Проблема правового регулирования международной информационной и кибербезопасности в современной мировой политике

Столетов О. В.,
кандидат политических наук,
старший преподаватель факультета политологии
МГУ им. М. В. Ломоносова
E-mail: Oleg-Stoletov1@yandex.ru

Аннотация. *В статье анализируются подходы США, России, Китая, Индии и Бразилии к проблеме правового регулирования международной информационной и кибербезопасности. Автор рассматривает позиции государств по отношению к основным принципам существующих международных документов в области информационной и кибербезопасности, анализирует новые инициативы в области выработки международных политико-правовых решений в данной сфере, а также исследует актуальную практику политического регулирования данной сферы на национально-государственном уровне. Автор приходит к выводу, что выработка общих принципов политико-правового регулирования сферы международной информационной и кибербезопасности становится насущной потребностью политики глобальной безопасности.*

Ключевые слова*: информационная безопасность, кибербезопасность, правое регулирование, информационный суверенитет, глобальная политика.*

Участие государств в обеспечении международной информационной и кибербезопасности в современном мире представляет огромную важность в силу той роли, которую информация играет в современной мировой политике[1]. В последние несколько лет наблюдалось все большее смещение сферы информационных и киберкоммуникаций в поле международной конфликтности. Взаимные обвинения государств в использовании информационных и кибернетических технологий для осуществления слежки, вмешательства во внутреннюю политику друг друга становятся все более частыми и политизированными. Кроме того, в прошедшие двадцать лет международное сообщество столкнулось с появлением целого ряда группировок киберхакеров, целенаправленно занимающихся взломом компьютерных систем по политическим, социальным или религиозным мотивам, и получивших значительную известность благодаря успешности своих операций[2]. К числу такого рода группировок относятся движение «Anonimous», «Альянс красных хакеров», «Модный медведь», «Объединенный Киберхалифат», «Теневые брокеры», «КиберБеркут», «КиберХунта» и ряд др. Подобная динамика делает вопросы о праве на свободное распространение информации, порядке обеспечении защиты информации, границах использования и возможности милитаризации новых сегментов информационного пространства крайне существенными для поддержания глобальной устойчивости. В этих условиях представляется важным рассмотреть подходы таких влиятельных государств мира как США, Россия, Китай, Индия и Бразилия к проблеме международно-правового регулирования международной информационной и кибербезопасности.

Принцип свободы распространения информации в сети Интернет наиболее активно внедряется США. Значительную поддержку правительству Соединенных Штатов в данном вопросе оказывают ведущие транснациональные корпорации, имеющие США в качестве страны происхождения. Например, в октябре 2008 г. крупнейшие интернет-корпорации Yahoo!, Microsoft

[1] Понятие международной информационной безопасности зафиксировано ООН и предполагает защищенность глобальной информационной системы от трех типов угроз: террористических, преступных и военно-политических.

[2] Вихул Л. Стремление к передовому опыту в киберсфере // Per Concordiam. 2014. Т. 5. № 2. С. 10-19; http://www.marshallcenter.org/MCPUBLICWEB/mcdocs/files/College/F_Publications/perConcordiam/pC_V5N2_ru.pdf (дата обращения: 28.12.2017).

и Google создали некоммерческую организацию Глобальная сетевая инициатива (ГСИ), миссия которой состоит в защите и развитии свободы выражения мнений и неприкосновенности частной жизни в информационно-коммуникационных технологиях[3]. Проекцией принципа глобальной проницаемости кибепространства на сферу международного противодействия киберпреступности стала Конвенция о компьютерных преступлениях Совета Европы (Будапештская конвенция), принятая в 2001 г. и вступившая в силу в 2004 г. Этот документ США ратифицировали в 2006 г.[4] Наряду с Соединенными Штатами документ подписали все страны-члены Совета Европы, за исключением России[5]. Особенностью Конвенции является ее статья 32, предусматривающая возможность «трансграничного доступа» одной стороны к компьютерным данным независимо от их географического местоположения без согласия другой стороны[6].

Показательно, что, декларируя принцип свободы распространения информации, Соединенные Штаты проводят политику, направленную на установление все более жесткого контроля за информацией иностранного происхождения внутри страны. В ноябре 2017 г. американский филиал российского телеканала Russia Today был вынужден зарегистрироваться в качестве иностранного агента в Министерстве юстиции США, согласившись с условиями дополнительного надзора за своей работой[7]. Альтернативой данному решению была бы приостановка деятельности канала на территории страны[8].

Соединенные Штаты Америки являются страной, которая одна из первых начала осуществлять стратегическое планирование в сфере кибербезопасности. Первая национальная доктринальная инициатива, определявшая необходимость координации различных государственных ведомств в сфере защиты национального информационного пространства, была утверждена в США в феврале 2003 г.[9] Стратегия национальной безопасности США 2010 г. впервые официально включает киберпространство в потенциальное поле войны. В специализированных доктринальных документах, принятых позднее, линия на милитаризацию киберпространства была продолжена[10]. В 2009 г. в США были созданы Кибернетическое командование (USCYBERCOM) вооруженных сил США и Национальный центр кибербезопасности и интеграции коммуникаций министерства внутренней безопасности США[11]. После широкого распространения в глобальном информационном пространстве обвинений со стороны ведущих спецслужб США во вмешательстве российских хакеров в кампанию по выборам президента Соединенных Штатов 2016 г. избранный президент Д. Трамп подписал указ об укреплении кибербезопасности правительственных структур США[12]. Необходимо отметить, однако, что задолго до обозначенных выше политических решений в американской системе национальной безопасности существовало Агентство национальной безопасности (АНБ), основанное еще в 1952 г. В 2013 г. из разоблачений WikiLeaks и бывшего сотрудника АНБ

[3] Лексютина Я.В. Свобода Интернета в современном дискурсе американо-китайских отношений // Общество. Среда. Развитие (Terra Humana). 2011. № 1; http://www.terrahumana.ru/arhiv/11_01/11_01_20.pdf (дата обращения: 26.12.2017); Вихул Л. Стремление к передовому опыту в киберсфере // Per Concordiam. 2014. Т. 5. № 2. С. 10-19; http://www.marshallcenter.org/MCPUBLICWEB/mcdocs/files/College/F_Publications/perConcordiam/pC_V5N2_ru.pdf (дата обращения: 28.12.2017).
Лексютина Я.В. Свобода Интернета в современном дискурсе американо-китайских отношений // Общество. Среда. Развитие (Terra 2017).

[4] Buchanan M. November 23, 2001, U.S. Signs «Convention on cybercrime» Treaty — Today in crime history // Blog and news, http://reasonabledoubt.org/criminallawblog/entry/november-23-2001-us-signs-convention-on-cybercrime-joined-by-29-other-countries-today-in-crime-history (дата обращения: 26.12.2017).

[5] МИД РФ предложил изменить правила борьбы с мировой киберпреступностью // Интерфакс, 14.04.2017; http://www.interfax.ru/russia/558389 (дата обращения: 28.12.2017).

[6] Конвенция о компьютерных преступлениях // Совет Европы, 23.11.2001; https://rm.coe.int/1680081580 (дата обращения: 26.12.2017).

[7] RT зарегистрировался в качестве иностранного агента в США // РГ. 2017. 13 нояб.; https://www.rg.ru/2017/11/13/rt-zaregistrirovalsia-v-kachestve-inostrannogo-agenta-v-ssha.html (дата обращения: 29.12.2017).

[8] Американский филиал RT зарегистрировался в США в качестве иностранного агента // ИТАР-ТАСС, 13.11.2017; http://tass.ru/obschestvo/4724977 (дата обращения: 29.12.2017).

[9] Корсаков Г.Б. Информационное оружие супердержавы: кибервойна и «управляемые кризисы» // Военно-политическое обозрение, 04.05.2012; http://www.belvpo.com/ru/10497.html (дата обращения: 26.12.2017).

[10] Демидов О.В. Обеспечение международной информационной безопасности и российские национальные интересы // Индекс безопасности. 2011. Т. 19. № 1(104). С. 129—168; URL: http://pircenter.org/media/content/files/10/13559089230.pdf (дата обращения: 27.12.2017).

[11] В Германии создают правительственный центр кибербезопасности // BaltInfo, 24.02.2011; http://www.baltinfo.ru/2011/02/24/V-Germanii-sozdayut-pravitelstvennyi-tcentr-kiberbezopasnosti-189865 (дата обращения: 27.12.2017).

[12] Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure // Office of the Press Secretary. 11.05.2017; https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal (дата обращения: 27.12.2017).

Э. Сноудена стало известно о том, что АНБ в рамках своей секретной программы на протяжении ряда лет вело нелегальную электронную слежку за интернет-активностью пользователей внутри США и за рубежом, в европейских и азиатских государствах, являющихся политическими партнерами США. Согласно рассекреченным документам объектами электронной слежки становились не только рядовые граждане, но и руководство зарубежных государств[13]. Данные слежки получили глобальную известность благодаря публикациям в ведущих изданиях ряда европейских государств. В июне 2013 г. немецкий журнал «Spiegel» опубликовал информацию об электронном шпионаже, осуществляемом АНБ в административных зданиях Европейского Союза в США и в самой Европе[14]. В июле 2013 г. британское издание «Guardian» сообщило, что АНБ вели наблюдение за электронными коммуникациями 38 иностранных посольств и дипломатических миссий, находящихся на территории Соединенных Штатов[15]. В числе объектов слежки оказались, в частности, представительства ЕС, Франции, Италии, Греции, Японии, Мексики, Южной Кореи, Индии и Турции[16]. В январе 2015 г. «Spiegel» обнародовал ряд новых документов из архива Э. Сноудена, свидетельствующих о том, что глобальная слежка спецслужб США за пользователями Интернета являлась лишь первой стадией американской военной киберстратегии, следующей должна была стать разработка и внедрение вредоносных программ, позволяющих вывести из строя объекты критически важной инфраструктуры противника, включая банковскую систему, электро- и водоснабжение, заводы и аэропорты[17]. В соответствии со сведениями, опубликованными Э. Сноуденом в июле 2016 г., Правительство США санкционировало хакерские атаки на ряд зарубежных политических партий и организаций, в числе которых находились Народная партия Пакистана, ливанское шиитское движение «Амаль», египетская партия «Братья-мусульмане», Индийская народная партия «Бхаратия Джаната» и румынский «Фронт национального спасения»[18]. Международный скандал вокруг электронного шпионажа, получивший широкую огласку, способствовал общему росту недоверия к Соединёнными Штатам в мире. Представляется, что проявившееся впоследствии последовательное стремление США переключить международное внимание на киберугрозу, исходящую от России, было направлено, в частности, на выведение себя самих из-под критики.

Оппонентом США в вопросе о принципах правового регулирования международной информационной и кибербезопасности выступает Россия, еще в 2011 г. выдвинувшая проект конвенции ООН об обеспечении международной информационной безопасности[19], который, однако, не был утвержден официально. Следует отметить, что Россия выдвигала международные инициативы в области обеспечения информационной безопасности и ранее — уже с 1998 г., однако не находила достаточной дипломатической поддержки для того, чтобы создать на глобальном уровне системную политико-правовую рамку, обеспечивающую выработку работающих механизмов регулирования развития данной сферы[20]. В проекте 2011 г. в числе основных угроз международному миру и безопасности в информационном пространстве было названо, в частности, «трансграничное распространение информации, противоречащей принципам и нормам международного права, а также национальным законодательствам государств»[21]. В целях создания и поддержания атмосферы доверия в информационном пространстве документ постулировал необходимость соблюдать принцип

[13] Президент Бразилии отменила госвизит в США // BBC Русская служба, 18.09.2013; http://www.bbc.com/russian/international/2013/09/130917_brazil_calls_off_us_visit (дата обращения: 27.12.2017).

[14] Как спецслужбы США собирают информацию? // BBC Русская служба, 31.10.2013; http://www.bbc.com/russian/international/2013/10/131030_spy_leaks_process (дата обращения: 27.12.2017).

[15] Союзники США обиделись на «большого брата» за электронный шпионаж // Россия сегодня, 15.07.2017; https://ria.ru/world/20130701/946870739.html (дата обращения: 28.12.2017).

[16] Пан Ги Мун призвал обеспечить неприкосновенность дипмиссий // Россия сегодня, 01.07.2013; https://ria.ru/world/20130701/946905338.html?ria=fn3umvgovpfgnm916acfclg85ipmme33 (дата обращения: 28.12.2017).

[17] Эдвард Сноуден дошел до второй стадии // Коммерсант.ru, 19.01.2015; https://www.kommersant.ru/doc/2649343 (дата обращения: 28.12.2017).

[18] Сноуден опубликовал секретный доклад о кибератаках США на зарубежные партии // Россия сегодня, 25.07.2016; https://ria.ru/world/20160725/1472831959.html (дата обращения: 28.12.2017).

[19] Конвенция об обеспечении международной информационной безопасности (концепция) // МИД РФ, 22.09.2011; http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666 (дата обращения: 28.12.2017).

[20] Бедрицкий А.В. Международные договоренности по киберпространству: возможен ли консенсус? // Проблемы национальной стратегии. 2012. № 4(13). С. 119-136; https://riss.ru/images/pdf/journal/2012/4/10.pdf (дата обращения: 28.12.2017).

[21] Конвенция об обеспечении международной информационной безопасности (концепция) // МИД РФ, 22.09.2011; http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666 (дата обращения: 28.12.2017).

информационного суверенитета — сохранение контроля государства над своим информационным пространством[22]. Впоследствии, в ходе обсуждения вопросов управления информационным пространством в Дубае на конференции Международного союза электросвязи (МСЭ) в декабре 2012 г. Россия указала на фактическую монополию управления Интернетом, которой обладает частная компания ICANN (Internet Corporation for Assigned Names and Numbers), базирующаяся на территории США[23]. Компания ICANN осуществляет распределение и регистрацию доменных имен, обеспечивает беспрепятственный доступ к ним всех пользователей сети Интернет. ICANN находится под юрисдикцией Соединенных Штатов. Позицию России, касающуюся передачи функций ICANN наднациональному органу под эгидой ООН, поддерживают Китай, Бразилия и Индия, многие развивающиеся страны «Группы-77»[24].

В июле 2016 г. в ходе XV Совещания руководителей специальных служб, органов безопасности и правоохранительных органов иностранных государств Россия впервые презентовала российский проект универсальной конвенции о сотрудничестве в сфере противодействия информационной преступности[25]. В мае 2017 г. данный проект был представлен на рассмотрение членами ООН в венской штаб-квартире организации[26]. Документ позиционируется как альтернатива упоминавшейся выше Будапештской конвенции, от подписания которой Россия ранее отказалась[27], и призван «содействовать принятию и укреплению мер, направленных на эффективное предупреждение преступлений и иных противоправных деяний в сфере информационно-коммуникационных технологий (ИКТ) и борьбу с ними»[28]. Кроме того, Россия предлагает на международном уровне выработать правила ответственного поведения государств в информационном пространстве, закрепляющие принципы уважения государственного суверенитета, невмешательства во внутренние дела других государств, основных прав и свобод человека, а также равные права для всех государств на участие в управлении сетью Интернет[29].

Выступая с представленными выше международными инициативами, Россия стремится не только продемонстрировать свою готовность к предметному международному обсуждению вопросов регулирования сферы информационной и кибербезопасности, но и позиционировать свою нацеленность на «демилитаризацию» информационно-кибернетического пространства. Со своей стороны Россия, в том числе на уровне ОДКБ, ШОС, ООН, выдвигает концепцию предотвращения конфликтов в информационной сфере и неприменения государствами силы в информационном пространстве. Тем не менее, на данном этапе эти инициативы не находят поддержки у Соединенных Штатов, которые активно политизируют угрозы кибербезопасности и информационной безопасности.

В условиях неготовности США и их партнеров активизировать международный диалог по нахождению приемлемых способов регулирования сферы информационной и кибербезопасности, руководство России прилагает активные усилия по созданию системы кибербезопасности на национальном и региональном уровнях. В апреле 2011 г. Правительственная комиссия по высоким технологиям и инновациям одобрила разработку национальной операционной системы[30]. В январе 2013 г. ФСБ России было поручено создание государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на российские

[22] Новацкий А. Борьба вокруг проекта Конвенции ООН о международной информационной безопасности // Международная жизнь: электрон. версия газ. 17.07.2012; http://interaffairs.ru/print.php?item=8614 (дата обращения: 25.12.2017).

[23] Черненко Е. Россия выступит за интернационализацию Интернета // Коммерсант.ru: электрон. версия газ. 03.12.2012; http://www.kommersant.ru/doc/2081615 (дата обращения: 25.12.2017).

[24] Зиновьева Е.С. Российские интересы в сфере управления Интернетом // Международные процессы. 2009. № 1. С. 101-108; http://www.intertrends.ru/nineteenth/010.htm (дата обращения: 25.12.2017).

[25] О презентации российского проекта универсальной конвенции о сотрудничестве в сфере противодействия информационной преступности // МИД РФ, 28.07.2016; http://www.mid.ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2375819 (дата обращения: 25.12.2017).

[26] Россия представила проект конвенции ООН о борьбе с киберпреступностью // Россия сегодня, 24.05.2017; https://ria.ru/world/20170524/1495007020.html (дата обращения: 25.12.2017).

[27] По мнению России, статья о «трансграничном доступе» создает возможность для спецслужб различных государств без официального уведомления проводить операции в компьютерных сетях третьих стран, что представляет угрозу национальной безопасности и суверенитету.

[28] МИД РФ предложил изменить правила борьбы с мировой киберпреступностью // Интерфакс, 14.04.2017; http://www.interfax.ru/russia/558389 (дата обращения: 25.12.2017).

[29] Выступление Первого заместителя Постоянного представителя РФ при ООН П.В. Ильичева на заседании Совета Безопасности ООН по «формуле Арриа» по кибербезопасности // Постоянное представительство Российской Федерации при ООН, 28.11.2016; http://russiaun.ru/ru/news/sc_csa (дата обращения: 25.12.2017).

[30] Правительство РФ одобрило разработку национальной ОС // Лента.ру, 06.04.2011; http://lenta.ru/news/2011/04/06/npp/ (дата обращения: 24.12.2017).

информационные ресурсы. В мае 2014 г. в составе Министерства обороны РФ появилась новая структура — войска информационных операций. Об активизации российской политики в сфере кибербезопасности говорит проведение учений, направленных на выработку мер по предотвращению нарушений работы сети Интернет на территории России[31]. Россия поддерживает стремление государств-партнеров к развитию взаимодействия в сфере кибербезопасности на региональном уровне. При ее участии было принято решение о создании центра кибербезопасности и кризисного реагирования ОДКБ[32].

В условиях отсутствия на международном уровне легитимной системы информационной и кибербезопасности КНР, Индия и Бразилия ведут самостоятельную работу по созданию механизмов защиты национальных сегментов информационно-кибернетического пространства.

Китай начал разработку программной платформы для национальной операционной системы «Kylin» еще в 2001 г.[33] К 2009 г. национальная операционная система такого рода была разработана. В КНР с 2000 г. функционирует собственная поисковая система «Baidu». На сегодня она занимает 1 место в Китае, 8 в Северной Корее, 10 в Гонконге, 15 в Японии, 27 на Тайване и 82 в США. Поисковик Baidu имеет такую же популярность в КНР, как Google в Европе. В середине 2006 г. главный поисковик Китая запустил проект «Байдупедия» или «Байду Байке». На начало 2017 г. там содержалось около 14 млн статей. Иными словами, в Байдупедии больше информации, чем в русской, английской, китайской и немецкой Википедии вместе взятых[34]. Китай активно развивает военный сектор кибертехнологий, руководствуясь концептуальным документом Народно-освободительной армии Китая «Комплексное использование кибернетических и радиоэлектронных средств ведения войны». В июле 2010 г. генеральный штаб НОАК объявил о создании первой военной базы кибероперацій[35]. Параллельно с развитием национальной инфраструктуры информационной безопасности КНР активизирует деятельность по налаживанию международной кооперации в этой сфере. Двусторонний меморандум между Россией и Китаем, направленный на обеспечение безопасности национальных сегментов Интернета и национальных доменов двух стран, был подписан регистраторами национальных доменов России и Китая 21.11.2014[36]. Впоследствии, в ходе российско-китайских переговоров на высшем уровне, прошедших в июле 2017 г. в Кремле, страны подписали Меморандум о намерениях по взаимодействию в области развития информационного пространства[37]. Кроме того, в 2014 г. КНР впервые провел трехсторонние переговоры по укреплению доверия и сотрудничеству в киберпространстве с Японией и Южной Кореей[38].

В апреле 2015 г. между Правительствами КНР и России было заключено Соглашение о сотрудничестве в области обеспечения международной информационной безопасности. В документе определены направления межгосударственного сотрудничества в области противодействия таким угрозам как использование информационно-коммуникационных технологий для осуществления актов агрессии, нанесения экономического и иного ущерба, в террористических целях, для совершения правонарушений и преступлений, для вмешательства во внутренние дела государств, распространения информации, наносящей вред социальным системам и социально-культурной среде[39].

В Национальной стратегии обороны Бразилии, принятой в 2008 г., кибербезопасность была выделена в качестве отдельного направления политики национальной безопасности. Впоследствии для противодействия киберугрозам

[31] Минкомсвязи провело учения по кибер-защите Рунета // http://uinc.ru/news/sn22087.html (дата обращения: 24.12.2017).

[32] Страны ОДКБ создают центр кибербезопасности // Profit, 20.03.2015; http://profit.kz/news/23183/Strani-ODKB-sozdaut-centr-kiberbezopasnosti/ (дата обращения: 24.12.2017).

[33] Китай создал защищенную операционную систему // Information Security, 13.05.2009; http://www.itsec.ru/newstext.php?news_id=57824 (дата обращения: 23.12.2017).

[34] Пряникова Е. Китайская поисковая система Baidu.com — конкурент Google? // ФБ.ру, 12.03.2017; http://fb.ru/article/300290/kitayskaya-poiskovaya-sistema-baidu-com---konkurent-google (дата обращения: 23.12.2017).

[35] Костин Н. А. Теория информационной борьбы // Palmarium Academic Publishing, 2014. С. 136-137.

[36] Тодоров В. Китай защитит рунет // Газета.ru, 25.11.2014; http://www.gazeta.ru/business/2014/11/24/6313205.shtml (дата обращения: 23.12.2017).

[37] Россия и Китай подписали порядка двух десятков документов о сотрудничестве // ТАСС, 04.07.2017; http://tass.ru/politika/4386636 (дата обращения: 23.12.2017).

[38] China, Japan, ROK hold cyber security meeting in Beijing // Xinhua, 22.10.2014; http://news.xinhuanet.com/english/china/2014-10/22/c_133735283.htm (дата обращения: 23.12.2017).

[39] Распоряжение Правительства РФ от 30.04.2015 №788-р «О подписании Соглашения между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности // http://government.ru/media/files/5AMAccs7mSlXgbff1Ua785WwMWcABDJw.pdf (дата обращения: 23.12.2017).

был создан Коммуникационный центр кибервойн (Cyber-Warfare Communication Centre), Центр кибербезопасности (Center of Cyber Defense)[40]. Бразилия стремится продвинуть кооперативный проект создания системы, позволяющей обеспечить кибербезопасность на уровне Союза южноамериканских наций (УНАСУР)[41]. В настоящее время в УНАСУР созданы рабочие группы по обеспечению кибербезопасности и снижению технологической зависимости[42].

Разоблачения Э. Сноудена подтолкнули Индию к созданию Национального координационного киберцентра (National Cyber Coordination Centre – NCCC)[43]. Создание такого ведомства можно рассматривать как значимый шаг в направлении развития национальной системы контроля за киберугрозами. Индия стремится развивать кооперацию в сфере кибербезопасности с Бразилией[44].

Проведенный анализ показывает, что выработка общих принципов политико-правового регулирования сферы международной информационной и кибербезопасности становится насущной потребностью политики глобальной безопасности, призванной защитить национально-государственный суверенитет, при этом, не допустив новой информационной изоляции, полномасштабной милитаризации информационно-цифрового пространства и глобального конфликта в нем.

Список литературы

1. Вихул Л. Стремление к передовому опыту в киберсфере // Per Concordiam. 2014. Т. 5. № 2. С. 10-19; http://www.marshallcenter.org/MCPUBLICWEB/mcdocs/files/College/F_Publications/perConcordiam/pC_V5N2_ru.pdf.
2. Корсаков Г.Б. Информационное оружие супердержавы: кибервойна и «управляемые кризисы» // Военно-политическое обозрение, 04.05.2012; http://www.belvpo.com/ru/10497.html.
3. Костин Н.А. Теория информационной борьбы // Palmarium Academic Publishing, 2014. 476 с.
4. Чихарев И.А., Столетов О.В. К вопросу о соотношении стратегий «мягкой силы» и «разумной силы» в мировой политике // Вестник Московского университета. Серия 12. Политические науки. 2013. № 5. С. 26-43.
5. Lewis J.A., Timlin K. Cybersecurity and Cyberwarfare. Preliminary Assessment of National Doctrine and Organization // Center for Strategic and International Studies, 2011; http://unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf.

[40] Lewis J.A., Timlin K. Cybersecurity and Cyberwarfare. Preliminary Assessment of National Doctrine and Organization // Center for Strategic and International Studies, 2011; http://unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf (дата обращения: 23.12.2017).

[41] Стратегические последствия разоблачений Эдварда Сноудена (II) // http://www.fondsk.ru/pview/2014/01/14/strategicheskie-posledstvija-razoblachenij-edvarda-snoudena-ii-25160.html (дата обращения: 22.12.2017).

[42] Mercosur to reduce reliance on foreign technology over spying // Xinhua, 17.07.2013; http://news.xinhuanet.com/english/world/2013-07/17/c_132548966.htm (дата обращения: 22.12.2017).

[43] Sandeep Joshi India gets ready to roll out cyber snooping agency // The Hindu, 10.06.2013; http://www.thehindu.com/news/national/india-gets-ready-to-roll-out-cyber-snooping-agency/article4798049.ece (дата обращения: 22.12.2017).

[44] Shobhan Saxena India working with Brazil on cyber security: Khurshid // The Hindu, 16.10.2013; http://www.thehindu.com/news/international/world/india-working-with-brazil-on-cyber-security-khurshid/article5239710.ece?ref=relatedNews (дата обращения: 22.12.2017).

The Problem of Legal Regulation of International Information and Cybersecurity in Modern World Politics

Stoletov O.V.,
PhD in Politics,
Senior Lecturer, Faculty of Political Science
Lomonosov Moscow State University
E-mail: Oleg-Stoletov1@yandex.ru

Abstract. *The article analyzes the approaches of the United States of America, Russia, China, India and Brazil to the problem of legal regulation of international information and cyber security. The author considers the positions of the states in relation to the basic principles of the existing international documents in the field of information and cyber security, analyzes new initiatives in the field of developing international political and legal decisions in this area, and studies the actual practice of political regulation of this sphere at the national-state level. The author concludes that the development of general principles of political and legal regulation of the sphere of international information and cyber security becomes an urgent need for a policy of global security.*
Keywords*: information security, cybersecurity, legal regulation, information sovereignty, global politics.*

References

1. Vikhul L. Stremlenie k peredovomu opytu v kibersfere // Per Concordiam. 2014. T. 5. № 2. S. 10-19; http://www.marshallcenter.org/MCPUBLICWEB/mcdocs/files/College/F_Publications/perConcordiam/pC_V5N2_ru.pdf.
2. Korsakov G.B. Informatsionnoe oruzhie superderzhavy: kibervojna i «upravlyaemye krizisy» // Voenno-politicheskoe obozrenie, 04.05.2012; http://www.belvpo.com/ru/10497.html.
3. Kostin N.A. Teoriya informatsionnoj borby // Palmarium Academic Publishing, 2014. 476 s.
4. Chikharev I.A., Stoletov O.V. K voprosu o sootnoshenii strategij «myagkoj sily» i «razumnoj sily» v mirovoj politike // Vestnik Moskovskogo universiteta. Seriya 12. Politicheskie nauki. 2013. № 5. S. 26-43.
5. Lewis J.A., Timlin K. Cybersecurity and Cyberwarfare. Preliminary Assessment of National Doctrine and Organization // Center for Strategic and International Studies, 2011; http://unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf.