УДК [327+316.012+004] (985+100) (045)

ТАМИЦКИЙ Александр Михайлович, *кандидат политических наук, доцент кафедры политологии и социологии института социально-гуманитарных и политических наук Северного (Арктического) федерального университета имени М.В. Ломоносова. Автор 26 научных публикаций*

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК ФАКТОР МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ В АРКТИЧЕСКОМ РЕГИОНЕ

В статье обращается внимание на возникающие угрозы и риски в современном информационном пространстве и на необходимость формирования системы информационной безопасности как на национальном, так и международном уровне. Представлено соотношение обеспеченности информационной безопасности циркумполярных государств, в т. ч. Российской Федерации, в условиях интенсификации международного сотрудничества и конкуренции в Арктическом регионе.

Ключевые слова: *Арктический регион, информационное пространство, информационная безопасность.*

Арктика в последние десятилетия приобретает новое геополитическое значение в современном мире. Интерес к региону продиктован его стратегическим потенциалом в обеспечении био-, эко-, энергоресурсами, транспортными коммуникациями, что рассматривается сегодня как основа для обеспечения национальных интересов государств, которые не ограничены циркумполярным миром, располагаются за его пределами.

Заинтересованные государства в различных формах рассматривают возможности укрепления и расширения своего влияния в Арктическом регионе. Наращивание собственного, в т. ч. числе военного, потенциала будет особенно интенсивно происходить в ближайшие годы. Вследствие этого начнет обостряться конкурентная борьба за Арктику [6, с. 160].

Вместе с тем большое значение в развитии международных отношений будут играть угрозы и риски в информационной сфере, которые станут фактором сотрудничества и соперничества между государствами. В настоящих условиях показателем военного могущества государства становится его способность действенно применять существующие информационные ресурсы и инфраструктуру для обеспечения обороноспособности страны.

Серьезную озабоченность станет вызывать стремление отдельных государств и их объединений контролировать мировое информационное пространство, разработка ими концепций ведения информационных войн с целью несанкционированного доступа к информационным ресурсам, разрушающего влияния на информационные и телекоммуникационные системы других стран благодаря использованию информационного оружия [12]. Объектами данного вида вооружения являются не только информационно-технические системы и сведения, но и психика и общественное сознание.

Современные IT-компании, специализирующиеся на противодействии информационным угрозам, систематически обнаруживают новейшее программное обеспечение, созданное для шпионажа и диверсий на особо важных инфраструктурных объектах и в компьютерных сетях, в т. ч. числе государственных учреждений. Наиболее яркими примерами последнего времени являются вирус Stuxnet, атаковавший в 2010 году ядерные объекты в Иране, вредоносная программа Flame, обнаруженная в компьютерных системах на Ближнем Востоке, и сеть кибершпионажа «Красный октябрь», функционировавшая по меньшей мере 5 лет и похищавшая информацию с компьютеров органов государственной власти многих стран. Отметим, что особенностью информационного оружия такого типа является его скрытое применение, что затрудняет его идентификацию на ранних этапах.

Российская Федерация также является объектом несанкционированного информационного вмешательства в деятельность государственных учреждений и коммерческих организаций. По данным ФСБ России, только на сайты президента, Госдумы и Совета Федерации осуществляется до 10 тысяч атак ежедневно [5]. В 2013 году наиболее крупными событиями стали взлом сайта полномочного представителя президента на Дальнем Востоке, хакерская атака на телеканал Russia Today и другие.

Эксперты по безопасности отмечают, что ущерб от киберпреступлений для всего мира ежегодно составляет 0,3–1 трлн долл., что равняется 0,4–1,4 % мирового ВВП [28, p. 3]. Только в России суммарный ущерб в 2012 году составил около 2 млрд долл. [23].

Сегодня уже не является тайной, что на государственном уровне реализуются программы глобального информационного мониторинга и сбора данных. Например, Центром правительственной связи Великобритании совместно с Агентством национальной безопасности США в 2011 году запущена программа Tempora [18]; с 2003 года реализуется программа интернет-цензуры и компьютерного слежения «Золотой щит» в КНР [24] и т. д.

Названные глобальные тенденции развития информационного пространства актуализировали проблему обеспечения его безопасности современным государством. Вместе с тем в научной литературе до сих пор отсутствует однозначное определение понятия «информационная безопасность» [3]. Как правило, под ней понимается часть общей системы безопасности личности, общества и государства в информационной сфере.

Информационная безопасность включает в себя три значимые группы проблем [1]:

1. Проблемы гуманитарного характера, связанные с неправомерным использованием персональных данных граждан, вмешательством в частную жизнь, дезинформацией;

2. Проблемы экономического и правового характера, связанные с кражей, искажением коммерческой и финансовой информации, неправомерным использованием интеллектуальной собственности, промышленным шпионажем и информационными кампаниями, направленными на причинение имиджевого ущерба организациям;

3. Проблемы политического характера, связанные с информационными войнами, электронной разведкой, нацеленной на раскрытие государственной тайны, доступом к автоматическим системам управления критически важных объектов государства, искажением ин-

формации и дезинформацией руководителей различного уровня государственной власти.

Следует признать, что проблема информационной безопасности фактически охватывает все сферы общественной и государственной жизни, затрагивает реализацию национальных интересов любой страны.

Вопрос обеспечения международной информационной безопасности находится на повестке дня по меньшей мере с 1998 года, когда Российская Федерация впервые предложила принять соглашение в Генеральной Ассамблее ООН о снижении риска информационных конфликтов. В то время лишь несколько государств обладали принятыми национальными программами в области информационной безопасности. На сегодняшний день уже более половины всех членов ООН в той или иной степени прикладывают организационные и правовые усилия для обеспечения сети реагирования на критические угрозы [27, p. 1].

Страны Арктического региона также поддержали уже сложившуюся мировую тенденцию формирования системы противодействия негативному информационному воздействию.

На первых этапах на национальном уровне утверждаются стратегии информационной безопасности. Такие документы принимаются странами «арктической восьмерки»: Российской Федерацией (2000 год) [4], США (2003, 2011–2012 годы) [18, 22, 30], Швецией (2006 год) [26], Финляндией (2008, 2013 годы) [16, 33], Данией (2009 год) [15], Канадой (2010 год) [14], Норвегией (2012 год) [21]. В них предлагаются государственные модели обеспечения информационной безопасности, их механизмы, цели и инфраструктура. Однако приходится признать, что на уровне принятых документов отсутствует единое понимание проблем информационной безопасности и приоритетов ее формирования. Данное обстоятельство свидетельствует об отсутствии сложившегося международного подхода к противостоянию возникающим информационным угрозам и рискам.

В странах Арктического региона, а также других государствах, для которых представляет интерес территория Арктики, система информационной безопасности включает деятельность специализированных служб, направленную на защиту информационного пространства страны и проведение специальных операций против противника. В частности, в США киберкомандование (USCYBERCOM) было основано в 2009 году, его задачами являются защита военных сетей от кибератак, проведение собственных кибератак и операций, обеспечивающих свободу действий США и их союзников в киберпространстве и блокирующих аналогичные действия противника [31]. Подобные структуры уже созданы в Китае, НАТО, в Эстонии. Министерство обороны Российской Федерации заявило о создании подобных кибервойск лишь к концу 2013 года [2].

В Российской Федерации формирование государственной системы информационной безопасности продиктовано Стратегией национальной безопасности Российской Федерации до 2020 года, где говорится о важности «создания единой системы информационно-телекоммуникационной поддержки нужд системы обеспечения национальной безопасности» [9], а также Доктриной информационной безопасности РФ, где обосновывается значимость создания и совершенствования системы информационной безопасности в Российской Федерации. Все перечисленное согласуется с Основами государственной политики Российской Федерации в Арктике на период до 2020 года и дальнейшую перспективу в сфере развития информационных технологий и обеспечения военной безопасности [7].

В России, как и в большинстве стран мира, функционируют государственные органы противодействия виртуальным угрозам: МВД (Управление «К»), ФСБ [8], Федеральная служба по техническому и экспортному контролю. Таким образом, российская система предотвращения информационных угроз находится на пути своего становления и требует дальнейшего совершенствования.

Срочность формирования действенной системы информационной безопасности Россий-

ской Федерации диктуется рядом обстоятельств. Так, интерактивная карта киберопасности [17], работающая по методике HostExploit, свидетельствует о невыгодном положении страны в рейтинге глобальной безопасности. Согласно полученной статистике, мировым лидером по распространенности вредоносных действий в информационных сетях по данным на сентябрь 2013 года стала Россия (с индексом 359,3 по 1000-балльной шкале), где обнаружено большое количество ботнетов, серверов ZeuS и фишинговых сайтов. Остальные страны Арктического региона заняли наиболее выгодное положение в этом рейтинге. Так, США заняли 12-е место, Канада – 27-е, Швеция – 32-е, Дания – 59-е место. Наиболее безопасными оказались сети Исландии (196-е место), Норвегии (205-е место) и Финляндии (214-е место). Таким образом, обнаружены значительные вариации по уровню информационной защищенности государств в циркумполярном регионе, где позиция России представляется как наиболее уязвимая перед современными рисками враждебного применения информационных технологий.

Для решения проблемы информационной безопасности на международном уровне представляют интерес сведения о странах-источниках кибератак, которые регистрируются Deutsche Telekom [19]. По итогам сентября 2013 года в Top15 на первом месте по количеству атак были США, на 5-м месте – Канада, на 7-м – Российская Федерация. Эти сведения позволяют характеризовать условно круг информационно-агрессивных государств мира.

Помимо представленных данных о позициях стран в мировом рейтинге информационной незащищенности и агрессивности показательными являются сведения о развитости информационно-коммуникационных технологий среди стран Арктического региона. Заметим, что развитость или отсталость страны по данному показателю не является прямым свидетельством уровня информационной безопасности, а лишь указывает на актуальность для государства и его готовность к использованию всего потенциала современных технологий.

В частности, обратимся к индексу сетевой готовности 2013 года (Networked Readiness Index) [29], который рассчитывается Всемирным экономическим форумом с 2002 года. Данный индекс включает показатели состояния деловой и нормативно-правовой среды с точки зрения информационных технологий, инновационного потенциала, государственной позиции относительно развития информационных технологий, государственных затрат на их развитие и т. д. Примечательно, что большинство стран Арктического региона вошли в первую десятку, которую возглавляет Финляндия. Канада заняла 12-е место, Исландия – 17-е. Российская Федерация занимает 54-е место из 144, поднявшись по сравнению с 2012 годом на две позиции вверх.

Интересны данные Индекса готовности к электронному правительству 2012 года [32], подготавливаемого ООН с 2001 года и включающего сведения о состоянии информационно-коммуникационной инфраструктуры и вебприсутствия органов государственной власти. По уровню готовности к развитию электронного правительства Россия по-прежнему демонстрирует низкие позиции среди стран Арктического региона. Так, Дания, США, Швеция, Норвегия, Финляндия вошли в список стран, которые занимают первые десять позиций. Канада заняла 11-е место, Исландия – 22-е место, Российская Федерация – 27-ю позицию среди 190 стран. Однако по показателю электронного участия Российская Федерация, как и большинство циркумполярных государств, вошла в десятку стран-лидеров. В этом списке Дания заняла 13-е место, Исландия – 26-е.

Представленные индексы, при некоторой доли их условности [13], свидетельствуют о поступательном развитии сферы информационно-комуникационных технологий России за последние годы, расширении их применения в бизнесе и управлении. Примечательно, что в условиях возрастающей международной конкуренции в Арктике позиции России в представленных рейтингах относительно циркумполярных государств вызывают серьезную обеспокоенность.

В связи с этим становится важной инициация международного сотрудничества по вопросам предотвращения конфликтов в информационной сфере, а также создания на правовом уровне действенных интернациональных механизмов разрешения подобного рода противоречий.

В этих целях в июне 2013 года президентами России и США на саммите G8 в Северной Ирландии было принято совместное заявление о новой области сотрудничества в направлении укрепления доверия. По результатам встреч была создана двусторонняя рабочая группа по вопросам угроз в сфере использования информационно-коммуникационных технологий в контексте международной безопасности.

Принципиальным сегодня становится поддержание информационной безопасности совместными усилиями стран Арктического региона. Россией уже реализуются интернациональные программы по обеспечению информационной безопасности государствами-членами Организации Договора о коллективной безопасности [10, 11]. Подобный опыт нашел бы позитивное применение среди циркумполярных государств и стал бы новым источником сотрудничества в названном регионе.

Кроме того, Россия, инициировав еще в 1998 году рассмотрение вопроса о проблеме международной информационной безопасности на Генеральной Ассамблее ООН, продолжает участвовать во всемирных саммитах по проблемам информационного общества и является участником международных соглашений. В 2011 году совместно с Китаем, Таджикистаном и Узбекистаном Россия направила письмо Генеральному секретарю ООН Пан Ги Муну с просьбой распространить проект «Правил поведения в области обеспечения международной информационной безопасности». Несмотря на критические высказывания по данным Правилам со стороны представителей США, Великобритании, Австралии и других стран, требуется дальнейшее обсуждение данного документа в международном сообществе и окончательное его принятие.

Таким образом, информационная безопасность в современных условиях становится фактором, влияющим на международные отношения. В одних случаях она рождает вопросы, решение которых способствует развитию межгосударственного сотрудничества; в других становится источником новых опасностей в условиях возрастающей конкуренции в мировом сообществе. Особенно актуальным становится обеспечение информационной безопасности в регионах, где сосредотачиваются национальные интересы развитых и развивающихся государств, участие которых в возможных конфликтах могут привести к глобальным потрясениям. Одним из таких регионов является Арктика, где позиции России по сравнению с другими циркумполярными странами свидетельствуют о возрастающей угрозе ее безопасности.

На наш взгляд, в ближайшие годы применение информационного оружия является гораздо более реальной перспективой в борьбе за Арктический регион, чем использование потенциала оружия массового поражения. В этих условиях насущным является формирование совершенной архитектуры международной информационной безопасности, как вариант, сначала в Арктическом регионе, а затем в мире. Активно решать данную задачу предстоит именно Российской Федерации, в противном случае под угрозой оказываются национальные интересы страны.

Список литературы

1. *Алиева М.Ф.* Информационная безопасность как элемент информационной культуры // Вестн. Адыг. гос. ун-та. Сер. 1: Регионоведение: философия, история, социология, юриспруденция, политология, культурология. 2012. № 4. С. 97–102.

2. *Благовещенский А.* В 2013 году России появятся свои кибервойска // Рос. газ. 2013. 5 июля. URL: http://www.rg.ru/2013/07/05/cyberwar-site-anons.html (дата обращения: 17.09.2013).

3. *Владимирова Т.В.* Информационная безопасность: к методологическим основаниям анализа вопроса // Информ. об-во. 2012. № 5. С. 47–52.

4. Доктрина информационной безопасности Российской Федерации: утв. Президентом РФ 9 сент. 2000 г. № Пр-1895 // Рос. газ. 2000. 28 сент. № 187.

5. *Егоров И.* ФСБ раскинет сеть // Рос. газ. 2013. 20 февр. № 6012.

6. *Журавлёв П.С.* Арктическая стратегия России: оценки, вопросы и проблемы реализации // Вестн. Сев. (Арктического) федер. ун-та. Сер.: Гуманит. и соц. науки. 2013. № 3. С. 154–160.

7. Основы государственной политики Российской Федерации в Арктике на период до 2020 года и дальнейшую перспективу: утв. Президентом РФ 18 сент. 2008 г. URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=119442 (дата обращения: 11.06.2013).

8. О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации: указ Президента Российской Федерации от 15 янв. 2013 г. № 31с // Собр. законодательства Рос. Федерации. 2013. № 3. Ст. 178.

9. О Стратегии национальной безопасности Российской Федерации до 2020 года: указ Президента РФ от 12 мая 2009 г. № 537 // Собр. законодательства Рос. Федерации. 2009. № 20. Ст. 2444.

10. Положение о сотрудничестве государств – членов ОДКБ в сфере обеспечения информационной безопасности (декабрь, 2010 г.). URL: http://www.businesspravo.ru/Docum/DocumShow_DocumID_181116.html (дата обращения: 11.09.2013).

11. Программа совместных действий по формированию системы информационной безопасности государств-членов Организации Договора о коллективной безопасности (сентябрь, 2008 г.). URL: http://zakon4.rada.gov.ua/laws/show/997_l67 (дата обращения: 11.09.2013).

12. *Цыгичко В.Н.* Информационное оружие как геополитический фактор и инструмент силовой политики. М., 1997. 31 с.

13. *Чугунов А.* Индекс ООН готовности стран к электронному правительству: соотнесение с правительственными данными // Информ. ресурсы России. 2009. № 1. С. 22–24.

14. Canada's Cyber Security Strategy: for a Stronger and More Prosperous Canada, 2010. URL: http://publications.gc.ca/collections/collection_2010/sp-ps/PS4-102-2010-eng.pdf (дата обращения: 15.08.2013).

15. Danish Defence Agreement 2010–2014. URL: http://www.fmn.dk/nyheder/Documents/ (дата обращения: 15.08.2013).

16. Finland´s Cyber Security Strategy, 2013. URL: http://www.yhteiskunnanturvallisuus.fi/ (дата обращения: 15.08.2013).

17. Global Security Map. URL: http://globalsecuritymap.com (дата обращения: 1.10.2013).

18. International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World, 2011. URL: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (дата обращения: 15.08.2013).

19. Life is For Sharing. URL: http://www.sicherheitstacho.eu (дата обращения: 1.10.2013).

20. *MacAskill E., Borger J., Hopkins N., Davies N., Ball J.* GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communications // The Guardian. 2013. 21 June.

21. Nasjonal strategi for informasjonssikkerhet, 2012. URL: http://www.regjeringen.no/pages/38169727/handplannasstratinfosikk2012.pdf (дата обращения: 15.08.2013).

22. National Strategy for Information Sharing and Safeguarding, 2012. URL: http://www.whitehouse.gov/sites/default/files/docs/2012sharingstrategy_1.pdf (дата обращения: 15.08.2013).

23. Norton Cybercrime Report 2012. URL: http://www.norton.com/2012cybercrimereport (дата обращения: 15.08.2013).

24. *Qiang X.* How China's Internet Police Control Speech on the Internet. URL: http://www.rfa.org/english/commentaries/china_internet-11242008134108.html (дата обращения: 10.09.2013).

25. Strategy for Information Security in Sweden 2010–2015. URL: https://www.msb.se/RibData/Filer/pdf/25940.PDF (дата обращения: 15.08.2013).

26. Strategy to Improve Internet Security in Sweden, 2006. URL: http://www.pts.se/upload/Documents/EN/Strategy_Internet_security_2006_12_July_2006.pdf (дата обращения: 15.08.2013).

27. The Cyber Index. International Security Trends and Realities. N. Y.; Geneva, 2013. 140 p.

28. The Economic Impact of Cybercrime and Cyber Espionage. Report. July 2013. URL: http://csis.org/files/publication/60396rpt_cybercrime-cost_0713_ph4.pdf (дата обращения: 15.08.2013).

29. The Global Information Technology Report 2013. URL: http://www3.weforum.org/docs/WEF_GITR_Report_2013.pdf (дата обращения: 10.04.2013).

30. The National Strategy to Secure Cyberspace, 2003. URL: http://www.fas.org/irp/threat/cyber/strategy.pdf (дата обращения: 15.08.2013).

31. U.S. Department of Defense, Cyber Command Fact Sheet, 21 May. URL: http://www.stratcom.mil/factsheets/Cyber_Command (дата обращения: 17.08.2013).

32. United Nations E-Government Survey 2012: E-Government for the People. N.Y., 2012.

33. Valtioneuvoston periaatepäätös kansalliseksi tietoturvastrategiaksi (Government Resolution on National Information Security Strategy), 2008. URL: http://www.lvm.fi/c/document_library (дата обращения: 15.08.2013).

References

1. Alieva M.F. Informatsionnaya bezopasnost' kak element informatsionnoy kul'tury [Information Security as an Element of Information Culture]. *Vestnik adygeyskogo gosudarstvennogo universiteta. Ser. 1. Regionovedenie: filosofiya, istoriya, sotsiologiya, yurisprudentsiya, politologiya, kul'turologiya*, 2012, no. 4, pp. 97–102.

2. Blagoveshchenskiy A. V 2013 godu Rossii poyavyatsya svoi kibervoyska [In 2013 Russia Will Have Her Own Cyberarmy]. *Rossiyskaya gazeta*, 5 July 2013. Available at: http://www.rg.ru/2013/07/05/cyberwar-site-anons.html (accessed 17 September 2013).

3. Vladimirova T.V. Informatsionnaya bezopasnost': k metodologicheskim osnovaniyam analiza voprosa [Information Security: On the Methodological Elements of Analysing the Issue]. *Informatsionnoe obshchestvo*, 2012, no. 5, pp. 47–52.

4. The Information Security Doctrine of the Russian Federation: approved by President of the Russian Federation Vladimir Putin on 9 September 2000 no. Pr-1895. *Rossiyskaya gazeta*, 28 September 2000 no. 187 (in Russian).

5. Egorov I. FSB raskinet set' [FSB Will Spread Its Net]. *Rossiyskaya gazeta*, 20 February 2013 no. 6012.

6. Zhuravlev P.S. Arkticheskaya strategiya Rossii: otsenki, voprosy i problemy realizatsii [Russia's Arctic Strategy: Estimates, Issues and Problems of Implementation]. *Vestnik Severnogo (Arkticheskogo) federalnogo universiteta. Ser.:* "*Gumanitarnye i sotsial'nye nauki*", 2013, no. 3, pp. 154–160.

7. *Fundamentals of the State Policy of the Russian Federation in the Arctic up to 2020 and Beyond: approved by President of the Russian Federation on 18 September 2008.* Available at: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=119442 (accessed 11 June 2013) (in Russian).

8. On the Development of a Statewide System for the Detection, Prevention and Response to Cyberattacks Against Information Resources of the Russian Federation: Decree of the President of the Russian Federation of 15 January 2013. No. 31s. *Sobranie zakonodatel'stva Rossiyskoy Federatsii*, 2013, no. 3, Art. 178 (in Russian).

9. National Security Strategy of the Russian Federation to 2020: Decree of the President of the Russian Federation of 12 May 2009. no. 537. *Sobranie zakonodatel'stva Rossiyskoy Federatsii*, 2009, no. 20, Art. 2444 (in Russian).

10. *Regulations on Cooperation of the the CSTO Member States in the Field of Information Security* (December 2010). Available at: http://www.busines-spravo.ru/Docum/DocumShow_DocumID_181116.html (accessed 11 September 2013) (in Russian).

11. *The Program of Joint Actions to Create a System of Information Security of the CSTO Member States* (September 2008). Available at: http://zakon4.rada.gov.ua/laws/show/997_l67 (accessed 11 September 2013) (in Russian).

12. Tsygichko V.N., Smolyan G.L., Chereshkin D.S. *Informatsionnoe oruzhie kak geopoliticheskiy faktor i instrument silovoy politiki* [Information Weapons as a Geopolitical Factor and a Tool of Power Politics]. Moscow, 1997. 31 p.

13. Chugunov A. *Indeks OON gotovnosti stran k elektronnomu pravitel'stvu: sootnesenie s pravitel'stvennymi dannymi* [United Nations Index of Readiness to the Electronic Government: Correlation with the Russian Data]. *Informatsionnye resursy Rossii*, 2009, no. 1, pp. 22–24.

14. *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada, 2010*. Available at: http://publications.gc.ca/collections/collection_2010/sp-ps/PS4-102-2010-eng.pdf (accessed 15 August 2013).

15. *Danish Defence Agreement 2010–2014*. Available at: http://www.fmn.dk/nyheder/Documents/ (accessed 15 August 2013).

16. *Finland's Cyber Security Strategy, 2013*. Available at: http://www.yhteiskunnanturvallisuus.fi/ (accessed 15 August 2013).

17. Global Security Map. Available at: http://globalsecuritymap.com (accessed 1 October 2013).
18. *International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World, 2011*. Available at: http://www.whitehouse.gov/sites/default/files/rss_vie-wer/international_strategy_for_cyberspace.pdf (accessed 15 August 2013).
19. Life Is for Sharing. Available at: http://www.sicherheitstacho.eu (accessed 1 October 2013).
20. MacAskill E., Borger J., Hopkins N., Davies N., Ball J. GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communications. *The Guardian*, 21 June 2013.
21. *Nasjonal strategi for informasjonssikkerhet, 2012*. Available at: http://www.regjerin-gen.no/pages/38169727/handplannasstratinfosikk2012.pdf (accessed 15 August 2013).
22. *National Strategy for Information Sharing and Safeguarding, 2012*. Available at: http://www.whitehouse.gov/sites/default/files/docs/2012sharingstrategy_1.pdf (accessed 15 August 2013).
23. *Norton Cybercrime Report 2012*. Available at: http://www.norton.com/2012cybercrimereport (accessed 15 August 2013).
24. Qiang X. *How China's Internet Police Control Speech on the Internet*. Available at: http://www.rfa.org/english/commentaries/china_internet-11242008134108.html (accessed 10 September 2013).
25. *Strategy for Information Security in Sweden 2010–2015*. Available at: https://www.msb.se/RibData/Filer/pdf/25940.PDF (accessed 15 August 2013).
26. *Strategy to Improve Internet Security in Sweden, 2006*. Available at: http://www.pts.se/upload/Documents/EN/Strategy_Internet_security_2006_12_July_2006.pdf (accessed 15 August 2013).
27. *The Cyber Index. International Security Trends and Realities*. New York, Geneva, 2013. 140 p.
28. *The Economic Impact of Cybercrime and Cyber Espionage. Report. July 2013*. Available at: http://csis.org/files/publication/60396rpt_cybercrime-cost_0713_ph4.pdf (accessed 15 August 2013).
29. *The Global Information Technology Report 2013*. Available at: http://www3.wefo-rum.org/docs/WEF_GITR_Report_2013.pdf (accessed 10 April 2013).
30. *The National Strategy to Secure Cyberspace, 2003*. Available at: http://www.fas.org/irp/threat/cyber/strategy.pdf (accessed 15 August 2013).
31. *U.S. Department of Defense, Cyber Command Fact Sheet, 21 May*. Available at: http://www.stratcom.mil/factsheets/Cyber_Command (accessed 17 August 2013).
32. *United Nations E-Government Survey 2012: E-Government for the People*. New York, 2012.
33. *Valtioneuvoston periaatepäätös kansalliseksi tietoturvastrategiaksi (Government Resolution on National Information Security Strategy), 2008*. Available at: http://www.lvm.fi/c/document_library (accessed 15 August 2013).

Tamitsky Aleksandr Mikhailovich
Institute of Social, Humanitarian and Political Sciences,
Northern (Arctic) Federal University named after M.V. Lomonosov (Arkhangelsk, Russia)

INFORMATION SECURITY AS A FACTOR OF INTERNATIONAL RELATIONS IN THE ARCTIC REGION

The article dwells on the threats and risks in today's information space and underlines the need for a system of information security both on the national and international levels. The paper analyzes the state of information security in circumpolar countries, including Russia, in the conditions of increasing international cooperation and competition in the Arctic region.

Keywords: *Arctic region, information space, information security.*

Контактная информация:
адрес: 163002, г. Архангельск, просп. Ломоносова, д. 24;
e-mail: a.tamitskiy@gmail.com

Рецензенты – *Голдин В.И.,* доктор исторических наук, профессор кафедры регионоведения и международных отношений института социально-гуманитарных и политических наук Северного (Арктического) федерального университета имени М.В. Ломоносова; *Иванкин И.И.,* кандидат технических наук, директор института нефти и газа Северного (Арктического) федерального университета