DOI: 10.7256/2226-6305.2014.1.11411
При цитировании этой статьи сноска на doi обязательна

МЕЖДУНАРОДНЫЕ ОРГАНИЗАЦИИ И РАЗВИТИЕ ОТДЕЛЬНЫХ ОТРАСЛЕЙ МЕЖДУНАРОДНОГО ПУБЛИЧНОГО ПРАВА

Касенова М.Б.

МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО И УПРАВЛЕНИЕ ИСПОЛЬЗОВАНИЕМ ИНТЕРНЕТА

Аннотация. *В дискуссиях о роли интернета, его глобального функционирования, формирования моделей его трансграничного использования и проч., – вопрос о том: «кто контролирует и управляет интернетом» является ключевым. В настоящей статье анализ проблематики управления использованием интернета осуществлен автором в связи с функционированием многосторонней модели управления интернетом, и в контексте проблематики кибербезопасности. При этом, по мнению автора, кибербезопасность нельзя рассматривать вне контекста управления интернетом в целом и формирования модели управления интернетом, в частности, поскольку иной подход понимания кибербезопасности может привести, как минимум, к полицентризму и фрагментации интернета рамками национальной юрисдикции государств, может разрушить глобальную сеть, став препятствием трансграничного функционирования интернета, а также к доминированию государств в мультистейкхолдерской модели управления интернетом. В статье также анализируется «Таллиннское руководство по международному праву, применимому в случае кибервойны» 2013 г., рассматриваются вопросы роли и значения современного международного права.*

Ключевые слова: *интернет, управление, международное сотрудничество, кибербезопасность, глобальная сеть, кибервойна, международное право, киберпространство, мультистейкхолдеризм, саморегулирование*

Abstract: *The discussions on the role of Internet, its global functioning and formation of the models for its trans-border use, the issue of who controls and manages the Internet is key. This article contains analysis of problems of Internet management in relation to the functioning of the multidimensional model of Internet management within the context of cyber-security problems. In the opinion of the author the cyber-security may not be viewed outside the context of Internet management in general and formation of the model for the Internet management in particular, since a different approach to understanding cyber-security may lead at least to polycentrism and fragmenting of the Internet within the frameworks of national jurisdiction of the states, and it may destroy the global networks, becoming an obstacle in the trans-border functioning of the Internet, as well as to the domination of state in the multi-stakeholder model of Internet management. The article also analyzes the Tallinn Manual on the International Law Applicable to Cyber Warfare of 2014, discussing the issues of role and value of modern international law.*

Keywords: *Internet, management, international cooperation, cyber-security, global network, cyber-warfare, international law, cyber-space, multi-stakeholderism, self-regulation.*

Революционный успех интернета приводит к «интернетизации» значительного числа государств, что, с одной стороны, расширяет и изменяет географию и аудиторию интернет-пользователей, а с другой, ввергает государства в своеобразную «технологическую гонку вооружений». Общеизвестным фактом является то, что интернет первоначально предназначался для военных целей и исторически одной из основных причин возникновения интернета стало военное противостояние 60-х годов XX века и угроза нанесения ракетно-ядерного удара. Правительство США инициировало научно-исследовательский проект американского военно-промышленного комплекса в целях создания системы управления стратегическими ядерными силами. Была поставлена задача

DOI: 10.7256/2226-6305.2014.1.11411
При цитировании этой статьи сноска на doi обязательна

создания устойчивой системы управления способной сохранять функциональность даже при нанесении ракетно-ядерного удара и уничтожения части компонентов такой системы. Интернет создавался и развивался как технологическая система информационного обмена между лицами, передающими и получающими информацию, по произвольным маршрутам через определенные узловые соединения. При этом базовая технологическая архитектура интернета изначально зиждилась на саморегулировании, децентрализованной «сетевой» организационной модели, не предполагающей иерархии управления и идентификации лиц, получающих и передающих информацию, включая определение статуса таких лиц. За более чем сорокапятилетнюю историю своего развития интернет превратился в глобальную коммерческую инфраструктуру трансграничного информационного обмена, но базовые технологические особенности интернета принципиально не изменились, а лишь модифицировались для удобства пользования интернетом возрастающим числом пользователей. Именно базовая технологическая структура интернета стала не только ключевым фактором захватывающего революционного развития и расширение интернета во всем мире, но и определяющим моментом формирования так называемой «мультистейкхолдерской модели» (*Multistakeholders' Model)*управления интернетом.

Мультистейкхолдерская, иначе многосторонняя модель управления интернетом означает участие всех «заинтересованных сторон», т.е. мультистейкхолдеризм означает, что в решении вопросов управления интернетом участвуют все «заинтересованные стороны» (*Stakeholders)*. К их числу относятся государства, международные организации, гражданское общество, частный сектор, техническое и академическое сообщество[1]. Без взаимодействия всех «заинтересованных сторон», без принятия согласованных между ними норм, правил и принципов регулирования, как показывает практика развития интернета, ни одно из предлагаемых решений или технических требований не может быть эффективно реализовано. Сложившаяся многосторонняя модель управления интернетом стала эффективным способом его трансграничного функционирования, обеспечивая совместимость, стабильность, безопасность и доступность глобальной инфраструктуры интернета, в то же время, предоставляя суверенным государствам возможность регулирования использования интернета в пределах национальной юрисдикции. Такая многосторонняя модель получила закрепление в документах международных межправительственных и международных организаций и форумов[2]. Мультистейхолдеризм, т.е. участие всех заинтересованных сторон, является основой трансграничного функционирования и дальнейшего развития интернета, включая формирование модели международно-правового управления интернетом.

В традиционном в настоящее время понимании, термин «управление интернетом» или «управление использованием интернета», появился в начале 2000-х годов, явившись неким условным переводом английского эквивалента «*Internet Governance*». К слову «*governance*», также как и к целому ряду понятий и категорий, выраженных по-английски, нелегко подобрать однозначный перевод в большинстве языков мира, включая русский. В доктринальном и практическом плане используются разнообразные переводы понятия «*Internet Governance*» на русский язык, в том числе – «регулирование интернета», «управление использованием интернета» и т.д. Представляется, что из всего терминологического многообразия предложенных переводов именно «управление интернетом» наиболее адекватно отражает суть описываемого явления.

[1] Английское слово «Multistakeholders» переводится как заинтересованные стороны. В доктрине используются слова, являющиеся «калькой» этого слова: «мультистейкхолдеризм», «мультистейкхолдерская модель» и т.д.

[2] См., например, Резолюция Генеральной Ассамблеи 58/201, а также), информация о Всемирном саммите Информационного общества (WSIS). URL:http://www.itu.int/wsis/basic/about.html.

DOI: 10.7256/2226-6305.2014.1.11411
При цитировании этой статьи сноска на doi обязательна

Определение, считающееся в настоящее время общепризнанным, было разработано Рабочей группой по управлению интернетом (*Working Group on Internet Governance, WGIG*) при Генеральном секретаре ООН[3], и формулируется оно следующим образом: «Управление интернетом» означает «*разработку и применение правительствами, частным сектором и гражданским обществом, при выполнении ими своей соответствующей роли, общих принципов, норм, правил, процедур принятия решений и программ, регулирующих эволюцию и применение интернета*»[4]. Следует обратить внимание на важный подход, закрепленный в данном определении, а именно: участие всех заинтересованных сторон в управлении интернетом.

Каждая заинтересованная сторона в управлении интернетом осуществляет «соответствующую роль»[5]. Так, роль и обязанности правительств связаны с такими аспектами деятельности как разработка, координация и осуществление государственной политики на национальном уровне, координация политики на региональном и международном уровнях; создание благоприятных условий для развития информационных и коммуникационных технологий (ИКТ); надзорные функции; разработка и принятие законов, положений и стандартов; разработка международных договоров и правил; развитие передового опыта; содействие созданию потенциала в сфере информационно-коммуникационных технологий и с их помощью; борьба с киберпреступностью; содействие международному и региональному сотрудничеству; решение общих вопросов развития; поощрение многоязычия и культурного разнообразия; и др.

В сферу ответственности частного сектора относятся вопросы саморегулирования информационной индустрии; развития передового опыта; разработки стратегических предложений, руководящих принципов и инструментария для директивных органов и других заинтересованных сторон; научных исследований и опытно-конструкторские разработки в области технологий, стандартов и процессов; участия в разработке национального законодательства и национальной и международной политики; содействия инновационной деятельности и др.

Роль и функции гражданского общества включают расширение информированности общественности и создание потенциала (знания, подготовка кадров, обмен опытом); предоставление экспертов, специалистов, обмен опытом и знаниями по вопросам политики в области информационно-коммуникационных технологий; научные исследования и опытно-конструкторские разработки в области технологий и стандартов; содействие в обеспечении соответствия политических и рыночных факторов потребностям всех членов общества; содействие формированию концепций информационного общества, ориентированного на человека, на основе прав человека, устойчивого развития, социальной справедливости и предоставления широких возможностей и др.

Таким образом мультистейкхолдерский подход является основополагающим элементом управления использования интернета.

2. Интернет, с одной стороны, представляет собой техническое изобретение и, будучи «техническим изобретением», он объективно требует технической поддержки и технологического обеспечения. В организационно-технической поддержке интернета, его технологического функционирования и развития принимают участие все заинтересованные стороны, а в многосторонней модели управления интернетом ведущая роль принадлежит частному сектору, гражданскому обществу, техническому и академическому сообществу[6]. С другой стороны, интернет не

[3] Например, в документах международных организаций термин «*Internet Governance*» переводится как «управление использованием интернета» и «управление интернетом». URL: http://www.wsis/wgig/docs/wgig-background report.pdf.

[4] Результаты Всемирного саммита информационного общества (World summit on the Information Society Outcome Documents): Geneva 2003 – Tunis 2005; URL: http://www.itu.int/wsis/outcome/booklet.pdf

[5] См. подробнее: Декларация принципов WSIS, пункт 49 (WSIS-03/GENEVA/DOC/0004).

[6] См. подробнее Касенова М.Б. Управление интернетом. Международно-правовой механизм. СПб., 2012. С. 13-20

DOI: 10.7256/2226-6305.2014.1.11411
При цитировании этой статьи сноска на doi обязательна

только «техническое изобретение». Интернет интегрирует материальные, финансовые, интеллектуальные, гуманитарные, политические, социальные и др. ресурсы, влияя на формирование национальных и международных процессов регуляции и обеспечивая коммуникационные связи в международном, глобальном масштабе. Организация использования интернета охватывает как технические вопросы, так и вопросы государственной политики связанных с интернетом, решение которых относится к суверенным правам государств. И внутригосударственные, и международные вопросы государственной политики, связанные с интернетом, не исключают участие всех заинтересованных сторон, но очевидно, что в решении этих вопросов ведущая роль принадлежит государствам. Отметим, что в более чем сорокапятилетней истории развития интернета решение проблем, связанных с государственной политикой в сфере интернета, практически насчитывает десятилетие.

Разграничение регулирования вопросов, связанных с трансграничным функционированием и развитием интернета нашло закрепление в ряде документов международных организаций и форумов, включая итоговые документы двух этапов Всемирной встречи на высшем уровне, WSIS. Так, резолюция Экономического и Социального Совета ООН (ЭКОСОС) 2011/16 от 26 июля 2011 года (п. п. 22, 24) разграничивает вопросы интернета на сферу, связанную с повседневной деятельностью технического и эксплуатационного характера, и сферу, связанную с государственной политикой, касающейся интернета не связанную с повседневной деятельностью технического и эксплуатационного характера, включая деятельность государств в выполнении своих обязательств в решении международных вопросов государственной политики, касающиеся интернета[7].

3. Несмотря на то, что существует аспект управления интернетом, находящийся в сфере международного публичного права, субъектами которого являются суверенные государства, международные межправительственный организации, государство-подобные образования, практические шаги в вопросах управления интернетом на международно-правовом уровне также невозможно решать без «участия всех заинтересованных сторон».

Интернет по своей технологической сути носит международный, глобальный характер, в том числе и потому, что техническая и технологическая поддержка функционирования интернета как таковая осуществляется таким образом, чтобы обеспечивать функционирование интернета не в рамках только одного государства, но в международном масштабе. Международный (в значении – «межстрановой»), глобальный характер интернета диктует саму логику его управления: вопросы управления интернетом не могут находиться вне международного, глобального контекста, неизбежно связываются с необходимостью международного взаимодействия государств, в том числе с формированием соответствующей международно-правовой модели управления. Интернет достаточно долгое время не был предметом системного анализа специалистов международного публичного права, хотя в силу своей трансграничной природы он должен был стать естественным объектом интереса международного права. Системный доктринальный анализ вопросов регламентации отношений в интернете, управления интернетом международным публичным правом, применимости международного права к интернету, и прочее, – относится к концу XX – началу XXI века и стал отражением понимания того, что без международно-правового сотрудничества, без использования международно-правовых институтов и механизмов невозможно решать вопросы управления интернетом. При этом традиционное понимание международного права как системы договорных и обычных норм и принципов, выражающих согласованную

[7] E/2011/INF/2. См. также Документ ООН: A/RES/59/220; Документ ООН: A/RES/60/252; Документ ООН: A/60/687; World Summit on the Information Society.URL: http://www.itu.int/wsis/.

DOI: 10.7256/2226-6305.2014.1.11411
При цитировании этой статьи сноска на doi обязательна

волю государств и регулирующих отношения между ними, международными организациями и другими субъектами международного права, – целесообразно рассматривать в качестве базового.

4. Одним из важнейших аспектов управления интернетом является обеспечение безопасности интернета и противодействие попыткам его противоправного использования. С развитием современных информационных технологий человечество столкнулось с новыми типами угроз: возможностями силового противостояния государств в информационной сфере («кибервойны»), использованием информационных технологий террористическими организациями либо в террористических целях («кибертерроризм»), а также использованием интернета в иных противоправных целях, и нарушением установленного правопорядка, преследуемым уголовным законодательством национальных государств («киберпреступность»).

Терминологическое и понятийное разнообразие, о котором говорилось применительно к термину «*Internet Governance*» в начале настоящей статьи, получает конкретное выражение, в частности в том, что в Российской Федерации, в ряде государств СНГ термин «киберпреступность» переводится термином «международная информационная безопасность». Примечательно, что принятая Советом Европы «Конвенция о преступности в сфере компьютерной информации» 2001 года, в английской версии называется «*Conventionon Cybercrime*», однако в переводе на русский язык (неофициальный перевод), этот документ получил название «Конвенция о преступности в сфере компьютерной информации», но в российской доктрине, в деловой лексике и проч. эта конвенция часто называется «Конвенцией о киберпреступности»[8]. Смысловые, содержательные различия употребления термина кибербезопасность, несомненно зависят от вариантов его перевода. Например, «*cybersecurity*» с английского языка на русский язык буквально переводится как «кибербезопасность», но в силу определённой политической мотивации переводиться, к примеру, как «информационная безопасность» или даже «безопасность применения информационных технологий». В качестве примера можно обратиться к такому документу как «Правила поведения в области обеспечения международной информационной безопасности», и получивший название Кодекс информационной безопасности, предложенный к рассмотрению на 66-й сессии Генеральной Ассамблеи ООН в 2011 году Китаем, Россией, Таджикистаном и Узбекистаном[9]. Еще одним примером является «Конвенция о международной информационной безопасности (концепция)», подготовленной Российской Федерацией в 2011 году и предложенной для обсуждения в рамках ООН[10].

Новизна и сложность регламентации отношений, связанных с интернетом, влияет на согласование публичных интересов государств в сфере управления интернетом, а кибербезопасность сети становится в настоящее время доминирующим контекстом обсуждения и ключевым вопросом управления интернетом. Вероятно, что это может быть связано контекстом обсуждения проблематики управления интернетом развернувшейся в начале 2000-х годов, выявившей два подхода. Узкий подход, *strictusensu,* ограничивал управление интернетом технико-организационными вопросами построения сети, сетевой адресации и нумерации, основами кибербезопасности. Широкий подход, *sensulato*, исходил из необходимости включения в «управление интернетом» различные общественно-политические и социально-экономические вопросы, включая принципы коммутации международных сетей электросвязи, монетизацию и обеспечение «более сбалансированных» денежных потоков за пропуск сетевого трафика и проч. Проблематика управления интернетом при таком широком подходе, фактически совпадает с проблематикой «построения информационного общества»

[8] См. Информационная система «Консультант плюс».

[9] См. текст Резолюции A66/356. – URL: http://inosmi.ru/russia/20110913/174603156.html

[10] URL: http://www.scrf.gov.ru/documents/6/112.html

DOI: 10.7256/2226-6305.2014.1.11411
При цитировании этой статьи сноска на doi обязательна

впервые обозначенной на международном уровне в Окинавской хартии глобального информационного общества группы стран «Большой восьмёрки» 2000 году[11].

2013 год может, по-видимому, стать неким новым этапом решения вопроса о применимости международного публичного права к интернету. По странной иронии применимость международного публичного права получила «системную аналитику» в контексте «военной киберугрозы». В 2013 году было опубликовано «Таллиннское руководство по международному праву, применимому в случае кибервойны» (*Tallinn Manualon The International Law Applicableto Cyber Warfare*), далее – «Таллиннское руководство»[12]. Таллиннское руководство совершенно неправомерно, на наш взгляд, ряд аналитиков называют руководством по ведению кибервойн, «легитемизацией милитаризации» киберпространства, правовыми основами ведения кибервойны и т. д.[13]

Представляется важным обратить внимание на то, что Таллиннское руководство является итогом трехлетней работы международной группы экспертов, приглашенных Центром передового опыта НАТО по совместной защите от киберугроз (*The NATO Cooperative Cyber Defence Center of Excellence*), г. Таллинн (Эстония)[14]. Соответственно Таллиннское руководство нельзя рассматривать как официальный документ ни Центра передового опыта НАТО по совместной защите от киберугроз НАТО, ни государств-членов, спонсировавших это исследование, ни НАТО, ни организаций или государств, имеющих статус наблюдателей НАТО. Таллиннское руководство – выражает точку зрения международной группы независимых экспертов, действующих исключительно в личном качестве и является своеобразным подтверждением того, что практические шаги в вопросах управления интернетом на международно-правовом уровне невозможно решать без «участия всех заинтересованных сторон», в данном случае – «экспертного сообщества»,.

Таллиннской руководство представляет собой обширный документ (более 340 страниц), а обращение к нему в рамках настоящей статьи вызвано несколькими причинами. Во-первых, кибербезопасность важна не сама по себе, и ее нельзя рассматривать вне контекста управления интернетом в целом и формирования международной модели управления интернетом, в частности. Иной подход понимания кибербезопасности может привести, как минимум, к полицентризму и фрагментации интернета рамками национальной юрисдикции государств, может разрушить глобальную сеть, став препятствием трансграничного функционирования интернета, а также к доминированию государств в мультистейкхолдерской модели управления интернетом. Во-вторых, Таллиннское руководство подготовлено на целом ряде нормативно-правовых источников: международные договоры, документы международных межправительственных организаций, решения (прецеденты) международных трибуналов и судов, обычаи и принципы международного права. Использованные источники приведены в самом начале Таллиннского руководства, а вся нормативная и правовая база призвана ответить на основной вопрос: применимы ли нормы современного международного права,

[11] См. *М.Б. Касенова, М.В. Якушев* Управление интернетом. Документы и материалы. СПб., 2013. С.323-329

[12] URL: www. Cambridge.org/9781107024434. Центр передового опыта НАТО по совместной защите от киберугроз (The NATO Cooperative Cyber Defence Center of Excellence), г. Таллинн (Эстония).

[13] См. например, материалы – URL: http://www.3dnews.ru/643092; URL: http://www.securitylab.ru/blog/personal/tsarev/29130.php и др. Взвешенная оценка документа дана А. Лукацким, URL: http://lukatsky.blogspot.ru/2013/05/blog-post.html

[14] Центр передового опыта НАТО по совместной защите от киберугроз (The NATO Cooperative Cyber Defence Center of Excellence, CCDCOE), называемый иногда – Объединенный центр передового опыта в сфере кибернетической защиты, создан в 2008 году в г. Таллинне (Эстония) в целях повышения эффективности взаимодействия стран НАТО и расширения их возможностей в сфере кибербезопасности, аккредитован при НАТО и имеет статус международной военной организации. В его компетенцию входит предоставление экспертных заключений по вопросам совместной кибернетической и информационной безопасности для НАТО и стран-членов НАТО.

DOI: 10.7256/2226-6305.2014.1.11411
При цитировании этой статьи сноска на doi обязательна

как обычные, так и конвенционные, к новым киберугрозам, киберконфликтам, кибервойнам, и если применимы, то каким образом. В самом общем плане Таллиннское руководство положительно отвечает на этот вопрос и формулирует правила, применимые в условиях киберконфликтов[15].Положительный ответ на вопрос применимости международного права к киберпространству, данный в Таллиннском руководстве, имеет важное значение и в связи с особенностью формирования принципов и норм международного права. Поэтому, в-третьих, следует сказать о принципе *opiniojuris*. *Убежденность в правомерности* (*opiniojuris*) для международного права – убеждение субъектов международного права в юридической полноценности (действительности) нормы права, означающее признание государством определенного правила в качестве нормы международного права – обычной или конвенционной. Любая норма международного права, независимо от ее источника и применяемой процедуры, проходит стадию выработки содержания правила, а затем стадию признания этого правила в качестве обязательной нормы международного права. При создании конвенционных норм *opiniojuris* имеет явно выраженный характер, а при квалификации обычных норм в качестве норм обычного международного права– молчаливый характер. Отсюда следует, что при квалификации норм обычного международного права – доказательство *opiniojuris* непосредственно связывается с кодификацией международного обычного права, в процессе которой *opiniojuris* получает явно выраженный характер[16]. Таллиннское руководство следует рассматривать именно в контексте «стремления к нормативной определенности» применимости нормы современного международного права к «киберугрозам».

Структурно Таллиннское руководство состоит из двух основных частей и закрепляет 95 правил (*Rules*): часть А – «Международное право кибербезопасности» (*International Cyber Security Law*), которая включает две главы, в пяти разделах которых сформулировано 19 правил; часть В – «Право киберконфликтов» (*The Law of Cyberarmed Conflict*), состоящая из 5 глав, в 7 разделов которых включено 76 правил. Таллиннское руководство формулирует конкретное правило (норму), содержание которого разъясняется в соответствующих комментариях, включая интерпретацию применимости правил, с указанием на существовавшие разногласия, возникшие среди экспертов по тому или иному правилу.

Приведем в качестве примера правило 1, изложенное в разделе 1 «Суверенитет, юрисдикция и контроль», главы 1 «Государство и киберпространство». Правило 1 «Суверенитет». *Государство может осуществлять контроль над киберинфраструктурой и за деятельностью в рамках своей суверенной территории.* В последующих 14 пунктах раскрывается содержания указанного правила и даются, к примеру, следующие комментарии: «Несмотря на то, что ни одно государство не обладает суверенитетом над киберпространством как таковым (*perse*), государство обладает исключительными суверенными правами над объектами киберинфраструктуры, находящимися на его территории. Государственный суверенитет над киберинфраструктурой в пределах суверенной территории означает то, что, во-первых, государство осуществляет нормативно-правовой контроль над объектами киберинфртаструктуры; во-вторых, государство осуществляет территориально-суверенную защиту объектов киберинфраструктуры. При этом такой контроль и защита осуществляется вне зависимости от того принадлежат ли такие объекты самому государству, частным организациям или индивидам, и вне зависимости от целей использования таких объектов». Основной единодушный вывод, сделанный группой экспертов, в Таллиннском руководстве (части А – «Международное право

[15] URL: www. Cambridge.org/9781107024434. Центр передового опыта НАТО по совместной защите от киберугроз (The NATO Cooperative Cyber Defence Center of Excellence), г. Таллинн (Эстония).

[16] См., например, URL: http://mirslovarei.com/content_eco/opinio-juris-49850.html#ixzz2YSq1YaOd

DOI: 10.7256/2226-6305.2014.1.11411
При цитировании этой статьи сноска на doi обязательна

кибербезопасности») – общие принципы и нормы международного права применимы к регулированию киберпространства.

В настоящее время довольно сложно предположить каким образом будет развиваться международное сотрудничество государств в сфере управления интернетом. Развитие общественных отношений в сфере информационных и коммуникационных отношений опережают их правовое регулирование и не исключено, что выявятся и иные вопросы развития информационных технологий, которые потребуют международно-регулирования, но любые вопросы в указанной сфере так или иначе будут связаны с необходимостью международно-правового сотрудничества в трансграничном управлении интернетом.

Библиография:

1. М.Б. Касенова, М.В. Якушев Управление интернетом. Документы и материалы. СПб., 2013. С.323-329
2. Касенова М.Б. Управление интернетом. Международно-правовой механизм. СПб., 2012. С. 13-20
3. И.Л. Андреев, Л.Н. Назарова. Интернет: когда слуга становится господином // Психология и Психотехника. – 2013. – № 5. – С. 104-107. DOI: 10.7256/2070-8955.2013.5.7930.
4. Будагова М.М.. Способы приобретения прав на доменное имя. // Право и политика. – 2014. – № 1. – С. 104-107. DOI: 10.7256/1811-9018.2014.1.10363.
5. Теленьга М.П.. Цифровая дипломатия (digital diplomacy) как дополнительный политический ресурс международных отношений // Международные отношения. – 2014. – № 1. – С. 104-107. DOI: 10.7256/2305-560X.2014.1.10059.
6. И.В. Сурма. Новый глобальный наднациональный актор международных отношений в контексте национальной безопасности // Национальная безопасность / nota bene. – 2013. – № 1. – С. 104-107. DOI: 10.7256/2073-8560.2013.01.7.
7. Д.К. Чирков, А.Ж. Саркисян. Преступность в сфере высоких технологий: тенденции и перспективы // Национальная безопасность / nota bene. – 2013. – № 1. – С. 104-107. DOI: 10.7256/2073-8560.2013.01.3.
8. С.А. Бахтин. Интернет-экономика – новый вызов национальной экономической безопасности: общая характеристика // Национальная безопасность / nota bene. – 2012. – № 6. – С. 104-107.
9. Ван Ши Лу. Проблема Интернет-зависимости в Китае: психология, культура, политика // Психология и Психотехника. – 2012. – № 12. – С. 104-107.
10. М.И. Бения. Восстание машин, или Человек и ковш // Психология и Психотехника. – 2012. – № 12. – С. 104-107.
11. С.С. Станчик. Роль интернета в современных переворотах // Национальная безопасность / nota bene. – 2012. – № 5. – С. 104-107.
12. М. В. Шугуров. «Группа восьми» (G8) и дилеммы глобального управления Интернетом: международно-правовой аспект // Право и политика. – 2012. – № 6. – С. 104-107.
13. Г. Л. Акопов. Политико-правовые угрозы распространения социально ориентированных интернет-технологий // Национальная безопасность / nota bene. – 2012. – № 2. – С. 104-107.
14. Г. Л. Акопов. Политическая интернет-модернизация: некоторые теоретические предпосылки к исследованию // Политика и Общество. – 2011. – № 8. – С. 104-107.
15. З. А. Расулов. Информационные технологии и факторы их эффективности в процессе регулирования политических отношений // Право и политика. – 2011. – № 7. – С. 104-107.
16. И. А. Бронников. Интернет как ресурс политической власти // Право и политика. – 2011. – № 6.

17. Г. Л. Акопов. Сеть «Интернет» – коммуникативное пространство для политического дискурса // Право и политика. – 2011. – № 5.
18. М. В. Шугуров. Совет Европы и информационно-коммуникационные технологии (ICT): реализация прав человека в информационном обществе. // Международное право и международные организации / International Law and International Organizations. – 2010. – № 4
19. М.В. Шугуров The tensions between international human right to freedom of expression and copyright in digital age: perspectives of theirs coinciding in the context of international law // Международное право и международные организации / International Law and International Organizations. – 2012. – 4. – С. 6 – 23.
20. Акопов Г.Л. Интернет-модернизация политической системы – базис для формирования информационного общества // NB: Проблемы общества и политики. – 2012. – 2. – С. 55 – 63. URL: http://www.e-notabene.ru/pr/article_180.html
21. Г. П. Жуков Создание и развитие международной системы и организации космической связи «Интерспутник». К сорокалетней годовщине // Международное право и международные организации / International Law and International Organizations. – 2012. – 1. – С. 6 – 9.

References (transliteration):

1. M.B. Kasenova, M.V. Yakushev Upravlenie internetom. Dokumenty i materialy. SPb., 2013. S.323-329
2. Kasenova M.B. Upravlenie internetom. Mezhdunarodno-pravovoi mekhanizm. SPb., 2012. S. 13-20
3. I.L. Andreev, L.N. Nazarova. Internet: kogda sluga stanovitsya gospodinom // Psikhologiya i Psikhotekhnika. – 2013. – № 5. – S. 104-107. DOI: 10.7256/2070-8955.2013.5.7930.
4. Budagova M.M.. Sposoby priobreteniya prav na domennoe imya. // Pravo i politika. – 2014. – № 1. – S. 104-107. DOI: 10.7256/1811-9018.2014.1.10363.
5. Telen'ga M.P.. Tsifrovaya diplomatiya (digital diplomacy) kak dopolnitel'nyi politicheskii resurs mezhdunarodnykh otnoshenii // Mezhdunarodnye otnosheniya. – 2014. – № 1. – S. 104-107. DOI: 10.7256/2305-560X.2014.1.10059.
6. I.V. Surma. Novyi global'nyi nadnatsional'nyi aktor mezhdunarodnykh otnoshenii v kontekste natsional'noi bezopasnosti // Natsional'naya bezopasnost' / nota bene. – 2013. – № 1. – S. 104-107. DOI: 10.7256/2073-8560.2013.01.7.
7. D.K. Chirkov, A.Zh. Sarkisyan. Prestupnost' v sfere vysokikh tekhnologii: tendentsii i perspektivy // Natsional'naya bezopasnost' / nota bene. – 2013. – № 1. – S. 104-107. DOI: 10.7256/2073-8560.2013.01.3.
8. S.A. Bakhtin. Internet-ekonomika – novyi vyzov natsional'noi ekonomicheskoi bezopasnosti: obshchaya kharakteristika // Natsional'naya bezopasnost' / nota bene. – 2012. – № 6. – S. 104-107.
9. Van Shi Lu. Problema Internet-zavisimosti v Kitae: psikhologiya, kul'tura, politika // Psikhologiya i Psikhotekhnika. – 2012. – № 12. – S. 104-107.
10. M.I. Beniya. Vosstanie mashin, ili Chelovek i kovsh // Psikhologiya i Psikhotekhnika. – 2012. – № 12. – S. 104-107.
11. S.S. Stanchik. Rol' interneta v sovremennykh perevorotakh // Natsional'naya bezopasnost' / nota bene. – 2012. – № 5. – S. 104-107.
12. M. V. Shugurov. «Gruppa vos'mi» (G8) i dilemmy global'nogo upravleniya Internetom: mezhdunarodno-pravovoi aspekt // Pravo i politika. – 2012. – № 6. – S. 104-107.
13. G. L. Akopov. Politiko-pravovye ugrozy rasprostraneniya sotsial'no orientirovannykh internet-tekhnologii // Natsional'naya bezopasnost' / nota bene. – 2012. – № 2. – S. 104-107.

DOI: 10.7256/2226-6305.2014.1.11411
При цитировании этой статьи сноска на doi обязательна

14. G. L. Akopov. Politicheskaya internet-modernizatsiya: nekotorye teoreticheskie predposylki k issledovaniyu // Politika i Obshchestvo. – 2011. – № 8. – S. 104-107.
15. Z. A. Rasulov. Informatsionnye tekhnologii i faktory ikh effektivnosti v protsesse regulirovaniya politicheskikh otnoshenii // Pravo i politika. – 2011. – № 7. – S. 104-107.
16. I. A. Bronnikov. Internet kak resurs politicheskoi vlasti // Pravo i politika. – 2011. – № 6.
17. G. L. Akopov. Set' «Internet» – kommunikativnoe prostranstvo dlya politicheskogo diskursa // Pravo i politika. – 2011. – № 5.
18. M. V. Shugurov. Sovet Evropy i informatsionno-kommunikatsionnye tekhnologii (ICT): realizatsiya prav cheloveka v informatsionnom obshchestve. // Mezhdunarodnoe pravo i mezhdunarodnye organizatsii / International Law and International Organizations. – 2010. – № 4
19. M.V. Shugurov The tensions between international human right to freedom of expression and copyright in digital age: perspectives of theirs coinciding in the context of international law // Mezhdunarodnoe pravo i mezhdunarodnye organizatsii / International Law and International Organizations. – 2012. – 4. – C. 6 – 23.
20. Akopov G.L. Internet-modernizatsiya politicheskoi sistemy – bazis dlya formirovaniya informatsionnogo obshchestva // NB: Problemy obshchestva i politiki. – 2012. – 2. – C. 55 – 63. URL: http://www.e-notabene.ru/pr/article_180.html
21. G. P. Zhukov Sozdanie i razvitie mezhdunarodnoi sistemy i organizatsii kosmicheskoi svyazi «Intersputnik». K sorokaletnei godovshchine // Mezhdunarodnoe pravo i mezhdunarodnye organizatsii / International Law and International Organizations. – 2012. – 1. – C. 6 – 9.