DOI 10.22394/1726-1139-2018-2-137-144

Информационная безопасность РФ: в поиске новых партнеров

Хижняк М. В.

Санкт-Петербургский государственный университет, Санкт-Петербург, Российская Федерация, mariakhizhnyak@gmail.com

РЕФЕРАТ

В статье анализируются актуальные тренды в области международного сотрудничества РФ в сфере информационной безопасности. Отмечено, что на сегодняшний день приоритетным технологическим партнером для России является Китай. За последние несколько лет тема информационной безопасности стала одной из ключевых, поднимаемых на переговорах между российскими и китайскими коллегами, как на правительственном уровне, так и на уровне частного бизнеса. Приводится сравнение подходов стран к обеспечению информационной безопасности, проведен анализ возможных точек соприкосновения в вопросах обеспечения национальной информационной безопасности и взглядов сторон на глобальную архитектуру информационной безопасности. Рассматриваются отличия западного и восточного подходов к обеспечению международной информационной безопасности. На основе анализа информационной политики, проводимой РФ и КНР, дана оценка перспектив дальнейшего сотрудничества двух стран.

Ключевые слова: информационная безопасность, киберпространство, информационные технологии, российско-китайское сотрудничество, архитектура международной информационной безопасности

Information Security of the Russian Federation: In Search of New Partners

Khizhnyak M. V.

Saint-Petersburg State University, Saint-Petersburg, Russian Federation, mariakhizhnyak@gmail.com

ABSTRACT

The analysis of the current trends in the Russia's state policy of international cooperation on the issue of information security reveals the fact that to date China remains the strategic technology partner for Russia. Over the past few years information security has become one of the key topics raised in the talks between the Russian and Chinese counterparts both in the governmental scale and at the level of private business. The author of the article compares the state approaches to information security, analyses possible points of contact in matters of national information security and the views of the parties on the global architecture of information security. Given this, the author draws a distinction between the Eastern (Russian-Chinese) and the Western (the USA, the EU) approaches to ensuring global information security. Based on the analysis of the state information and communication policy of Russia and China, the article provides an assessment of the prospects for further cooperation between the two countries in the field of information technologies.

Keywords: information security, cyberspace, information technology, Russian-Chinese cooperation, the architecture of international information security

С переходом к цифровым бизнес-моделям, развитием платежных технологий, цифровых финансовых услуг, облачных систем, приложений и виртуализации перед пользователями прогрессивных технологий возникает ряд новых угроз их информационной безопасности (ИБ). В таких условиях у пользователей появляется естественное стремление защитить свои информационные ресурсы от возможных срывов в работе,

кибератак, мошенничества или утечки данных. Кроме того, постоянное расширение возможностей информационно-коммуникационных технологий (ИКТ) усиливает уязвимость современного государства перед угрозами его национальной безопасности в глобальном информационном пространстве [3].

Использование мощных информационных ресурсов развитыми государствами способно оказать существенное влияние на геополитическую обстановку на международной арене, а также дестабилизировать политические режимы в разных регионах мира [4]. Таким образом, киберпространство стало необходимой платформой для поддержания роста и развития государства и, в то же время, полем для военно-политического противоборства. Вследствие этого на глобальную повестку дня встает вопрос эффективной защиты деятельности в киберпространстве и обеспечение международной информационной безопасности.

Под международной информационной безопасностью (МИБ) понимается «такое состояние глобального информационного пространства, при котором исключены возможности нарушения прав личности, общества и прав государства в информационной сфере, а также деструктивного и противоправного воздействия на элементы национальной критической информационной инфраструктуры»[1].

Обеспечение ИБ, представляя собой необходимый элемент для формирования сильного государства и нации, стало первоочередной задачей для правящих элит. Защита цифрового пространства в широком смысле проявляется двумя формами: техническая защита и юридическая защита. Наиболее развитые государства в сотрудничестве с бизнес-сообществом ведут активную работу по обоим направлениям, создавая системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы, в то же время, совершенствуя законодательное регулирование деятельности в информационном пространстве. Однако, учитывая специфику сети Интернет, как распределенного ресурса, а также с усилением тенденции к милитаризации информационного пространства и изменением баланса сил на мировой арене, возникает необходимость в многостороннем сотрудничестве государств для совместного противостояния киберугрозам.

Расширение международного сотрудничества в информационной сфере представляет собой одно из приоритетных направлений в обеспечении глобальной и национальной безопасности РФ. Это подтверждается рядом официальных документов государства, в числе которых новая Доктрина информационной безопасности РФ[2], Основы государственной политики РФ в области международной информационной безопасности[3], а также заявлениями на высшем уровне[4]. Россия является активным партнером в области обеспечения МИБ стран-членов таких международных организаций, как СНГ, БРИКС, ШОС, ОДКБ, ЕАЭС, о чем свидетельствует ряд соглашений о сотрудничестве в данной сфере[5].

---

[1] Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (утв. Президентом РФ 24 июля 2013 г., № Пр-1753) [Электронный ресурс]. URL:http://www.scrf.gov.ru/documents/6/114.html (дата обращения: 15.12.2016).

[2] Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента от 05.12.2016 № 646 [Электронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/0001201612060002?index=16&rangeSize=1 (дата обращения: 15.12.2016).

[3] Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года.

[4] Вступительное слово Президента РФ на заседании Совета Безопасности 01.10.2014 [Электронный ресурс]. URL: http://kremlin.ru/events/president/news/46709 (дата обращения: 15.12.2016).

[5] Распоряжение Правительства РФ от 28.05.2012 № 856-р «О подписании Соглашения о сотрудничестве государств — участников Содружества Независимых Государств в области обеспечения информационной безопасности» [Электронный ресурс]. URL: http://minsvyaz.ru/ru/

Еще в декабре 1998 г. вопрос МИБ был впервые поднят Россией на глобальном уровне. На полях Генеральной Ассамблеи ООН была принята консенсусом резолюция «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», инициированная российскими дипломатами[1]. Этот момент стал одним из ключевых для постановки проблемы МИБ и ее вынесения на повестку дня работы Генеральной Ассамблеи ООН. Мировое сообщество признало существование угроз МИБ и начало предпринимать попытки договориться о выработке единых принципов, нацеленных на укрепление безопасности глобальных информационных систем.

Традиционным союзником России в вопросе МИБ является Китай. Уже около 20 лет РФ и Китай совместно выступают за продвижение модели многостороннего управления Интернетом на площадке ООН. По данному вопросу цели обеих сторон полностью совпадают. На международных дискуссионных площадках по вопросам управления и регулирования Интернета обе страны критично высказывались в адрес ICANN — корпорации по распределению имен и адресов в Сети, которая до недавнего времени была подотчетна правительству США, делая их монополистом в управлении ключевой инфраструктурой Интернета.

Еще одна совместная российско-китайская инициатива была озвучена осенью 2011 г. Тогда страны выступили с предложением принятия правил поведения государств в киберпространстве, продвигая в ООН концепцию Конвенции «Об обеспечении международной информационной безопасности». Документ отражал базовые принципы и правила поведения всех стран в информационном пространстве для обеспечения ИБ.

Однако подобные инициативы были критично восприняты в правящих кругах США и Евросоюза. Их подход к обеспечению МИБ предусматривает иные действия для предотвращения киберугроз. Западная модель оправдывает вмешательство государственных структур в международное информационное пространство в случае возникновения угрозы их национальной безопасности. Кроме того, вопрос демонополизации управления Интернетом также вызывает очевидные разногласия между западной и восточной моделью обеспечения МИБ. Вследствие этого по последнему вопросу долгое время не наблюдалось никаких активных действий со стороны США, пока в июне 2013 г. Эдвард Сноуден, бывший сотрудник ЦРУ и АНБ, не опубликовал секретные документы о глобальной слежке спецслужб США и Великобритании в Сети. Только тогда интернет-пользователи всего мира обратили внимание на проблему монополизации управления Интернетом. Потеряв доверие, технические организации начали искать иные пути решения проблемы. Таким образом, с истечением срока действия контракта между организацией ICANN и правительством США 1 октября 2016 г. и отказом его дальнейшего продления, контроль над управлением Интернетом начал свой переход из рук США к международному сообществу[2].

---

documents/3729/; Официальный сайт Организации Договора о Коллективной Безопасности. URL: http://www.odkb-csto.org/documents/detail.php?ELEMENT_ID=133; Соглашение между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. Екатеринбург, 16 июня 2009 года (вступило в силу с 5 января 2012 г.) [Электронный ресурс]. URL: https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreementRussian.pdf (дата обращения: 15.12.2016).

[1] Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. Официальный сайт ООН. URL: https://www.un.org/disarmament/ru/достижения-в-сфере-информатизации-и-т/ (дата обращения: 15.12.2016).

[2] «США лишились возможности влиять на мировое управление интернетом». 02.10.2016 [Электронный ресурс]. URL: https://lenta.ru/news/2016/10/02/noinetusa/ (дата обращения: 16.12.2016).

Трудности в продвижении вопроса МИБ на глобальных международных площадках заставили РФ и Китай переключить свое внимание на региональный уровень сотрудничества. В 2011 г. вступило в силу соглашение между правительствами государств-членов Шанхайской организации сотрудничества (ШОС) в области обеспечения МИБ[1]. Оно впервые выявило существование конкретных угроз МИБ, а также определило основные направления и принципы сотрудничества сторон в данной области. Далее география сотрудничества РФ и Китая в сфере МИБ расширилась за счет других крупных мировых игроков. В 2014 г. в Форталезской декларации участников объединения БРИКС страны осудили «акты массовой электронной слежки и сбора данных о частных лицах по всему миру, а также нарушение суверенитета государств и прав человека»[2], призвав друг друга к выработке «универсального и имеющего обязательную юридическую силу международно-правового документа в данной области»[3]. Тема информационной безопасности была продолжена в рамках VII саммита БРИКС в Уфе и закреплена в Уфимской декларации[4].

Признавая общность подходов и предвидя взаимный национальный интерес, РФ и Китай продолжили развитие темы МИБ на двустороннем уровне. Активное сотрудничество двух стран в информационной сфере берет свое начало в 1993 г., когда было подписано соглашение «О сотрудничестве в области почтовой и электрической связи»[5]. Позднее было подписано множество других двусторонних меморандумов в сфере информатизации. Однако двустороннее соглашение между РФ и КНР о сотрудничестве в области МИБ было подписано лишь в 2015 г., когда страны договорились совместно реагировать на угрозы МИБ, разрабатывать нормы международного права, обмениваться информацией правоохранительных органов, а также технологиями и специалистами для обеспечения безопасности критической информационной инфраструктуры[6].

Совместное заявление Президента РФ и Председателя КНР о взаимодействии в области развития информационного пространства, подписанное в июне 2016 г., только укрепило намерения государств тесно сотрудничать в данной сфере. В заявлении подчеркивается общность интересов обеих стран, в частности, в обеспечении государственного суверенитета в информационном пространстве[7].

В ноябре 2016 г. российские и китайские специалисты приступили к работе по созданию документа, предусматривающего выработку международных норм регу-

---

[1]«О вступлении в силу Соглашения между правительствами государств-членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности» 14.06.2011. Официальный сайт Министерства иностранных дел РФ. URL: http://www.mid.ru/mezdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/UsCUTiw2pO53/content/id/203770 (дата обращения: 16.12.2016).

[2]Там же.

[3]Там же

[4]Уфимская декларация (принята по итогам седьмого саммита БРИКС): г.Уфа, Российская Федерация, 9 июля 2015 г. [Электронный ресурс]. URL: http://www.brics.mid.ru/bdomp/brics.nsf/Ufa_Declaration_rus.pdf (дата обращения: 16.12.2016).

[5] «Двустороннее сотрудничество с Китайской Народной Республикой». Официальный сайт Министерства связи и массовых коммуникаций РФ. URL: http://minsvyaz.ru/ru/activity/directions/711/ (дата обращения: 16.12.2016).

[6]Распоряжение Правительства РФ от 30 апреля 2015 г. № 788-р «О подписании Соглашения между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности» [Электронный ресурс]. URL: http://government.ru/media/files/5AMAccs7mSIXgbff1Ua785WwMWcABDJw.pdf (дата обращения: 16.12.2016).

[7]Совместное заявление Президента РФ и Председателя КНР о взаимодействии в области развития информационного пространства 25.06.2016. Официальный сайт Президента РФ. URL: http://www.kremlin.ru/supplement/5099 (дата обращения: 16.12.2016).

лирования интернета. Признавая наличие правового вакуума в международном законодательстве в настоящий момент, страны видят необходимость обеспечить суверенитет в информационном пространстве и вывести правовые нормы Интернета на уровень ООН. А поскольку американская модель уже утратила свою актуальность в отношении соответствия международным требованиям регулирования киберпространства, встал вопрос разработки новых принципов[1].

Подобные решения ясно демонстрируют отличие российско-китайского подхода к вопросу МИБ от подхода западных стран. РФ и Китай ищут пути для сотрудничества, призывая к выработке «общих правил игры» в информационном пространстве. В то же время, тенденция к милитаризации информационной сферы заставляет США и другие страны НАТО рассматривать киберпространство как потенциальное поле для конфликта. Все чаще звучат обвинения официальных представителей США в адрес «российских и китайских хакеров» во взломе информационных систем американских государственных ведомств, компаний и краже конфиденциальной информации. И единственным возможным решением проблемы в США видят введение санкций[2].

Сотрудничество России и Китая обусловлено не только общностью подходов к обеспечению глобальной ИБ. Страны имеют взаимный национальный интерес в подобном сотрудничестве. Для России в условиях западных санкций именно Китай может стать тем сильным и надежным партнером, с которым возможно взаимовыгодное сотрудничество. Безусловно, сравнивая успехи обеих стран в сфере развития ИКТ, следует отметить, что Китай во многом опережает Россию. Согласно докладу «Индикаторы науки и техники», Китай заметно усиливает свои позиции на мировой арене, заняв второе место в мире по объему инвестиций, вкладываемых в научные исследования, наращиванию высокотехнологичного производства, а также лидируя в обеспечении научными и инженерными кадрами[3].

27% глобального высокотехнологичного производства приходится на Китай, что выводит его на второе место в мире, он уступает лишь США[4]. Особое внимание Китай уделяет производству и развитию ИКТ, составивших уже в 2014 г. 39% от мирового показателя[5]. Экспорт китайских высокотехнологичных продуктов в сумме составил 2,4 трлн долл.[6]. По сравнению с российскими показателями в 7 млрд долл. в 2016 г. — показателем, озвученным Президентом В. В. Путиным в послании Федеральному Собранию, китайские успехи выглядят более чем убедительно[7].

Поддержка отечественных технологических инноваций, подготовка высококлассных специалистов, практика ведения ИТ-бизнеса — наиболее сильные стороны китайского опыта в сфере ИКТ. Приоритет собственных технологических инноваций заставил Китай открыть государственные границы для иностранного капитала, при-

---

[1] *Лыков Р.* «Кодекс глобальной сети: Россия и Китай предложат ООН принять свод законов интернета» // Политика сегодня. 16.11.2016. [Электронный ресурс]. URL: https://fapnews.ru/302896-kodeks-globalnoi-seti-rossiya-i-kitai-predlozhat-oon-prinyat-svod-zakonov-interneta (дата обращения: 18.12.2016).

[2] «США высылают российских дипломатов и вводят новые санкции из-за кибератак» // Русская служба BBC 29.12.2016 [Электронный ресурс]. URL: http://www.bbc.com/russian/news-38464443 (дата обращения: 09.01.2017).

[3] Science and Engineering Indicators (SEI) Report 2016 [Электронный ресурс]. URL: https://www.nsf.gov/statistics/2016/nsb20161//report/overview/summary-and-conclusions (дата обращения: 18.12.2016).

[4] См. там же.

[5] См. там же.

[6] Там же.

[7] Послание Президента РФ Федеральному Собранию 01.12.2016. Официальный сайт Президента РФ. URL:http://kremlin.ru/events/president/news/53379 (дата обращения: 18.12.2016).

влекая финансирование для экспортно-ориентированных и высокотехнологичных отраслей. Подобный опыт, умения и квалификации, безусловно, были бы полезны для применения в РФ, что стало темой для обсуждения в рамках российско-китайских форумов. Сотрудничество в сфере инноваций перешло в активную стадию с 2014 г., когда Китай стал главным партнером III Московского международного форума «Открытые инновации»[1]. В последующие годы Китай и РФ неоднократно обменивались визитами промышленных и инновационных форумов, проводимых в обеих странах[2].

В китайской Государственной стратегии развития информатизации на 2006–2020 гг. акцент сделан на развитие Интернета для обеспечения экономического роста страны. В числе основных приоритетов информатизации указываются медицина, образование, банковская сфера, научные исследования, развитие бизнеса, а также внедрение электронного правительства [2]. Похожие направления развития отражены в аналогичной государственной программе РФ «Информационное общество (2011–2020 годы)». Интернет видится для обоих государств эффективным средством модернизации экономики и ослабления остроты проблем в социальной сфере. Именно по этой причине стратегии информатизации РФ и КНР предусматривают широкую поддержку распространения сети в самых удаленных уголках стран. В то же время признается значимость обеспечения социальной стабильности, что достигается нейтрализацией внешнего нежелательного информационно-психологического воздействия на сознание народа. Предоставляя исключительную возможность оказывать влияние на поведение граждан, интернет способен дестабилизировать политические режимы, вследствие чего государства ищут свои пути решения проблемы двойственности влияния интернета [4].

Касательно последнего вопроса Китай демонстрирует большие успехи. Уже более 10 лет в стране действует «Золотой щит» — система фильтрации нежелательного контента, который блокирует доступ к запрещенным веб-сайтам, а также защищает от внешних вирусов и кибератак. Китайские власти активно контролируют материалы, передаваемые по IP-сетям, что предотвращает распространение реакционных настроений в Сети. Функции контроля над Сетью перераспределены между операторами связи и органами власти на местах. За техническое функционирование интернета в Китае отвечает Министерство промышленности и информатизации, а вопросами регулирования контента занимается Государственное управление по делам радиовещания, кинематографии и телевидения [2]. Кроме того, в Китае функционирует специальное полицейское ведомство для контроля за интернетом.

В России фактически все функции контроля над распространяемой информацией, а также обеспечением функционирования Интернета исполняет Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), находящаяся в ведении Министерства связи и массовых коммуникаций Российской Федерации. Однако существующее законодательство, а также несовершенство структуры органа и процедуры принятия решений не позволяют оперативно реагировать на возникающие угрозы [1]. Таким образом, действующая в России система интернет-контроля не отвечает требованиям эффективности, вследствие чего Правительство переключило свой фокус сотрудничества на

[1] Российско-китайский форум «Инвестиции в инновации» 15–16.09.2016. Официальный сайт. URL: http://invest-to-innovation.com/ (дата обращения: 18.12.2016).

[2] «Итоги Седьмого Международного Инновационного Форума «Пуцзян 2014» // Союз общественных объединений «Международный союз приборостроителей и специалистов по информационным и телекоммуникационным технологиям» 20.11.2014 [Электронный ресурс]. URL: http://e-expo.ru/index.php/2010-07-23-11-37-45/60-pujiang-2014/472-pujiang2014itogishort.html (дата обращения: 18.12.2016).

Китай, полагая, что опробованные им технологии в этой области смогут быть применены и к российской реальности. Ряд встреч российских высокопоставленных чиновников с основателями «китайского файерволла» в 2015–2016 гг. дают основание полагать, что Россия пытается перенять опыт китайских коллег в данной сфере. Тем более что в условиях западных санкций Китай остается для России чуть ли не единственным источником новых технологий.

В свою очередь, в КНР видят свою выгоду от подобного сотрудничества. Анализируя российский рекламный теле- и интернет-контент в сфере электроники, можно заметить, что в настоящий момент очевидно преобладание в нем китайских устройств. Несмотря на провозглашаемую РФ политику импортозамещения российский рынок ИТ-продуктов все больше заполняется китайскими предложениями, что может нанести ущерб развитию отечественной ИТ-индустрии. Кроме того, Китай заинтересовался российским положительным опытом государственного регулирования информационного пространства. Новый закон о кибербезопасности, принятый в КНР в ноябре 2016 г., обязывает иностранные ИТ-компании хранить данные об организациях и китайских гражданах на внутренних серверах, предусматривая обязательную сертификацию компьютерного оборудования ИТ-компаний. Этот закон практически повторяет требования «Пакета Яровой» — аналогичных документов, принятых в РФ 6 июля 2016 г.[1]

Имея много общего в подходах к обеспечению ИБ, выступая союзниками перед лицом глобальных информационных угроз, РФ и КНР, тем не менее, видят в первую очередь свои национальные интересы в подобном сближении. Если страны станут партнерами сегодня, то это не гарантирует продолжение их сотрудничества завтра. Сложная и нестабильная геополитическая ситуация вокруг РФ, агрессивная политика Запада заставили Россию искать союзников на Востоке, однако станет ли такое сотрудничество долговечным — большой вопрос.

Уже сейчас наблюдаются случаи несоблюдения Китаем своих соглашений о кибербезопасности и ненападении, о чем говорит увеличение числа кибератак китайских хакеров на российские объекты критической инфраструктуры[2]. Кроме того, стало заметно стремление КНР к налаживанию сотрудничества в сфере кибербезопасности с США — еще недавно провозглашаемым общим противником[3]. И подобный интерес понятен, ведь Китай, имея устоявшуюся практику производства высокотехнологичных продуктов, осуществляет их выпуск на основе скопированных западных технологий. А следовательно, ему также нужны союзники из числа стран-источников новых технологий.

Таким образом, разворот курса РФ «на восток» выглядит весьма перспективным в контексте подготовки ИТ-специалистов, развития систем государственного регулирования, онлайн-фильтрации нежелательной информации, а также ведения ИТ-бизнеса. Однако для продвижения собственных технологических продуктов России придется искать другие рынки, для реализации чего многообещающе выглядит сотрудничество со странами БРИКС, ШОС, ЕЭС. Тем не менее, учитывая геополитическую обстановку на мировой арене, на сегодняшний день именно Китай остается для России приоритетным технологическим партнером.

---

[1] *Анушевская А., Чунихина М.* «Что такое «пакет Яровой» и в чем его суть?» // Аргументы и факты. 23.06.2016 [Электронный ресурс]. URL: http://www.aif.ru/dontknows/actual/chto_takoe_paket_yarovoy_i_v_chyom_ego_sut (дата обращения: 19.12.2016).

[2] Bloomberg: «Китайский пылесос» угрожает безопасности России» // RT 26.08.2016 [Электронный ресурс]. URL: https://russian.rt.com/inotv/2016-08-26/Bloomberg-Kitajskij-pilesos-ugrozhaet-bezopasnosti (дата обращения: 19.12.2016).

[3] «Китай готов развивать сотрудничество с США по кибербезопасности» // РИА-новости 15.03.2016 [Электронный ресурс]. URL:https://ria.ru/world/20160315/1389884620.html (дата обращения: 19.12.2016).

Литература

1. *Байкова И. А.* Информационно-регулирующая функция государства в сети Интернет // Евразийский Союз Ученых (ЕСУ). 2015. № 11 (20). С. 84–86.
2. *Ибрагимова Г.* Стратегия КНР в области управления интернетом и обеспечения информационной безопасности // Индекс безопасности. 2013. № 1 (104). Т. 19. С. 169–184.
3. *Кучерявый М. М.* Роль информационной составляющей в системе политики обеспечения национальной безопасности Российской Федерации // Известия Российского государственного педагогического университета им. А. И. Герцена. 2014. № 164. С. 155–163.
4. *Панцерев К. А.* «Твиттерные революции» в странах Северной Африки — обратная сторона развития информационного общества // Азия и Африка сегодня. 2016. № 4. С. 14–19.

Об авторе:
Хижняк Мария Владимировна, аспирант факультета международных отношений Санкт-Петербургского государственного университета (Санкт-Петербург, Российская Федерация), mariakhizhnyak@gmail.com

References

1. Baikova I. A. Information-regulating function of the state in the Internet // Eurasian Union of Scientists [Evraziysky soyuz uchenyh]. 2015. N 11 (20). P. 84–86 (rus).
2. Ibragimova G. China's strategy in the field of Internet governance and information security // Security Index [Index bezopasnosti]. 2013. N 1 (104). V. 19. P. 169–184 (rus).
3. Kucheriavyi M. M. The role of the information component in the system policy National security of the Russian Federation // News of the Russian State Pedagogical University of A. I. Herzen [Izvestiya Rossiyskogo gosudarstvennogo pedagogicheskogo universiteta im. A. I. Gertsena] 2014. N 164. P. 155–163 (rus).
4. Pantserev K. A. Twitter revolutions» in North Africa — the flip side of the Information Society // Asia and Africa today [Aziya I Afrika segodnya] 2016. N 4. P. 14–19 (rus).

About the author:
Maria V. Hizhnyak, graduate student of Saint-Petersburg State University (Saint-Petersburg, Russian Federation), mariakhizhnyak@gmail.com