УДК 341.24

Российский подход к формированию пространства коллективной информационной безопасности стран БРИКС

А. В. Манойло
Московский государственный университет имени М. В. Ломоносова

Научная статья

Статья посвящена исследованию принципов, направлений, форм и методов формирования единого пространства коллективной безопасности стран БРИКС в информационной сфере. Цель создания такого пространства коллективной безопасности – совместное противодействие новым вызовам и угрозам в информационной сфере, таким как киберпреступность, информационный терроризм и экстремизм, операции информационной войны, с которыми каждая из входящих в БРИКС стран в отдельности на сегодня не справляется. Основанием для создания такого пространства и системы, обеспечивающей его информационную безопасность на уровне, отвечающем национальным интересам стран БРИКС, является общая для всех указанных стран потребность в противодействии транснациональной киберпреступности и в отражении операций информационной войны, организуемых зарубежными противниками и конкурентами БРИКС. В этой связи изучается опыт противодействия таким новым вызовам и угрозам международной и национальной безопасности, как киберпреступность, информационный терроризм и экстремизм, операции информационной войны, с которыми не способна справиться каждая по отдельности из стран БРИКС. Обосновывается целесообразность формирования системы наднациональных органов БРИКС, отвечающих за обеспечение информационной безопасности объединения в целом. Одним из таких органов может стать международная киберполиция БРИКС, наделенная оперативными и следственными функциями. Автор видит в формировании системы наднациональных органов БРИКС эффективный инструмент обеспечения информационной безопасности объединения БРИКС в целом и отражения операций информационной войны в частности. В этом плане такую систему органов можно организо-

Russian approach to the formation of the space of collective information security of the BRICS countries

A. M. Manoylo
Lomonosov Moscow State University
E-mail: cyberhurricane@yandex.ru

Scientific article

The article devotes to the exploration of the principles, directions, forms and methods of the creation of common area of collective security among BRICS member states in the information field. The goal of creating such a space of collective security is the joint opposition to new challenges and threats in the information sphere, such as cybercrime, information terrorism and extremism, information warfare operations, with which each of the countries included in the BRICS alone cannot cope today. The basis for creating such a space and a system providing its information security at a level that meets the national interests of the BRICS countries is the common for all these countries the need to counter transnational cybercrime and to repel information warfare operations organized by foreign opponents and BRICS competitors. In this regard the author investigates the experience to counteract such new challenges and threats as cybercrimes, information terrorism and extremism. The paper notes that no one of BRICS countries individually is able to cope with these problems. One of such bodies may be the international cyberpolicy BRICS, endowed with operational and investigative functions. The author shows the expediency of forming a system of supranational bodies BRICS which are responsible for ensuring the information security of BRICS as a whole and the reflection of information warfare operations, in particular. In this regard, such a system of bodies can be organized, using the experience of the creation and functioning of relevant supranational bodies of the European Union.

вать, используя опыт создания и функционирования соответствующих наднациональных органов Европейского Союза.

Ключевые слова: безопасность; Россия; киберпреступность; информационный терроризм; БРИКС; информационная война; кибератаки; киберполиция

Keywords: Security; Russia; cybercrimes; information terrorism; BRICS; information warfare; cyberattacks; cyberpolicy

В условиях дигитализации различных процессов развития стран, регионов и мира в целом – экономических (в частности, переход к «Индустрии 4.0» ведущих промышленных стран мира), политических, военных – значимость решения вопросов обеспечения кибер- и информационной безопасности резко повышается. Так, удачно проведённая организованная хакерская атака на автоматизированные системы связи и управления войсками могжет фактически «выключить» штаб войсковой части (соединения), тем самым резко понизив его боеспособность, что, в свою очередь, может иметь критическое значение в бою. Именно по этой причине как в институтах ЕС, НАТО, так и в институтах Евро-Атлантического сообщества наблюдается процесс создания нового рода войска – киберкомандования, ответственного за защиту критически важной инфраструктуры военного и двойного назначения. Так, в 2016 г. киберкомандование было создано во французских ВС [1], а в 2017 г. – в бундесвере [2]. Примечательно, что оба они тесно взаимодействуют с профильными гражданскими компаниями, в том числе в ходе проведения учений по отражению угроз в киберсфере [2]. Это показывает, сколь значима для государств эта проблема в современных реалиях.

Еще одним инструментом политического давления на суверенные государства и проводимую ими внешнюю политику являются информационные войны и психологические операции. Современные технологии информационных войн, основанные на манипулятивном управлении политическим сознанием и поведением граждан, исключительно опасны: их главная задача – разделить и поляризовать общество, разорвать его на множество клочков и фрагментов, заставить эти фрагменты искренне ненавидеть друг друга с тем, чтобы впоследствии столкнуть их между собой, инициировав борьбу на уничтожение, или объединить их агрессию в общий поток и направить его против действующей власти. При этом цель информационной войны – сломить волю противника к сопротивлению и подчинить его сознание своей воле. Высокая эффективность информационных атак и растерянность, являющаяся типичной реакцией большинства стран на акции информационной войны, делает информационные войны одним из основных элементов современных гибридных войн, таких как война в Сирии или конфликт в Украине.

Информационная война (ИВ) – это вооруженный конфликт, в котором столкновение сторон происходит в форме информационных операций с применением информационного оружия.

Структурно современная информационная война состоит из последовательности информационных операций, объединенных единым замыслом и согласованных по целям, задачам, формам и методам информационного воздействия.

В Соединенных Штатах Америки термин «информационная операция» официально закреплен в полевом уставе Армии США «Психологические операции» FM 33-1. Согласно этому источнику, информационная операция – это проводимая в мирное или военное время плановая пропагандистская и психологическая деятельность, рассчитанная на иностранные дружественные, враждебные или нейтральные аудитории с тем, чтобы влиять на их отношение и поведение в благоприятном направлении для достижения как политических, так и военных целей.

При этом американские военные выделяют три уровня ведения информационных войн: стратегический, тактический и оперативный. Уровень информационных операций –

Для цитирования: Манойло А. В. Российский подход к формированию пространства коллективной информационной безопасности стран БРИКС // Социальные и гуманитарные знания. 2018. Том 4, № 3. С. 156–163.

For citation: Manoylo A. M. Russian approach to the formation of the space of collective information security of the BRICS countries. 2018; 3 (4): 156–163. (in Russ.)

это тактический уровень ведения информационной войны. Оперативный уровень ведения ИВ – это уровень отдельных информационных атак, совокупность которых составляет одну информационную операцию. Стратегический уровень соответствует самой информационной войне.

Стандартная англосаксонская операция информационной войны представляет собой последовательность информационных вбросов, разделенных периодами экспозиции (информационной «тишины») и согласованных по времени, целям, задачам и объектам воздействия.

С помощью вбросов, содержащих заведомо провокационную информацию, объект информационной атаки пытаются вывести на эмоции и совершение необдуманных поступков, которые затем становятся предметом острой критики и в конечном итоге ведут к его дискредитации.

Информационный вброс – это блок специально подготовленной информации, стимулирующей объект информационного воздействия на совершение немедленных ответных действий (в качестве реакции на полученный внешний стимул).

Ошибочно считать, что информационный вброс должен содержать только компрометирующую информацию. Содержанием информационного вброса может быть любая информация стимулирующего характера, способная вывести объект атаки из состояния равновесия и побудить его к немедленному совершению спонтанных, неосознанных, необдуманных действий. Если грубая лесть воздействует на психоэмоциональное состояние объекта атаки сильнее, чем компромат или шантаж, заставляя его под наплывом эмоций «терять голову» (временно утрачивать над собой контроль), то вброс будет насыщен именно такого рода информацией.

Любая операция информационной войны начинается с информационного вброса, направленного на объект (мишень) атаки или на его ближайшее окружение. Если одного вброса недостаточно для того, чтобы сломить противника или подчинить себе его волю, в операциях ИВ используют серию информационных вбросов, вбрасываемых в публичное информационное пространство по очереди, последовательно, через заранее намеченные промежутки времени, обеспечивающие эффект экспозиции.

Период экспозиции – это период информационной «тишины», разделяющий два последовательных вброса, предназначенный для считывания и анализа реакции объекта (мишени) воздействия на вброшенную в его адрес стимулирующую информацию (с помощью обязательно присутствующего в схеме операции ИВ механизма положительной обратной связи). В схеме операции ИВ периоды экспозиции – это технические паузы; их присутствие в обязательно.

Наиболее часто объектом информационной атаки становятся первые лица государства – президент и премьер: с них, как правило, информационная война и начинается. Причина этого предельно проста: первые лица всегда находятся под прицелом, они ведут публичный образ жизни, каждый их шаг, каждое их действие или движение рассматриваются сквозь лупу. То, что прощается любому публичному политику, даже самому высокопоставленному и известному, никогда не прощают лидерам государства: они часто просто не имеют права на ошибку, что в определенном смысле роднит их с саперами. В силу своей публичности именно первые лица государства выступают главными ньюсмейкерами и производят большинство резонансных инфоповодов, которые затем интерпретируются национальными и зарубежными СМИ. Информационная война всегда разворачивается вокруг первых лиц, их действий, реакций на те или иные события, которые на первоначальном этапе тщательно прощупываются и тестируются с помощью заведомо провокационных вбросов ложной информации, запуска в социальных сетях вирусного контента, распространения слухов и сплетен, способных эмоционально «зацепить» хотя бы одного из первых лиц государства и вызвать его ответную резкую, эмоционально окрашенную реакцию.

Однако в качестве объекта информационной атаки может быть выбрана и групповая мишень: например, политическая элита, входящая в окружение президента, – тот самый «ближний круг» доверенных лиц, на которых лидер страны опирается. В этом случае целью атаки становится внесение раскола в ряды элиты, стремление заставить их забыть об интересах государства и полностью переключиться на спасение своих личных капиталов. В результате лидер страны в самый ответственный момент может оказаться без поддержки и проиграть.

Информационная атака на окружение президента может быть направлена как напрямую, так и опосредованно, с использованием «отраженного» эффекта. Нередко лидер страны, отбивая информационную атаку, сам становится ретранслятором информационного воздействия: защищая себя, он отражает информационную волну на свое окружение, своими комментариями многократно усиливая ее поражающий эффект.

Противостоять внешним хакерским и информационным атакам призвана система обеспечения информационной безопасности государства. В свою очередь, обеспечение информационной безопасности любого государства в современном мире находится в прямой зависимости от наличия высокоразвитой и конкурентоспособной информационно-коммуникативной инфраструктуры государства, которая подразумевает под собой наличие двух составляющих: технологической и смысловой (содержательной).

Технологическая (кибер-) составляющая национальной информационно-коммуникативной инфраструктуры представляет собой совокупность информационных систем, подсистем и центров, баз знаний и данных, систем связи, центров управления, средств и технологий сбора, хранения, обработки и передачи информации и т. д. Таким образом, кибербезопасность государства подразумевает наличие таких организационных мер и структур, как национальные системы спутниковой связи, навигации и вещания, национальная система платёжных карт, национальные базы данных и знаний, государственные системы защиты и блокировки информации, национальные поисковые системы и т. д. Следует отметить, что список требований, предъявляемых к высокоразвитым информационно-коммуникативным инфраструктурам, с каждым годом становится всё более и более обширным.

Состояние информационно-коммуникативной инфраструктуры и информационной индустрии государства в реалиях глобального информационного общества является важнейшим условием успешности реализации внутренней политики. Однако процесс информатизации в разных государствах неравномерен, что приводит к существованию такого феномена, как «цифровая асимметрия», которая заключается в неравномерности распределения информационных ресурсов между различными государствами и, как следствие, неравномерных возможностях использования глобального информационного пространства. В связи с этим борьба за информационные ресурсы и информационное пространство между государствами приобретает принципиально важное значение.

Не менее значимой для вопроса информационной безопасности является и смысловая (содержательная) сторона информационно-коммуникативной инфраструктуры государства. Если говорить упрощённо, она представляет собой тот посыл (контент), который транслирует государство в общество и/или международное сообщество посредством наличествующих у него информационно-коммуникативных ресурсов. Также к содержательной стороне обеспечения информационной безопасности относятся вопросы её концептуального и стратегического оформления и нормативно-правового регулирования.

С одной стороны, значимость данных вопросов нашла отражение в концептуальных документах России в области безопасности. Так, в действующей (2014) Военной доктрине РФ указывается, что «наметилась тенденция смещения военных опасностей и военных угроз в информационное пространство» [3]. В Стратегии национальной безопасности, принятой в 2015 г., также отмечается: «Все большее влияние на характер международной обстановки оказывает усиливающееся противоборство в глобальном информационном пространстве, обусловленное стремлением некоторых стран использовать информационные и коммуникационные технологии для достижения своих геополитических целей, в том числе путем манипулирования общественным сознанием и фальсификации истории» [4]. С другой стороны, в России до сих пор не принято официального профильного документа по вопросам обеспечения кибербезопасности, хотя необходимость его принятия и проработка предварительных вариантов (в том числе на площадке Совета Федерации) ведутся как минимум с начала 2010-х гг.

Из системной сложности и разветвлённости информационно-коммуникативной инфраструктуры государства логически проистекает идея формирования единого пространства информационной безопасности в наднациональных рамках международных интегративных организаций с участием России (БРИКС, ЕАЭС). Это, с одной стороны, позволит соединить самые передовые технологии стран-участниц, произвести обмен бесценным опытом в сфере обеспечения информационной безопасности, снизить ресурсные затраты и издержки каждого отдельного государства. С другой – может стать «рупором» развития

единого информационного пространства, основанного на общих принципах и ценностях для государств объединения. Это позволит организовать культурный и символический обмен между различными обществами, усилить сотрудничество в различных областях экономики за счёт её высокой информатизации. Кроме того, станет возможно формирование, например, единой платёжной системы и в отдалённой перспективе – даже единого рынка товаров и услуг.

Актуальные вызовы и угрозы информационной безопасности РФ

С точки зрения автора, те вызовы, которые встают перед Россией в информационной сфере, можно условно разделить на три группы.

Первая из них связана с имиджевыми аспектами. К их числу следует отнести:

– формирование негативного восприятия России якобы как «продуцента угроз», «спойлера миропорядка», то есть государства, не вписывающегося в парадигму либеральной демократии, в понимании отдельных граждан, гражданских обществ, элит стран-участниц Евро-Атлантического сообщества;

– активизация СМИ, блогеров внешних государств, стремящихся дискредитировать не только действующую власть, но и в принципе институт государства в России в глазах граждан РФ, стран СНГ, ЕАЭС, ОДКБ с целью создания соответствующих моделей политического поведения у граждан данных стран в её отношении.

Вторая группа рисков включает в себя проблемы технологического характера, уменьшающие нынешние и потенциальные место и роль России в мировом информационном пространстве. К числу таковых относятся:

– ослабление международного авторитета России за счёт вытеснения её с внешнего информационного рынка;

– формирование информационной зависимости российского общества, заключающейся в доминировании на внутреннем рынке и рынках стран-партнёров зарубежных систем спутниковой связи, навигации, вещания и платежей;

– содействие повышению зависимости России от импорта высоких технологий;

– возникновение комплекса новых угроз, связанных с феноменами «интернета вещей» и технологиями Big Data, к которым Россия может быть технологически не готова;

– усиление информационного влияния на территории России, а также стран СНГ и ЕАЭС международных террористических организаций (в частности «Исламского государства» (запрещено в РФ)).

Наконец, третья группа включает в себя вызовы, имеющие существенное военно-политическое измерение. Она представлена следующими положениями:

– разработка рядом государств концепций информационных и гибридных войн, направленных против России и её союзников и партнёров;

– потенциальная угроза вторжения ряда стран и террористических организаций в информационное пространство России и её партнёров, а также нарушение нормального функционирования национальных информационных и телекоммуникационных систем России, стран БРИКС, СНГ и ЕАЭС;

– возможность попыток нарушения систем связи и управления Вооружёнными Силами и войсками союзников РФ на всех уровнях (тактическом, оперативном, стратегическом);

– угроза возрастания уровня киберпреступности на территориях России, её союзников и партнёров.

Наличие широкого перечня новых вызовов и угроз требует от России активизации усилий по формированию единого пространства коллективной безопасности в информационной сфере и привлечение к этому строительству стран БРИКС.

Каковы особенности обеспечения своей безопасности в информационной сфере другими странами объединения? Импульсом для развития системы безопасности в Бразилии стал доклад Э. Сноудена о слежке различных ведомств США за гражданами страны в интернете (2013). Уже в апреле 2014 г. Национальный конгресс Бразилии утвердил так называемый «Билль Марко», более известный как «Интернет-конституция». Его основное содержание посвящено декларированию прав и свобод личности в интернет-пространстве,

а также мерам и механизмам их соблюдения [5]. Основные положения документа должны быть, с точки зрения автора статьи, учтены при разработке концептуальных документов РФ в исследуемой сфере.

Закон стал отправной точкой для создания обособленной от США национальной системы в информационной сфере. Так, государственные служащие Бразилии отказались от использования поставщиков услуг электронной почты из США и перешли на бразильские. В 2015 г. в Бразилии начата реализация крупномасштабного проекта по прокладыванию интернет-кабеля из Европы в Бразилию по дну Атлантического океана в обход США, в дальнейшем планируется также соединение Бразилии с Африкой и Азией. В развитие этого 17 февраля 2017 г. бразильское правительство заявило о необходимости создания киберполиции, ответственной за предотвращение киберпреступлений (незаконное использование персональных данных, кибершпионаж, кибертерроризм и т. д.). Интересно, что уже в 2017 г. началась институционализация сотрудничества по этому направлению между Бразилией и Европолом [6], что демонстрирует заинтересованность в этом ЕС как института на фоне расхождений с администрацией Д. Трампа по широкому кругу вопросов.

Индия занимает одно из лидирующих мест в мире по числу киберпреступлений, хакерских атак и распространения вредоносного программного обеспечения. В 2012 г. правительством страны был утверждён пятилетний план «по повышению уровня информационной безопасности учреждений критически важной инфраструктуры на территории всей страны». В рамках данного плана предполагалось претворение в жизнь следующих мер: создание ведомства быстрого реагирования на киберугрозы, национальной операционной системы, полное обеспечение информационно-коммуникативной безопасности правительственных структур, создание национальных баз данных и знаний, использование биометрических технологий для получения гражданами доступа к сети интернет и осуществления финансовых онлайн-операций [7]. В развитие этого в 2013 г. был создан Национальный центр защиты критически важной инфраструктурной информации и учреждена полиция по кибербезопасности. В феврале 2017 г. была создана Команда при правительстве Индии по реагированию на чрезвычайные ситуации, которая запустила проект «Cyber Swachha Kendra» [8]. Думается, что опыт учреждения профильных гражданских (и смешанных, то есть с участием военных) структур по обеспечению кибербезопасности может быть весьма востребован в России.

Китай по праву считается одним из государств-лидеров по части технологий национальной информационной и киберзащиты, направленных на контроль и регулирование интернет-пространства на своей территории. С 1998 г. в рамках общего проекта «электронного правительства» в Китае существует 12 так называемых «золотых проектов», направленных на регулирование интернет-пространства. Наиболее известным из них является проект «Золотой щит», представляющий собой систему фильтрации содержимого интернета за счёт ограничения доступа к ряду ресурсов и страниц на территории КНР [9]. На данный момент «Золотой щит» использует следующие методы фильтрации: блокировка IP-адресов, фильтрация DNS-запросов и их переадресация, блокировка интернет-адресов (URL), фильтрация на этапе пересылки пакетов, блокировка соединений, осуществляемых через VPN.

Параллельно ещё с начала 2000-х Народно-освободительной армией Китая реализуются проекты по модернизации радиоэлектронной разведки и контрразведки. Ещё в середине 1990-х гг. КНР были введены в эксплуатацию 4 новых центра радиоразведки в Тихом Океане, а в 1999 г. на Кубе был развёрнут китайский центр радиоперехвата.

В развитие этих мер в 2016 г. Всекитайское собрание народных представителей приняло решение о создании киберполиции. Борьба с кибертерроризмом и кибершпионажем в Китае осуществляется за счёт деятельности десятого (сбор научно-технической информации) и одиннадцатого (радиоэлектронная разведка и компьютерная безопасность) бюро Министерства государственной безопасности КНР, подчиняющегося КПК.

В Южно-Африканской республике уже в 2010 г. были впервые созданы специальные подразделения киберполиции, деятельность которых направлена на предотвращение и отслеживание киберпреступлений экономического характера и против личности и значимых государственных инфраструктурных объектов. В конце 2016 г. правительством ЮАР

был издан «Билль о киберпреступлениях и кибербезопасности», поставивший первоочередной задачей в рамках постепенной информатизации общества создание пространств общенациональной и личной информационной безопасности [10]. Согласно данному Биллю, в 2017 г. в ЮАР был создан Центр Кибербезопасности при Национальном Университете Йоханнесбурга при содействии правительства республики. Данный центр занимается подготовкой профессиональных кадров, созданием нормативно-правовых основ регулирования информационного пространства ЮАР, информационно-технической подготовкой деятельности правительственных органов в данной сфере, а также научными исследованиями по вопросам кибер- и информационной безопасности. 6 сентября 2017 г. между Россией и ЮАР было подписано Соглашение о сотрудничестве в области кибербезопасности [11].

Таким образом, основная масса шагов по созданию национальных систем обеспечения безопасности в кибер- и информационной сфере была предпринята партнёрами России по БРИКС с середины 2010-х гг. Это связано как с общим ростом значимости угроз в данной области, так и с повышением неопределённости как результата бурных изменений мирополитической системы на региональном и глобальном уровнях.

Перспективные направления деятельности для РФ в рамках создания пространства коллективной безопасности БРИКС

Каковы же конкретные направления углубления сотрудничества РФ со странами БРИКС? С точки зрения автора, требуется скорейшая институциализация сотрудничества киберполиций указанных стран с профильными структурами МВД РФ. Кроме того, опосредованно (через Бразилию) имеет смысл налаживать взаимодействие и с ЕС, а также отдельными странами-участницами. Необходимость этого продиктована прежде всего тем, что ни одна страна самостоятельно неспособна полностью быть готовой к отражению широкого спектра угроз в кибер- и информационной сферах.

Параллельно должны реализовываться меры по созданию:

– единой системы предупредительных мер противодействия киберпреступлениям, международному терроризму в интернете и информационным атакам;

– программных документов в области обеспечения коллективной информационно-коммуникативной безопасности: концепции информационной безопасности, стратегий коллективного противодействия информационным и гибридным войнам, имиджевой стратегии;

– возможностей приоритетного доступа РФ к информационному пространству стран-участниц БРИКС. Например, точечное проникновение российских ресурсов и компаний под «Золотой щит»;

– ряда совместных инфраструктурных проектов. Например, единой платёжной системы стран-участниц БРИКС, единых систем поиска и навигации;

– единых медиа: агентств новостей, телеканалов, периодических изданий, информационных онлайн-ресурсов и т. д.

Кроме того, требуется углубление сотрудничества с компаниями стран-участниц БРИКС и в области IT- технологий, и по вопросам обмена информацией и обеспечение равного доступа к информации всех граждан членов-государств БРИКС. Немаловажной задачей является обеспечение доступа аудитории стран-участниц БРИКС к российским информационным ресурсам и телеканалам («1 канал», «Russia Today» и т. д.) на русском и национальных языках и проведение совместных информационных и имиджевых компаний странами-участницами БРИКС в рамках позиционирования на международной арене.

В этой связи автором предлагается двуосновная организационная структура пространства коллективной информационной безопасности БРИКС:

1. Совет коллективной информационной безопасности БРИКС призван явиться центральным концептуальным и стратегическим органом. В состав совета следует включить высших должностных лиц, руководящих вопросами развития ИКТ и информационной безопасности в соответствующих странах-участницах объединения.

2. Центр обеспечения кибербезопасности БРИКС будет заниматься технологическим обеспечением единого киберпространства, стратегическим планированием операций,

предупреждением кибератак и оперативным реагированием на них. В качестве одного из подразделений данного центра предлагается создание киберполиции БРИКС.

К основным сферам ведения Центра информационной политики и коммуникаций БРИКС будут относиться вопросы совместных информационных и имиджевых кампаний, международного сотрудничества, внутренних коммуникаций и связей с общественностью.

*** * ***

В условиях стратегического отчуждения Запада и России для РФ важным направлением наращивания своих возможностей в области решения проблем обеспечения кибер- и информационной безопасности выступает сотрудничество со странами БРИКС. Оно может существенно повысить возможности России в рассматриваемой сфере и тем самым повысить интерес к сотрудничеству с ней со стороны стран и институтов Евро-Атлантического сообщества. При этом укрепление мер доверия со странами БРИКС (особенно Бразилией и Индией) позволит России получить опосредованный канал для убеждения западных стран в непричастности РФ к попыткам повлиять на электоральные циклы в странах Европы и США посредством осуществления кибератак и иных мер в информационной сфере. Таким образом, сотрудничество со странами БРИКС в исследуемой области может содействовать делу постепенного доверия в отношениях России и Запада в целом.

Ссылки / Reference

1. France unveils cyber command in response to 'new era in warfare'. 2016. 16.12. URL: https://www.scmagazineuk.com/france-unveils-cyber-command-in-response-to-new-era-in-warfare/article/579671/ (date of access: 25.06.2018).
2. German army launches new cyber command // DW. 2017. 01.04. URL: http://www.dw.com/en/german-army-launches-new-cyber-command/a-38246517 (date of access: 25.06.2018).
3. Военная доктрина Российской Федерации // Российская газета. 2014. 30.12. URL: https://rg.ru/2014/12/30/doktrina-dok.html (дата обращения: 25.06.2018).
4. Стратегия национальной безопасности // Российская газета. 2015. 31.12. URL: https://rg.ru/2015/12/31/nac-bezopasnost-site-dok.html (дата обращения: 31.05.2018).
5. Brazil lays down the law with Internet 'Bill of Rights' // CNET. 2014. 23.04. URL: https://www.cnet.com/news/brazil-lays-down-the-law-with-internet-bill-of-rights/ (date of access: 25.06.2018).
6. Europol and Brazil agree co-operation on cybercrime. 2017. 11.04. URL: https://www.computerweekly.com/news/450416640/Europol-and-Brazil-agree-co-operation-on-cyber-crime (date of access: 25.06.2018).
7. Protecting interconnected systems in the cyber era. Assocham: PWC, 2015. 19 p.
8. Cyber Swachhta Kendra: BrickerBot: IoT Malware. 2017. 25.04. URL: https://www.cyberswachhtakendra.gov.in/alerts/BrickerBotIoTMalware.html (date of access: 25.06.2018)
9. Golden projects. 1997. 27.06. URL: https://www.cnet.com/news/golden-projects/ (date of access: 25.06.2018)
10. Cybercrimes and cybersecurity bill. republic of South Africa. Capetown: Ministry of Justice and Correctional Service, 2016. 85 p. URL: http://www.justice.gov.za/legislation/bills/CyberCrimesBill2017.pdf (date of access: 25.06.2018).
11. Девятый саммит БРИКС: заявления о дружбе, открытости и сотрудничестве // РИА Новости. 2017. 05.09. URL: https://ria.ru/world/20170905/1501845256.html (дата обращения: 25.06.2018).