Лебедева Е.В.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ГОСУДАРСТВ СНГ: ЭТАПЫ РЕАЛИЗАЦИИ

Аннотация. *В представленной работе автор сконцентрировал внимание на процессе международного диалога по вопросам информационной безопасности, выделив в качестве объекта информационную политику государств СНГ на международной арене. Цель статьи заключается в определении специфики этапов работы государств СНГ над созданием нормативно-правовой и методологической основы обеспечения международной информационной безопасности. Для достижения заявленной цели были поставлены задачи по выявлению ключевых разногласий по данному вопросу с западными коллегами; обозначению динамики понятия «информационная безопасность». Основой теоретико-методологического изучения стали системный подход и историко-сравнительный метод, которые позволили сделать выводы об этапах диалога по вопросам информационной безопасности государств СНГ на региональном и международному ровнях. Научная новизна представленного материала состоит в полученных результатах исследования, касающихся оценки международной политики государств СНГ в информационно-коммуникационной сфере в рамках характеристики этапов ее развития с 1990 – 2015 гг. Анализ деятельности региональных структур в разрезе межгосударственных документов позволил обосновать выводы о стремлении государств СНГ в настоящее время к созданию комплексной и открытой системы международной информационной безопасности, основанной на следовании ее участниками универсальным правилам, позволяющим обеспечить безопасность информационной среды. В качестве результата работы представлена характеристика информационной политики государств СНГ в совокупности ее целей и принципов в разрезе трех периодов ее развития.*

Ключевые слова: *Информационная безопасность, информационное пространство, региональная информационная безопасность, источники угроз, СНГ, ШОС, ООН, киберпреступность, политическая манипуляция, нормативная база.*

Abstract. *In this work the author focuses his attention on the process of international dialogue with regards to the questions of information security. The object of this research is the information policy of CIS countries on international arena. The goal of this article consists in determination of specificity of the stages of CIS countries' work over the establishment of the normative legal and methodological base of ensuring the international information security. In order to achieve the set goal it is necessary to detect the key disputes on this issue with the Western colleagues, as well as to underline the dynamics of the notion "information security". The scientific novelty consists in the acquired results during the course of this research pertaining to the assessment of CIS countries international policy in the information-communication sphere within the framework of the stages of its development throughout the period of 1990-2015. The analysis of the work of regional institutions from a perspective of the intergovernmental documents allowed explaining the conclusions that currently CIS states attempt to establish a complex and open system of international information security based on compliance of its participants to the universal rules that ensure security of information environment. The author presents the characteristic of CIS states information, its goals and principles in the context of three periods of its development.*

Key words: *Normative base, Political manipulation, Cybercrime, United Nations, Shanghai Cooperation Organization (SCO), Commonwealth of Independent States (CIS), Sources of threats, Regional information security, Information space, Information security.*

DOI: 10.7256/2073-8560.2016.4.17585

С течением времени все более очевидным становится влияние информационной среды на политическую, военную, экономическую, культурную и прочие компоненты национальной безопасности государств СНГ. Проведение различных социально-экономических, политических и иных преобразований на государственном уровне становится невозможным без использования информационно-коммуникативных технологий. Актуальность исследования процесса обеспечения информационной безопасности (ИБ) связана, в первую очередь, с неуклонно возрастающей зависимостью всех областей современной жизни общества от развития информационно-коммуникационной структуры. Данная зависимость приводит к возможности глобального воздействия на мировое, региональные и национальные информационные сферы, в результате чего возникает единое (интегрированное) информационное пространство. Научная новизна представленного материала состоит в полученных результатах исследования, касающихся оценки международной политики государств СНГ в информационно-коммуникационной сфере в рамках характеристики этапов ее развития с 1990 – 2015 гг.

В представленной работе автор сконцентрировал внимание на процессе международного диалога по вопросам информационной безопасности, выделив в качестве объекта информационную политику государств СНГ на международной арене. Цель статьи заключается в определении специфики этапов работы государств СНГ над созданием нормативно-правовой и методологической основы обеспечения международной информационной безопасности. Для достижения заявленной цели были поставлены задачи по выявлению ключевых разногласий по данному вопросу с западными коллегами; обозначению динамики понятия «информационная безопасность». Основой теоретико-методологического изучения стали системный подход и историко-сравнительный метод, которые позволили сделать выводы об этапах диалога по вопросам информационной безопасности государств СНГ на региональном и международному ровнях.

Вместе с тем, колоссальные возможности данной области априори содержат в себе не только конструктивный, но и деструктивный потенциал, о принципах и способах регулирования которого ведутся политические дискуссии на национальном и международном уровнях. Информационно-коммуникационные технологии (ИКТ) в современном мире становятся стратегическим политическим инструментом. Современные исследователи отмечают уязвимость и разнообразие форм негативного воздействия на информационно-коммуникационную сферу, в том числе информационный криминал, информационный терроризм, искажение и сокрытие фактов, информационная война.

Все чаще опасения вызывает возможность применения ИКТ с целью достижения военно-политического превосходства, в качестве инструмента силового противоборства и международного терроризма. Как отмечал еще в начале 2000-х гг. профессор МГИМО А.В. Крутских, а сейчас – спецпредставитель Президента РФ по вопросам международного сотрудничества в области ИБ (с 2014 г.), «…озабоченность возникает, прежде всего, в связи с возможностью применения колоссального потенциала информационно-кибернетических технологий в интересах обеспечения военно-политического превосходства, силового противоборства, шантажа. Возникает соблазн воспользоваться преимуществами в обладании информационными технологиями для информационной, политической, экономической, культурной и военной экспансии» [1]. Таким образом, разработка и реализация комплекса эффективных мер требуют согласованных действий и комплексного подхода не только на национальном, но и на межгосударственном уровне.

На международном уровне ежегодно с 1998 г. Россия выступает инициатором принятия в ООН резолюции «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности». Каждый год происходит регулярное дополнение документа: расширяется спектр рисков и угроз, с которыми сталкивается международное и национальное информационные пространства, выдвигаются предложения по координации международных усилий.

В начале 2000-х гг. в рамках обсуждения в системе ООН информационных угроз можно выделить два основных направления, касающихся представления о сути и принципах обеспечения международной информационной безопасности (МИБ). Представители государств евро-атлантического региона склонялись, в первую очередь, к необходимости разработки мер по нейтрализации угроз преступного (террористического) характера. Усилия европейских го-

DOI: 10.7256/2073-8560.2016.4.17585

сударств в этот период были сконцентрированы на разработке методологических основ борьбы с киберпреступностью, больше внимания уделяя прикладным вопросам ИБ (защита сетей и информационных систем государства). С другой стороны, в первую очередь представители государств-участников СНГ, были обеспокоены не только техническими аспектами данного вопроса, но также возрастающей (особенно в отношении постсоветского пространства) угрозой информационной пропаганды, политического манипулирования и дезинформации. Предлагался комплексный подход, в основе которого была заложена потребность в предотвращении угрозы информационной войны.

После принятия в 2004 г. очередной российской резолюции в ООН, которая намечала запуск работы международных правительственных экспертов с целью выработки практических решений, значительные разногласия участников дискуссии затруднили конструктивный диалог по МИБ.

После того, как обсуждение вопросов ИБ в системе ООН не принесло желаемых результатов, данная работа активизировалась на уровне региональных организаций Евразии – СНГ, ШОС, ОДКБ.

В 2006 г. на учредительном заседании по МИБ группы экспертов государств-членов ШОС было принято решение выработать к саммиту в Бишкеке (2007 г.) план действий и определить пути разрешения проблем МИБ[2]. В итоге, в 2007 г. была подписана Бишкекская декларация, а также утвержден План действий по обеспечению информационной безопасности**.**

Ключевым этапом на пути решения вопросов безопасности регионального информационного пространства стало подписание в 2009 г. Межправительственного соглашения государств-членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности (вступило в силу в 2011 г.). На наднациональном уровне Соглашение конкретизировало суть ключевых понятий, ввело четкие определения угроз в области информационной безопасности, определило основные принципы, направления и механизмы взаимодействия государств по данным проблемам.

Указанное Соглашение определяет следующий круг угроз МИБ [3]:

1) разработка и применение информационного оружия, подготовка и ведение информационной войны;
2) информационный терроризм;
3) информационная преступность;
4) использование доминирующего положения в информационном пространстве в ущерб интересам и безопасности других государств;
5) распространение информации, наносящей вред общественно-политической и социально-экономической системам, духовной, нравственной и культурной среде других государств;
6) угрозы безопасному, стабильному функционированию глобальных и национальных информационных инфраструктур, имеющие природный и (или) техногенный характер.

С принятием данного документа региональное пространство подтвердило намерение создать всеохватывающую систему обеспечения ИБ в контексте международной политики.

В 2012 г. на заседании группы экспертов ШОС по ИБ обсуждались вопросы, связанные с практической реализацией положений Соглашения [4].

В январе 2015 г. государствами-членами ШОС внесены в качестве официального документа ООН «Правила поведения в области обеспечения международной информационной безопасности». В Правилах обозначена необходимость предотвращения конфликтов в информационной сфере путем закрепления обязательства государств не применять информационные технологии в деструктивных целях, в т.ч. с целью вмешательства во внутренние дела иных государств, а также обязательства отказаться от применения силы или угрозы силой для разрешения конфликтов в информационной сфере [5].

В Стратегии развития ШОС до 2025 г. сказано, что «приоритетное значение государства-члены ШОС будут придавать взаимодействию с ООН, прежде всего в вопросах поддержания международного мира и безопасности …Приоритетными направлениями будут … … работа по тематике международной информационной безопасности на базе разработанного ШОС проекта «Правил поведения государств в области обеспечения международной информационной безопасности» [6].

Анализ угроз МИБ в рамках ШОС сегодня представляет собой важнейшее стратегическое направление по созданию единого информационного пространства, в равной степени безопасного для всех участников. Участие крупнейшего государства и важнейшего партнера России по

DOI: 10.7256/2073-8560.2016.4.17585

международному диалогу – Китайской Народной Республики придает данной работе стратегический характер.

Наряду с сотрудничеством по ИБ государств-членов ШОС, в рамках СНГ также проводится активная работа по совершенствованию и развитию правовой и организационной базы в области обеспечения безопасности. В 1996 г. была принята Концепция формирования информационного пространства Содружества независимых государств. Концепция носила рекомендательный характер и представляла собой систему согласованных взглядов на цели и приоритеты в сферах сотрудничества государств-участников СНГ в развитии международных информационных обменов [7]. В 1998 г. Решением Совета глав правительств СНГ от 25 ноября 1998 г. был утвержден Перспективный план подготовки документов и мероприятий по реализации Концепции.

В 1999 г. в рамках Содружества был принят важнейший документ – Концепция информационной безопасности государств-участников СНГ в военной сфере [8]. Источниками угроз были обозначены следующие: компьютерная преступность, отсутствие нормативно-правовой базы, нарушение регламента сбора и передачи информации, разведывательная деятельность со стороны иностранных государств, отсутствие необходимой инфраструктуры и т.д. Документ также обозначает потребность государств в конструировании общего безопасного информационно-коммуникационного пространства путем превенции угроз технического характера, противодействия сетевым угрозам, нормативной работы, развития соответствующей инфраструктуры.

Со своей стороны, Межпарламентская Ассамблея государств Содружества совместно с Региональным содружеством в области связи (на основании Соглашения о взаимодействии от 2002 г.) в целях развития и сближения национального законодательства в сфере информационных технологий ведет разработку модельных законов в сфере связи и информатизации, которые используются государствами СНГ при разработке новых законодательных актов и дополнении существующих. Например, были приняты следующие модельные законодательные акты: «О международном информационном обмене», «О принципах регулирования информационных отношений в государствах-участниках СНГ», «Об информатизации, информации и защите информации» и пр. [9].

В 2004 г. по решению Координационного совета государств-участников СНГ по информатизации при Региональном содружестве в области связи создается Комиссия по информационной безопасности. В задачи новой структуры входит выработка рекомендаций по взаимодействию государств-участников, организация обмена опытом, подготовка предложений по приоритетным направлениям деятельности, в т.ч. гармонизации национального законодательства, прогнозирование возможных угроз, а также выработка рекомендаций по нейтрализации существующих угроз и т.д. [10].

Результатом работы Комиссии по ИБ стал ряд важнейших межправительственных документов в сфере ИКТ [11]:

1) Стратегия сотрудничества государств-участников СНГ в сфере информатизации и План действий по ее реализации до 2010 г. в части информационной безопасности;
2) Концепция сотрудничества государств-участников СНГ 2008 г. в сфере обеспечения информационной безопасности и Комплексного плана мероприятий по ее реализации до 2010 г.
3) Стратегия сотрудничества государств-участников СНГ в построении и развитии информационного общества и План действий до 2015 г. [12].
4) Соглашение 2013 г. о сотрудничестве государств-участников СНГ в области обеспечения информационной безопасности (угрозами здесь названы также информационный терроризм, применение информационного оружия и информационная преступность).

В 2008 г. государства Содружества одобряют Концепцию сотрудничества государств-участников в сфере обеспечения информационной безопасности, где четко обозначены современные угрозы информационного пространства, согласована терминологическая база, обозначены методы и основные направления сотрудничества [13].

К угрозам ИБ в Концепции отнесены следующие:

1) осуществление действий в интересах получения несанкционированного доступа к информации государств-участников СНГ;
2) проведение третьими странами в информационном пространстве мероприятий, направленных на дестабилизацию социально-политической обстановки;

DOI: 10.7256/2073-8560.2016.4.17585

3) деятельность организованных преступных групп и сообществ, в том числе экстремистской и террористической направленности в информационной сфере СНГ;
4) обострение международной конкуренции за обладание стратегически важной информацией и стремление ряда стран к доминированию в мировом информационном пространстве;
5) введение ограничений, ущемляющих интересы государств-участников СНГ в информационной сфере, а также основные права и свободы граждан;
6) нарушение исторически сложившихся в СНГ научно-технических связей;
7) природные и техногенные катастрофы, а также другие физические явления, приводящие к сбоям и отказам информационных систем;
8) зависимость от третьих стран-производителей программных и аппаратных средств при создании и развитии информационной структуры.

Также в 2011 г. постоянные представители при ООН России, Китая, Таджикистана, Узбекистана предложили к рассмотрению документ «Правила поведения в области обеспечения международной информационной безопасности». Вместе с тем, в этом же году российскими экспертами был подготовлен проект конвенции ООН «Об обеспечении международной информационной безопасности». Оба документа, по сути, подводят международное сообщество к принятию идеи о необходимости всестороннего изучения и регулирования информационной среды. В частности, в проекте конвенции представлено определение информационной войны – «противоборства между двумя или более государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим структурам, подрыва политической, экономической и социальной систем, массированной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны» [14].

Работа над созданием комплексной нормативно-правовой и методологической основы по обеспечению безопасности информационной сферы в евразийском регионе регулярно проводится с конца XX в. Условно в данном процессе можно выделить следующие этапы.

Первый этап включает в себя параллельную работу в рамках СНГ и ООН.

На региональном уровне первоначально работа велась в основном в рамках СНГ в области непосредственного установления коммуникаций и поддержания информационного сообщения между бывшими союзными государствами. Были приняты законы, касающиеся поддержания информационного обмена и сообщения, а также защиты государственной информации, установления каналов культурных связей между государствами. В указанный период действия мотивировались необходимостью «смягчения» социального, политического и экономического кризиса, в котором оказались постсоветские государства. На данном этапе перед Содружеством стоит первоочередная задача в создании базы для обмена информацией и решении иных, по большей части практических аспектов информационного взаимодействия.

Вместе с тем с конца 1990-х гг. на международном уровне российской стороной предпринимались попытки по обозначению и регулированию сферы информатизации в более широком ее смысле – с учетом процессов идеологического характера и возможностей деструктивного информационного воздействия на общество. В целом, данный период работы принес определенные успехи, однако подойти вплотную к вопросам превенции конкретных угроз оказалось затруднительно ввиду разногласий ключевых участников международного политического процесса: США и Европы с одной стороны, и государств Евразии – с другой.

Второй этап работы над проблемами обеспечения МИБ связан с «перемещением» центра обсуждения данных вопросов с международного (в рамках ООН) на региональный уровень (ШОС, СНГ). В это время фокус работы сконцентрирован не только на аспектах практической защиты информации, но и на проблеме принципов использования информации как инструмента власти. Продвигается работа над ключевыми понятиями данной области, обозначаются возможные угрозы, обсуждаются способы борьбы с ними.

Началом третьего этапа можно условно считать 2010 г., когда по инициативе России Комиссия ООН по предупреждению преступности и уголовному правосудию приняла решение создать открытую межправительственную группу экспертов для всеобъемлющего изучения проблем киберпреступности. На данном этапе про-

DOI: 10.7256/2073-8560.2016.4.17585

исходит «вывод» идей – вызревших и частично проработанных в региональном контексте – на международный уровень. Если в конце 1990-х – начале 2000-х гг. международное сообщество еще не было готово обсуждать вопросы информационного противоборства и войны, то после череды международных революционных и военных событий в Центральной Азии, Ближнем Востоке и государствах СНГ стала очевидна необходимость диалога по данным вопросам.

На основании рассмотренных межгосударственных документов можно сделать вывод о постепенном и неуклонном пересмотре понятия «информационная безопасность». С течением времени происходит расширение терминологической базы данного феномена, дополнение новыми дефинициями. Информационная политика понимается как высокодинамичный процесс, масштаб которого, равно как и значимость, с течением времени возрастает под влиянием современных политических реалий национального, регионального и международного уровня.

В целом, позиции государств СНГ свойственен комплексный подход к рассмотрению вопросов ИБ: изучаются как техническая сторона вопроса, так и идеологическая (или информационно-психологическая). В частности, акцентируется внимание на необходимости демилитаризации сферы безопасности, на недопущении использования информационных технологий в военных целях, на принятии правил поведения, гарантирующих свободное и безопасное использование информационной среды.

В свою очередь, взгляды западных коллег по диалогу по ИБ имеют существенные отличия: акцент ставится на борьбе с киберпреступностью, безопасностью информационных структур и сетей, на вопросах защиты информации, имеющий ограничения в доступе, также на предотвращении попадания новейших информационных разработок в руки к преступным группировкам и криминальным элементам. Что касается вопросов информационно-психологического противоборства, в том числе с использованием новейших коммуникационных систем, то их относят к вопросам, которые не поддаются точному измерению, для которых не отработана методика анализа, высказываются опасения в части ограничения свободы информации и т.д. В итоге длительное «неучастие» западноевропейского международного сообщества в обсуждении важнейшей проблематики информационно-коммуникационной сферы являлось препятствием всестороннего регулирования данной области в рамках международного права.

Таким образом, принимая во внимание позицию международного сообщества по данному вопросу, Россия, будучи одним из ключевых государств СНГ и евразийского региона, продолжает развивать понятие ИБ на платформе Содружества независимых государств и Шанхайской организации сотрудничества. Происходит регулярная работа по согласованию понятий ИБ, разработке принципов и подходов к превенции современных рисков и угроз. Предпринимаются конкретные меры по созданию единого информационного пространства. Благодаря усилиям государств Содружества в рамках ООН также происходит постепенный «пересмотр» взглядов на вопросы ИБ.

Информационная политика государств СНГ нацелена на создание комплексной безопасности с учетом интересов не только региональных государств, но также всего международного сообщества путем следования «универсальным» правилам. Также политика региональных государств носит открытый характер и основана на стремлении к созданию регулируемого информационного пространства, безопасного для всех его участников и пользователей.

БИБЛИОГРАФИЯ

1. А.В. Крутских. Война или мир: международные аспекты информационной безопасности. Научные и методологические проблемы информационной безопасности (сборник статей) под ред. В.П. Шерстюка. – М.: МЦНМО, 2004.
2. О заседании в Пекине Группы экспертов государств-членов ШОС по международной информационной безопасности. 31.10.2006. [Электронный ресурс] // МИД России [Офиц.сайт]. URL: http://www.mid.ru/mezdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/UsCUTiw2pO53/content/id/389112/pop_up?_101_INSTANCE_UsCUTiw2pO53_viewMode=tv&_101_INSTANCE_UsCUTiw2pO53_qrIndex=0 (дата обращения: 14.11.2015)
3. О вступлении в силу Соглашения между правительствами государств-членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности. [Электронный ресурс] //

DOI: 10.7256/2073-8560.2016.4.17585

Министерство иностранных дел Российской Федерации [Офиц.сайт]. 14.06.2011. URL: http://www.mid.ru/mezdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/UsCUTiw2pO53/content/id/203770 (дата обращения: 15.11.2015)
4. Заседание Группы экспертов государств-членов ШОС по международной информационной безопасности [Электронный ресурс] // Институт проблем информационной безопасности [Офиц. сайт]. 16.03.2012. URL: http://www.iisi.msu.ru/news/news55/ (дата обращения: 14.11.2015)
5. Правила поведения в области обеспечения международной информационной безопасности [Электронный ресурс] // Министерство иностранных дел Российской Федерации. [Офиц.сайт]. URL: http://archive.mid.ru/bdomp/ns-dmo.nsf/c85969b2329a429944257d5600225ebb/44257b100055f7e6c3257db4004192e4/$FILE/A%2069%20723%20En.pdf (дата обращения: 04.12.2015)
6. Стратегия развития ШОС до 2025 года [Электронный ресурс] // Сайт председательства Российской Федерации в ШОС в 2014 – 2015 годах [Офиц.сайт]. URL: http://sco-russia.ru/documents/ (дата обращения: 10.11.2015)
7. КОНЦЕПЦИЯ формирования информационного пространства Содружества Независимых Государств [Электронный ресурс] // Исполнительный комитет СНГ [Офиц.сайт]. URL: http://cis.minsk.by/page.php?id=7548 (дата обращения: 02.11.2015)
8. Список конвенций, концепций и программ, принятых в рамках СНГ [Электронный ресурс] // Постоянное представительство Российской Федерации при СНГ [Офиц.сайт]. URL: http://www.cismission.mid.ru/ii6.html (дата обращения: 02.11.2015)
9. ИНФОРМАЦИЯ о модельных законах в сфере связи и информатизации, принятых и разрабатываемых Межпарламентской Ассамблеей государств-участников Содружества Независимых Государств, с участием Регионального содружества в области связи [Электронный ресурс] // Исполнительный комитет СНГ [Офиц.сайт]. URL: http://www.cis.minsk.by/page.php?id=16318 (дата обращения: 02.11.2015)
10. Задачи и функции (из положения о Комиссии) [Электронный ресурс] // Региональное содружество в области связи [Офиц.сайт]. URL: http://www.rcc.org.ru/index.php?option=com_content&view=article&id=161&Itemid=909 (дата обращения: 01.11.2015)
11. Комиссия РСС по информационной безопасности. [Электронный ресурс] // Региональное содружество в области связи [Офиц.сайт]. URL: http://www.rcc.org.ru/index.php?option=com_content&view=section&id=39&Itemid=549 (дата обращения: 01.11.2015)
12. Стратегия сотрудничества государств-участников СНГ в построении и развитии информационного общества и Плане действий по её реализации на период до 2015 года [Электронный ресурс] // Региональное содружество в области связи [Офиц.сайт]. URL: http://www.rcc.org.ru/index.php?option=com_content&view=article&id=61&Itemid=383 (дата обращения: 14.11.2015)
13. РЕШЕНИЕ о Концепции сотрудничества государств-участников Содружества Независимых Государств в сфере обеспечения информационной безопасности и о Комплексном плане мероприятий по реализации Концепции сотрудничества государств-участников Содружества Независимых Государств в сфере обеспечения информационной безопасности на период с 2008 по 2010 год [Электронный ресурс] // Интернет-портал СНГ [Офиц.сайт]. URL: http://www.e-cis.info/page.php?id=20229 (дата обращения: 14.11.2015)
14. Конвенция об обеспечении международной информационной безопасности (концепция) [Электронный ресурс] // Совет Безопасности Российской Федерации [Офиц.сайт]. URL: http://www.scrf.gov.ru/documents/6/112.html (дата обращения: 15.11.2015)
15. Петухов А.Ю., Ивлиева П.Д. Психолингвистический анализ информационного сопровождения украинского кризиса в германских сми в 2014 году // Национальная безопасность / nota bene. – 2015. – № 4. – С. 548-556. DOI: 10.7256/2073-8560.2015.4.15770 URL: http://www.nbpublish.com/library_read_article.php?id=-34253
16. Старкин С.В. Противостояние в киберпространстве в контексте развития военной стратегии. // Политика и Общество.-2015.-№ 3.-С. 395-406. DOI: 10.7256/1812-8696.2015.3.14566 URL: http://nbpublish.com/library_read_article.php?id=-32967
17. Шульц В.Л., Кульба В.В., Шелков А.Б., Чернов И.В.. Информационное управление в условиях глобализации и геополитического противоборства. // Национальная безопасность / nota bene.-2015.-№ 2.-С. 202-243. DOI: 10.7256/2073-8560.2015.2.14622 URL: http://www.nbpublish.com/library_read_article.php?id=-33291
18. Петренко А.И. Теоретические основы организации противодействия использованию арсенала сил, средств и методов информационно-психологической войны в политических целях // Тренды и управление. – 2014. – 2. – С. 154 – 167. DOI: 10.7256/2307-9118.2014.2.12412.

DOI: 10.7256/2073-8560.2016.4.17585

19. Яшина А.В. Информационные технологии и трансформация системы обеспечения безопасности. // Вопросы безопасности. – 2014. – 4. – С. 104 – 130. DOI: 10.7256/2409-7543.2014.4.13332. URL: http://www.e-notabene.ru/nb/article_13332.html

REFERENCES (TRANSLITERATED)

1. A.V. Krutskikh. Voina ili mir: mezhdunarodnye aspekty informatsionnoi bezopasnosti. Nauchnye i metodologicheskie problemy informatsionnoi bezopasnosti (sbornik statei) pod red. V.P. Sherstyuka. – M.: MTsNMO, 2004.
2. O zasedanii v Pekine Gruppy ekspertov gosudarstv-chlenov ShOS po mezhdunarodnoi informatsionnoi bezopasnosti. 31.10.2006. [Elektronnyi resurs] // MID Rossii [Ofits.sait]. URL: http://www.mid.ru/mezdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/UsCUTiw2pO53/content/id/389112/pop_up?_101_INSTANCE_UsCUTiw2pO53_viewMode=tv&_101_INSTANCE_UsCUTiw2pO53_qrIndex=0 (data obrashcheniya: 14.11.2015)
3. O vstuplenii v silu Soglasheniya mezhdu pravitel'stvami gosudarstv-chlenov ShOS o sotrudnichestve v oblasti obespecheniya mezhdunarodnoi informatsionnoi bezopasnosti. [Elektronnyi resurs] // Ministerstvo inostrannykh del Rossiiskoi Federatsii [Ofits.sait]. 14.06.2011. URL: http://www.mid.ru/mezdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/UsCUTiw2pO53/content/id/203770 (data obrashcheniya: 15.11.2015)
4. Zasedanie Gruppy ekspertov gosudarstv-chlenov ShOS po mezhdunarodnoi informatsionnoi bezopasnosti [Elektronnyi resurs] // Institut problem informatsionnoi bezopasnosti [Ofits.sait]. 16.03.2012. URL: http://www.iisi.msu.ru/news/news55/ (data obrashcheniya: 14.11.2015)
5. Pravila povedeniya v oblasti obespecheniya mezhdunarodnoi informatsionnoi bezopasnosti [Elektronnyi resurs] // Ministerstvo inostrannykh del Rossiiskoi Federatsii. [Ofits.sait]. URL: http://archive.mid.ru/bdomp/ns-dmo.nsf/c85969b2329a429944257d5600225ebb/44257b100055f7e6c3257db4004192e4/$FILE/A%2069%20723%20En.pdf (data obrashcheniya: 04.12.2015)
6. Strategiya razvitiya ShOS do 2025 goda [Elektronnyi resurs] // Sait predsedatel'stva Rossiiskoi Federatsii v ShOS v 2014 – 2015 godakh [Ofits.sait]. URL: http://sco-russia.ru/documents/ (data obrashcheniya: 10.11.2015)
7. KONTsEPTsIYa formirovaniya informatsionnogo prostranstva Sodruzhestva Nezavisimykh Gosudarstv [Elektronnyi resurs] // Ispolnitel'nyi komitet SNG [Ofits.sait]. URL: http://cis.minsk.by/page.php?id=7548 (data obrashcheniya: 02.11.2015)
8. Spisok konventsii, kontseptsii i programm, prinyatykh v ramkakh SNG [Elektronnyi resurs] // Postoyannoe predstavitel'stvo Rossiiskoi Federatsii pri SNG [Ofits.sait]. URL: http://www.cismission.mid.ru/ii6.html (data obrashcheniya: 02.11.2015)
9. INFORMATsIYa o model'nykh zakonakh v sfere svyazi i informatizatsii, prinyatykh i razrabatyvaemykh Mezhparlamentskoi Assambleei gosudarstv-uchastnikov Sodruzhestva Nezavisimykh Gosudarstv, s uchastiem Regional'nogo sodruzhestva v oblasti svyazi [Elektronnyi resurs] // Ispolnitel'nyi komitet SNG [Ofits.sait]. URL: http://www.cis.minsk.by/page.php?id=16318 (data obrashcheniya: 02.11.2015)
10. Zadachi i funktsii (iz polozheniya o Komissii) [Elektronnyi resurs] // Regional'noe sodruzhestvo v oblasti svyazi [Ofits.sait]. URL: http://www.rcc.org.ru/index.php?option=com_content&view=article&id=161&Itemid=909 (data obrashcheniya: 01.11.2015)
11. Komissiya RSS po informatsionnoi bezopasnosti. [Elektronnyi resurs] // Regional'noe sodruzhestvo v oblasti svyazi [Ofits.sait]. URL: http://www.rcc.org.ru/index.php?option=com_content&view=section&id=39&Itemid=549 (data obrashcheniya: 01.11.2015)
12. Strategiya sotrudnichestva gosudarstv-uchastnikov SNG v postroenii i razvitii informatsionnogo obshchestva i Plane deistvii po ee realizatsii na period do 2015 goda [Elektronnyi resurs] // Regional'noe sodruzhestvo v oblasti svyazi [Ofits.sait]. URL: http://www.rcc.org.ru/index.php?option=com_content&view=article&id=61&Itemid=383 (data obrashcheniya: 14.11.2015)
13. REShENIE o Kontseptsii sotrudnichestva gosudarstv-uchastnikov Sodruzhestva Nezavisimykh Gosudarstv v sfere obespecheniya informatsionnoi bezopasnosti i o Kompleksnom plane meropriyatii po realizatsii Kontseptsii sotrudnichestva gosudarstv-uchastnikov Sodruzhestva Nezavisimykh Gosudarstv v sfere obespecheniya informatsionnoi bezopasnosti na period s 2008 po 2010 god [Elektronnyi resurs] // Internet-portal SNG [Ofits.sait]. URL: http://www.e-cis.info/page.php?id=20229 (data obrashcheniya: 14.11.2015)

DOI: 10.7256/2073-8560.2016.4.17585

14. Konventsiya ob obespechenii mezhdunarodnoi informatsionnoi bezopasnosti (kontseptsiya) [Elektronnyi resurs] // Sovet Bezopasnosti Rossiiskoi Federatsii [Ofits.sait]. URL: http://www.scrf.gov.ru/documents/6/112.html (data obrashcheniya: 15.11.2015)
15. Petukhov A.Yu., Ivlieva P.D. Psikholingvisticheskii analiz informatsionnogo soprovozhdeniya ukrainskogo krizisa v germanskikh smi v 2014 godu // Natsional'naya bezopasnost' / nota bene. – 2015. – № 4. – S. 548-556. DOI: 10.7256/2073-8560.2015.4.15770 URL: http://www.nbpublish.com/library_read_article.php?id=-34253
16. Starkin S.V. Protivostoyanie v kiberprostranstve v kontekste razvitiya voennoi strategii. // Politika i Obshchestvo.-2015.-№ 3.-C. 395-406. DOI: 10.7256/1812-8696.2015.3.14566 URL: http://nbpublish.com/library_read_article.php?id=-32967
17. Shul'ts V.L., Kul'ba V.V., Shelkov A.B., Chernov I.V.. Informatsionnoe upravlenie v usloviyakh globalizatsii i geopoliticheskogo protivoborstva. // Natsional'naya bezopasnost' / nota bene.-2015.-№ 2.-C. 202-243. DOI: 10.7256/2073-8560.2015.2.14622 URL: http://www.nbpublish.com/library_read_article.php?id=-33291
18. Petrenko A.I. Teoreticheskie osnovy organizatsii protivodeistviya ispol'zovaniyu arsenala sil, sredstv i metodov informatsionno-psikhologicheskoi voiny v politicheskikh tselyakh // Trendy i upravlenie. – 2014. – 2. – C. 154 – 167. DOI: 10.7256/2307-9118.2014.2.12412.
19. Yashina A.V. Informatsionnye tekhnologii i transformatsiya sistemy obespecheniya bezopasnosti. // Voprosy bezopasnosti. – 2014. – 4. – C. 104 – 130. DOI: 10.7256/2409-7543.2014.4.13332. URL: http://www.e-notabene.ru/nb/article_13332.html

DOI: 10.7256/2073-8560.2016.4.17585