного гуманитарного права к информационной сфере, прежде всего, к применению информационного оружия против объектов критической информационной инфраструктуры. Информационные войны по многим параметрам отличаются от противостояния государств в «реальном» мире. Тем не менее это не отменяет необходимости нормативно-правовой регламентации. Многие из положений международного гуманитарного права были выработаны применительно к обычным условиям ведения войны и в современных условиях требуют доработки.

Право вооруженных конфликтов, несмотря на свою оторванность от политической практики, определяет правила цивилизованного ведения вооруженных действий. Международное гуманитарное право обладает лишь ограниченной применимостью по отношению к информационным конфликтам. Между тем существует насущная потребность в выработке правил регулирования конфликтов в информационной сфере. Это связано с тем, что информационные атаки по своим последствиям становятся все более масштабными, создавая реальную угрозу безопасности государству. Более того, участниками информационных конфликтов могут быть не только государства, но и неправительственные участники, в том числе террористические группировки.

К настоящему времени существует множество международно-правовых актов, регулирующих отношения государств в период вооруженного конфликта. К рассмотренным в работе группы экспертов источникам международного гуманитарного права отнесены: Женевская конвенция 1964 г. об улучшении состояния раненых на поле боя, Гаагские конвенции 1899 и 1907 гг. о законах и обычаях сухопутной войны, Женевский протокол 1928 г. о запрещении использования на войне удушающих газов и бактериологического оружия, Женевская конвенция 1949 г. об улучшении состояния раненых и больных и членов экипажа судов на море, Женевская конвенция 1949 г. об обращении с военнопленными, Женевская конвенция 1949 г. об улучшении положения гражданского населения во время войны, Женевская конвенция 1975 г. о запрещении разработки создания и хранения

бактериологических и токсических вооружений и их уничтожении, Дополнительные протоколы к Женевским конвенциям 1977 г. о защите жертв международных вооруженных конфликтов, о защите жертв немеждународных вооруженных конфликтов, Дополнительный протокол 2005 г. о принятии дополнительных отличительных знаков.

Как представляется, наибольшим потенциалом обладает международное гуманитарное право применительно к защите критических информационных инфраструктур. Несмотря на то что термин «защита критических инфраструктур» не используется в конвенциях, безопасность человека, в особенности гражданского населения, имеет прямое отношение к их содержанию. Большое значение в праве вооруженных конфликтов придается защите гражданских объектов: «гражданские объекты не должны являться объектом нападения или репрессалий»[12]. Конвенции предписывают исключение такого рода объектов из возможных объектов атаки, а также постоянную защиту и осторожное обращение. В том случае, если прекращено действие защищаемого статуса гражданских объектов, атакующая сторона обязуется сделать должное предупреждение.

Таким образом, международное гуманитарное право применимо к защите объектов критической информационной инфраструктуры, используемой в гражданских целях, как, например, информационные ресурсы и системы, обеспечивающие работу госпиталей и больниц. Вполне эффективно могут применяться положения Дополнительного протокола Гаагской конвенции 1907 г., запрещающие подвергать нападению или уничтожению объекты, необходимые для выживания гражданского населения (запасы пресной воды, запасы продуктов питания и др.). Отметим, что среди критических информационных инфраструктур можно выделить лишь незначительное количество систем, используемых исключительно в гражданских целях, что сужает применимость норм гуманитарного права. Большая часть может использоваться как в гражданской, так и в военной сферах, вследствие чего нормы права нуждаются в доработке. Гражданские информационные ресурсы и системы не обладают отличительными знаками, что потенциально повышает их уязвимость и снижает степень защиты.

В большинстве случаев в информационной сфере сложнее определить гражданские объекты, так как в наступательных и оборонительных операциях могут быть задействованы гражданские объекты. Согласно источникам международного гуманитарного права, военным относятся объекты, «которые в силу своего характера, размещения, назначения или использования вносят эффективный вклад в военные действия и полное или частичное разрушение, захват или нейтрализация которых при существующих в данный момент обстоятельствах дает явное военное преимущество»[13].

Почти все государства рассматривают информационную безопасность объектов критической инфраструктуры как проблему национальной безопасности. Отметим, что, несмотря на пробелы в международном праве, информационная безопасность в большинстве стран регулируется внутренними законодательными нормами. Пионерами в данном контексте являются США, в которых после событий 11 сентября 2001 г. безопасность критических информационных инфраструктур начинает рассматриваться в контексте антитеррористической стратегии. Вполне эффективно могут применяться положения Дополнительного протокола №1 Гаагской конвенции 1907 г., запрещающие подвергать нападению или уничтожению объекты необходимые для выживания гражданского населения (запасы пресной воды, запасы продуктов питания и др.).

В настоящее время многие элементы национальной инфраструктуры находятся в сфере владения частного сектора и не являются собственностью государства. Поэтому важным в организации системы ее эффективной защиты является сотрудничество правительственных ведомств, общественных организаций, с привлечением коммерческих структур, осуществляющих деятельность в ключевых секторах национальной критической инфраструктуры. Очевидно, что опыт внутригосударственного регулирования должен быть использован при выработке международно-правовых норм.

Очевидно, что изучение вопроса применимости и достаточности международного гуманитарного права для правового регулирования действий с применением информационного оружия осуществимо только при понимании того, что признается существование и возможность использования информационных систем как оружия, а организованное противоборство с его использованием признается как война. В настоящее время международное сообщество приходит к такому пониманию. Страны склонны признавать свою уязвимость в информационной сфере, и проявляют готовность принимать международно-правовые документы, регулирующие и ограничивающие возможность агрессивных действий в информационной сфере.

В этих условиях необходима адаптация норм права, чтобы компьютеры и программные коды можно было классифицировать как системы вооружения. Термин «информаци-

[12] Дополнительный протокол I к Женевским конвенциям от 12 августа 1949 г., касающийся защиты жертв международных вооруженных конфликтов (Протокол I). Женева, 8 июня 1977 г. (ст. 52)

[13] Второй протокол к Гаагской конвенции о защите культурных ценностей в случае вооруженного конфликта 1954 года. Гаага, 26 марта 1999 г. (ст. 1).

онное оружие» используется в ряде международных документов, принятых в рамках ШОС и СНГ[14]. Например, согласно ст. 1 Соглашения между Правительствами государств-членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности от 16.07.2009 главной угрозой международной информационной безопасности является «разработка и применение информационного оружия, подготовка и ведение информационной войны», ее признаками являются «... воздействие на системы транспортировки, коммуникаций и управления воздушными, противоракетными и другими видами объектов обороны, в результате чего государство утрачивает способность обороняться пред лицом агрессора и не может воспользоваться законным правом самозащиты, нарушение функционирования объектов информационной инфраструктуры, в результате чего парализуются системы управления и принятия решений в государствах, деструктивное воздействие на критически важные структуры»[15]. Подобный подход может быть использован международным сообществом в качестве основы для выработки общепризнанного определения информационного оружия.

Группа российских и американских ученых выработала следующие рекомендации по международно-правовой регламентации информационной сферы:

1) привлечение частного сектора и неправительственный организаций к выработке мер по разделению защищенных и незащищенных инфраструктур;

2) необходимость использования отличительных знаков для защищенных объектов в информационной сфере;

3) следует признать рост влияния негосударственных акторов и пользователей Интернета [13].

Подводя итог рассмотрению применимости международного гуманитарного права к информационным войнам, отметим, что, несмотря на то что большая часть его положений разрабатывалась в отношении обычных вооружений, его положения разрабатывались с целью гуманизировать войну, избежать страданий мирного населения, поэтому если они и устарели, то лишь формально, но не по сути. Как отмечает российский эксперт, канд. физ.-мат. наук А.В. Федоров, «в информационном обществе доминируют интересы государств, прежде всего, интересы политические, и их столкновение ведет к противоборству, в наиболее острой форме – информационной войне. Тем не менее это не отменяет регламентации международных отношений нормами международного публичного права» [7, с. 138].

* * *

На современном этапе не сложилось единого международного режима обеспечения информационной безопасности. Скорее, мы можем наблюдать совокупность разрозненных инициатив и режимов, направленных на решение специфических проблем безопасности, возникающих в «цифровую эпоху».

Глобальное международное взаимодействие по обеспечению информационной безопасности на современном этапе находится на стадии определения повестки дня. На этом этапе, согласно теории международных режимов, особое значение приобретает взаимодействие в рамках исследовательских структур и МНПО (формирующих эпистемическое сообщество и способных повлиять на ход международного сотрудничества). Несмотря на отдельные попытки кооперации между исследовательскими структурами, на сегодняшний день существенного сближения двух секьюритизирующих дискурсов не наблюдается.

Переход от стадии определения повестки дня к переговорному процессу и впоследствии имплементации достигнутых соглашений был бы возможен вследствие осознания участниками баланса угроз, что чаще всего происходит в результате острого международного кризиса. В сфере информационной безопасности кризиса пока не произошло, причем ситуация осложняется спецификой информационного оружия – сложностью идентификации источника атаки, относительной доступностью, а также асимметрией наступательных и оборонительных вооружений в кибер-пространстве (в настоящее время наступательное информационное оружие гораздо эффективнее оборонительного).

В ряде регионов сложились эффективные режимы информационной безопасности, сторонам удалось выработать повестку дня, договориться по согласованным вопросам и приступить к имплементации достигнутых решений: Евроатлантический регион в рамках НАТО, Юго-восточная Азия в рамках АСЕАН, евразийский регион в рамках ОДКБ и ШОС. На двустороннем уровне сотрудничество по вопросам информационной безопасности реализуется, как правило, между государствами, обладающими значительными кибер-потенциалами (и воспринимающими друг друга как угрозу или же объединяющимися против общей угрозы) и режимы двустороннего взаимодействия находится в состоянии имплементации. Как правило, подобные режимы ориентированы на формирование доверия и предсказуемости в отношениях между государствами.

На современном этапе развития США стремятся закрепить свои лидирующие позиции как в рамках режима управления Интернетом, так и

[14] См. напр.: Соглашение между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. 2009 г.

[15] Там же.

в сфере информационной безопасности. В этих условиях США не заинтересованы в развитии международного сотрудничества на глобальном уровне по обеспечению информационной безопасности, желая сохранить «свободу рук» в развитии и военном применении информационных технологий, в том числе информационного оружия (за исключением выработки правил применения норм международного гуманитарного права к информационной сфере, что позволит легитимировать кибер-конфликты, подчинив их правовым нормам). Однако, постепенное распространение новых технологий и инноваций в мире может подорвать технологически лидерство США. В случае если Китаю удастся оспорить технологические лидерство США, повысится вероятность интенсификации международного сотрудничества по обеспечению информационной безопасности на глобальном уровне.

Как представляется международное сотрудничество по обеспечению информационной безопасности будет отражать общую логику развития международного взаимодействия, для которого характерны новые модели кооперации при участии государств и негосударственных акторов, получившие название многосторонних партнерств или многоуровневого сотрудничества. Роль подобного взаимодействия при обеспечении информационной безопасности будет возрастать. При этом за государствами остается координирующая роль в данной области.

В интересах России поддерживать тенденцию к регионализации режима информационной безопасности. Россия может сформировать режим информационной безопасности на постсоветском пространстве на основе ОДКБ и потенциально в рамках ШОС на более широком евразийском пространстве. Регионализация режимов информационной безопасности создает для России возможность более эффективно контролировать формирующийся режим информационной безопасности на постсоветском пространстве и снимает угрозу потенциальных «цветных революций», инспирируемых по информационным каналам (в том числе с использованием социальных сетей и новых медиа). Кроме того, Россия могла бы учесть ряд перспективных технологических тенденций («большие данные», «интернет вещей) при определении повестки дня, что позволило бы получить «преимущества первопроходца» при обсуждении исследуемой проблематики на международном уровне.

Список литературы

1. Бедрицкий А.В. Международные договорённости по киберпространству: возможен ли консенсус? // Проблемы национальной стратегии. 2012. №4. С. 119-136. URL: http://www.riss.ru/images/pdf/journal/2012/4/10_.pdf (проверено 22.08.2016 г.)
2. Болгов Р.В. Информационные технологии в современных вооруженных конфликтах и военных стратегиях // Дисс. … ученой степени кандидата политических наук. СПб: СПбГУ, 2011.
3. Демидов О.В. Обеспечение международной информационной безопасности и российские национальные интересы // Индекс Безопасности. 2013. № 1. С. 129-168. URL: http://www.pircenter.org/media/content/files/10/13559089230.pdf (проверено 22.08.2016 г.)
4. Коротков А.В., Зиновьева Е.С. Безопасность критических информационных инфраструктур м международном гуманитарном праве // Вестник МГИМО-Университета. 2011, №4.
5. Ибрагимова Г. Стратегия КНР в области управления Интернетом и информационной безопасности // Индекс безопасности. 2013. № 1. 169-184. URL: http://www.pircenter.org/media/content/files/10/13559074100.pdf (проверено 22.08.2016 г.)
6. Курбалиа Й. Управление Интернетом. М.: Координационный центр национального домена сети Интернет, 2010.
7. Федоров А.В. Информационная безопасность в мировом политическом процессе: учеб пособие. М.: МГИМО, 2006.
8. Busch M. L. Overlapping institutions, forum shopping, and dispute settlement in international trade // International Organization. 2007. №. 04. P. 735-761
9. Giles K., Hagestad W. Divided by a common language: cyber definitions in Chinese, Russian and English // Cyber Conflict (CyCon), 2013 5th International Conference on. IEEE, 2013. Pp. 1-17.
10. Haas P. Epistemic Communities and International-Policy Coordination - Introduction // International Organization. 1992. No. 46 (1). Pp. 1-35.
11. Lessig L. Code and other laws of cyberspace. NY: Basic books, 1999.
12. Lieberthal K., Singer P. Cybersecurity and U.S. - China Relations. Jonh L. Torton China Institute in Brookings, 2012. URL: https://www.brookings.edu/wp-content/uploads/2016/06/0223_cybersecurity_china_us_lieberthal_singer_pdf_english.pdf (проверено 22.08.2016 г.)
13. Rauscher K., Korotkov A.Working towards rules for governing cyber conflict.Rendering Geneva and Hague conventions in cyberspace // East-West institute. 2011. URLhttps://www.eastwest.ngo/idea/towards-rules-governing-cyber-conflict-0 (проверено 22.08.2016 г.)

14. Tallinn Manual on the International Law Applicable to Cyber Warfare / ed. by M.Schmitt – N.Y.: Cambridge University Press, 2013.

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

Об авторе

Е.С. Зиновьева – к.полит.н., доцент кафедры мировых политических процессов МГИМО МИД России.
E-mail: elena.zinovyeva@gmail.com.

FUTURE TRENDS OF FORMATION OF THE INTERNATIONAL REGIME ON THE PROVISION OF INFORMATION SECURITY

E.S. Zinovieva

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

Abstract: *The article discusses the key trends shaping the international regime on information security. International cooperation in this area at the global level encounters contradictions of state interest. The main actors of the information security are the United States, Russia, China and the EU countries (Britain, France and Germany). The main contradiction is developing between the US on one side and Russia and China on the other. EU countries occupy the middle position, gravitating to that of US. The article proves that international cooperation on information security will reflect the overall logic of the development of international cooperation, which is characterized by a new model of cooperation, with the participation of state and non-state actors, known as multi-stakeholder partnerships and multi-level cooperation. The logic of the formation of an international regime on information security is closest to the logic of the formation of the international non-proliferation regime. It is in the interest of Russia to support the trend towards regionalization of information security regime. Russia can form a regional information security regime in the former Soviet Union on the basis of the CSTO and SCO and potentially on a wider Eurasian space. Such regional regime would give Russia an opportunity to shape the international regime and closely monitor emerging information security issues in the former Soviet Union, and remove the potential threat of "color revolutions".*

Key words: information security, trends, international regime regionalization.

References

1. Bedritskiy A.V. Mezhdunarodnye dogovorennosti po kiberprostranstvu: vozmozhen li konsensus? [International agreement on cyberspace: Is consensus possible?] *Problems of National Strategy.* 2012. №4. Pp 119-136. URL: http://www.riss.ru/images/pdf/journal/2012/4/10_.pdf (accessed 22.08.2016) (In Russian).
2. Bolgov R.V. Informatsionnye tekhnologii v sovremennykh vooruzhennykh konfliktakh i voennykh strategiiakh [*Information technology in contemporary armed conflicts and military strategies*]. Diss. ... A scientific degree of candidate of political sciences. St. Petersburg: St. Petersburg State University, 2011. (In Russian).
3. Demidov O.V. Obespechenie mezhdunarodnoi informatsionnoi bezopasnosti i rossiiskie natsional'nye interesy [Ensuring international information security and national interests of Russia]. *Security Index.* 2013. № 1. Pp. 129-168. URL: http://www.pircenter.org/media/content/files/10/13559089230.pdf (accessed 22.08.2016) (In Russian).
4. Korotkov A.V., Zinovieva E.S. Bezopasnost kriticheskih informatsionnih infrastruktur v megdunarodnom gumanitarnom praven [Security of Critical Information Infrastructures in the International Humanitarian Law] Vesnik MGIMO-Universitets, 2011. № 4.
5. Ibragimov G. Strategiia KNR v oblasti upravleniia Internetom i informatsionnoi bezopasnosti [China Strategy for Internet governance and information security] *Security Index.* 2013. № 1. 169-184. URL: http://www.pircenter.org/media/content/files/10/13559074100.pdf (tested 22.08.2016 city) (In Russian).
6. Kurbalia J. *Upravlenie Internetom* [Internet governance]. Moscow: Coordination Center for TLD RU, 2010. (In Russian).

7. Fedorov A.V. *Informatsionnaia bezopasnost' v mirovom politicheskom protsesse* [Information security in global political process]. Moscow: MGIMO 2006. (In Russian).
8. Busch M.L. Overlapping institutions, forum shopping, and dispute settlement in international trade. *International Organization*. 2007. Vol. 61. No. 04. P. 735-76. DOI: http://dx.doi.org/10.1017/S0020818307070257
9. Giles K., Hagestad W. Divided by a common language: cyber definitions in Chinese, Russian and English. *Cyber Conflict (CyCon), 2013 5th International Conference on IEEE,* 2013. Pp. 1-17.
10. Haas P. Epistemic Communities and International-Policy Coordination – Introduction. *International Organization*. 1992. Vol. 46, no. 1. Pp. 1-35.
11. Lessig L. *Code and other laws of cyberspace.* NY: Basic books, 1999.
12. Lieberthal K., Singer P. *Cybersecurity and U.S. - China Relations.* Jonh L. Torton China Institute in Brookings, 2012. URL: https://www.brookings.edu/wp-content/uploads/2016/06/0223_cybersecurity_china_us_lieberthal_singer_pdf_english.pdf (accessed 22.08.2016)
13. Rauscher K., Korotkov A. *Working towards rules for governing cyber conflict. Rendering Geneva and Hague conventions in cyberspace*. East-West institute. 2011. URL: https: //www.eastwest.ngo/idea/towards-rules-governing-cyber-conflict-0 (accessed 22.08.2016)
14. *Tallinn Manual on the International Law Applicable to Cyber Warfare.* ed. by M .Schmitt. N.Y .: Cambridge University Press, 2013.

The article is prepared with RSF financial support, project "Long-term forecasting of international relations» № 14-18-02973.

About the author

Elena S. Zinovieva – PhD in Political Science, associate Professor at the Department of World Politics, MGIMO-University. E-mail: elena.zinovyeva@gmail.com.