DOI: 10.24411/2221-3279-2019-10004

ДЕЯТЕЛЬНОСТЬ ООН В ОБЛАСТИ ИНФОРМАЦИИ И МЕЖДУНАРОДНЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИИ

Радомир Викторович Болгов

Санкт-Петербургский государственный университет, Санкт-Петербург, Россия

Информация о статье:

Поступила в редакцию:

11 декабря 2017

Принята к печати:

24 августа 2018

Об авторе:
к.полит.н., доцент, кафедра мировой политики, Санкт-Петербургский государственный университет

e-mail: rbolgov@yandex.ru

Ключевые слова:
международная информационная безопасность; кибербезопасность; Интернет; ООН; внешняя политика России; международные организации

Аннотация: В статье проанализирована политика России в ООН по вопросам информационной безопасности. Рассмотрены основные доктрины и документы, регулирующие политику информационной безопасности в России, а также международно-правовые инициативы России. Кроме того, показана деятельность ООН в данной сфере в качестве контекста для российских инициатив по международной информационной безопасности. Подчеркивается необходимость совместных действий России и ООН по борьбе с угрозами информационной безопасности

Статья подготовлена при финансовой поддержке Российского научного фонда, проект № 16-18-10315, реализуемый в Санкт-Петербургском государственном университете

Введение

Тематика кибербезопасности для России становится всё более актуальной. Так, по данным ФСБ, в России в 2016 году зафиксировано более 52 млн кибератак на сайты государственных органов, что втрое больше, чем в 2015 году1. Влияние русских хакеров на выборы в США стало темой для политических спекуляций. В соответствии с рядом индексов и рейтингов кибербезопасности (например, *ITU Global Cybersecurity Index*, рейтинг Р. Кларка и Р. Нейка) Россия входит в число лидеров по киберпотенциалу[2].

Для международных организаций эта тематика также актуальна. У ряда международных организаций появляются собственные цифровые стратегии (ЕС, НАТО, Франкофония, ЕАЭС и др.), и здесь ООН не является исключением. Государства рассматривают международные организации в качестве подходящих платформ для обеспечения национальных интересов в киберпространстве.

Интерес и востребованность выбранного исследовательского направления во

[1] В России в 2016 году зафиксировано более 52 млн кибератак на сайты госорганов // Ведомости, 3 марта 2017. Режим доступа: https://www.vedomosti.ru/politics/news/2017/03/03/679830-zafiksirovano-bolee-52-mln-kiberatak [V Rossii v 2016 godu zafiksirovano bolee 52 mln kiberatak na sajty gosorganov [In Russia in 2016, more than 52 Million Cyber Attacks on Government Websites] // *Vedomosti,* 3rd March 2017. Mode of access: https://www.vedomosti.ru/politics/news/2017/03/03/679830-zafiksirovano-bolee-52-mln-kiberatak]

[2] ITU Global Cybersecurity Index 2017. Mode of access: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf; Clarke, R.; Knake, R. Cyberwar. The Next Threat to National Security and What to Do about It. HarperCollins Publishers New York, 2010.

России не вызывает сомнений. В библиометрической базе РИНЦ было найдено более 500 статей по тематике «международная информационная безопасность», при этом публикационная активность продолжает расти. Для уточнения тематической направленности статей автором был проведен анализ динамики публикационной активности с разбивкой на 2 временных отрезка: 2000-2008 гг. и 2009-2016 гг. (по базе РИНЦ). В среднем число опубликованных статей во втором периоде более чем в 3 раза превышает количество публикаций до 2008 г., что свидетельствует о возрастании интереса российского научного сообщества к данной проблематике.

Значительная часть этих работ изучает правовые аспекты международной информационной безопасности[3]. Так, Р. Хурвитц рассматривает усилия государств по созданию правовых норм в сфере кибербезопасности через структуры ООН и международные коалиции. Кроме того, ряд авторов выступают с позиций практиков-международников, занимающихся данными вопросами в рамках международных организаций[4].

В рамках данной тематики стоит выделить несколько направлений:

– теоретические аспекты международной информационной безопасности[5];– деятельность международных организаций, в т.ч. ООН, в деле обеспечения информационной безопасности[6]

---

[3] Hurwitz, R. The Play of States: Norms and Security in Cyberspace // *American Foreign Policy Interests,* 2014, Vol. 36, Issue 5, pp. 322-331; Maurer, T. Cyber Norm Emergence at the United Nations: An Analysis of the Activities of the UN Regarding Cybersecurity. Cambridge, MA: Harvard Kennedy School's Belfer Center for Science and International Affairs, 2011. P. 22.

[4] Бойко С.М. Группа правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности: взгляд из прошлого в будущее // Международная жизнь. – 2016. – № 8. – С. 53-71. [Boiko, S.M. Gruppa pravitel'stvennyh ehkspertov OON po dostizheniyam v sfere informatizacii i telekommunikacij v kontekste mezhdunarodnoj bezopasnosti: vzglyad iz proshlogo v budushchee (UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: a View from the Past to the Future) // *Mezhdunarodnaya zhizn'*, 2016, No. 8, pp. 53-71.]; Kane, A. The Rocky Road to Consensus: The Work of UN Groups of Governmental Experts in the Field of ICTs and in the Context of International Security, 1998–2013 // *American Foreign Policy Interests,* 2014, Vol. 36, Issue 5, pp. 314-321. DOI: 10.1080/10803920.2014.969175

[5] Международная информационная безопасность: дипломатия мира. Сборник материалов / Под общ. ред. Комова С.А. – М., 2009. – 272 с. [Mezhdunarodnaya informacionnaya bezopasnost': diplomatiya mira (International Information Security: Diplomacy around the World). Collection of materials, Ed. Komov S.A. Moscow, 2009, 272 p.]; Болгов Р.В. Информационные технологии в современных вооруженных конфликтах и военных стратегиях (политические аспекты). Диссертация на соискание ученой степени кандидата политических наук / Санкт-Петербургский государственный университет. – СПб, 2011. [Bolgov, R.V. Informacionnye tekhnologii v sovremennyh vooruzhennyh konfliktah i voennyh strategiyah (politicheskie aspekty) (Information Technology in Contemporary Armed Conflicts and Military Strategies (Political Aspects)). Thesis for a PhD degree in Political Science / Saint Petersburg State University. St. Petersburg, 2011.]

[6] Кванталиани И.Э. Роль международных организаций в деле обеспечения безопасности информационного пространства // Актуальные проблемы современного международного права. Материалы X ежегодной Всероссийской научно-практической конференции. 2012. – С. 26-30. [Kvantaliani, I.E. Rol' mezhdunarodnyh organizacij v dele obespecheniya bezopasnosti informacionnogo prostranstva [The Role of International Organizations in the Security of Information Space]. Aktual'nye problemy sovremennogo mezhdunarodnogo prava. Materialy X ezhegodnoj Vserossijskoj nauchno-prakticheskoj konferencii (Actual Problems of Modern International Law. Materials of the 10th All-Russian Annual Scientific Conference), 2012. Pp. 26-30.]; Ромашкина Н.П. ООН и международная информационная безопасность // Безопасность и контроль над вооружениями 2015-2016. Международное взаимодействие в борьбе с глобальными угрозами. – Москва, 2016. – С. 273-286. [Romashkina, N.P. OON i mezhdunarodnaya informacionnaya bezopasnost' (The UN and the International Information Security). Bezopasnost' i kontrol' nad vooruzheniyami 2015-2016. Mezhdunarodnoe vzaimodejstvie v bor'be s global'nymi ugrozami (Security and Arms Control 2015-2016. International Cooperation in the Fight

– позиция России по данной проблематике[7];

– деятельность России в деле обеспечения информационной безопасности в рамках международных организаций, в т.ч. ООН[8].

Теоретические основания исследования

Информационную безопасность можно определить как состояние общества, при котором обеспечена надёжная и всесторонняя защита личности, общества и государства в информационном пространстве от воздействия на них особого вида угроз, выступающих в форме организованных или стихийно возникающих информационных и коммуникационных потоков. Составляющими информационной безопасности являются:

1) состояние безопасности информационного пространства, при котором обеспечивается его формирование и развитие в интересах граждан, организаций и государства;

2) состояние безопасности информационной инфраструктуры, при котором информация используется строго по назначению и не оказывает негативного воздействия на систему (объект) при ее использовании;

3) состояние безопасности самой информации, при котором исключается или существенно затрудняется нарушение таких ее свойств, как конфиденциальность, целостность, доступность.

Международная информационная безопасность определяется ООН как «состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве»[9].

Against Global Threats). Moscow, 2016, pp. 273-286.]; Томилова Ю.Н. ООН и проблема обеспечения международной информационной безопасности // Международная жизнь. – 2015. – № 8. – С. 73-85. [Tomilova, Y.N. OON i problema obespecheniya mezhdunarodnoj informacionnoj bezopasnosti (The UN and the Problem of Ensuring International Information Security) // *Mezhdunarodnaya zhizn',* 2015, No. 8, pp. 73-85.]

[7] Демидов О.В. Обеспечение международной информационной безопасности и российские национальные интересы // Индекс безопасности. – 2013. – № 1 (104). – С. 129-168. [Demidov, O.V. Obespechenie mezhdunarodnoj informacionnoj bezopasnosti i rossijskie nacional'nye interesy (Ensuring International Information Security and National Interests of Russia) // *Indeks bezopasnosti,* 2013, No. 1(104), pp. 129-168.]; Зиновьева Е.С. Анализ внешнеполитических инициатив РФ в области международной информационной безопасности // Вестник МГИМО-Университета. – 2014. – № 6 (39). – С. 47-52. [Zinovieva, E.S. Analiz vneshnepoliticheskih iniciativ RF v oblasti mezhdunarodnoj informacionnoj bezopasnosti (Analysis of Russian Foreign Policy Initiatives in the Field of International Information Security) // *Vestnik MGIMO-Universiteta,* 2014, No. 6(39), pp. 47-52.]; Ширин С.С. Российские инициативы по вопросам управления Интернетом // Вестник МГИМО Университета. – 2014. – № 6 (39). – С. 73-81. [Shirin S.S. Rossijskie iniciativy po voprosam upravleniya Internetom (Russian Initiatives on Internet Governance) // *Vestnik MGIMO Universiteta*, 2014, No. 6(39), pp. 73-81.]

[8] Лобанова Е.Н. Некоторые инициативы РФ в ООН по решению проблемы международной информационной безопасности // Глобализация и проблема войн в современном мире. Сборник статей. Под общ. ред. В.В. Барабаша. – М., 2011. – С. 29-35. [Lobanova, E.N. Nekotorye iniciativy RF v OON po resheniyu problemy mezhdunarodnoj informacionnoj bezopasnosti (Some Russian Initiatives in the United Nations to Address the Issue of International Information Security). Globalizaciya i problema vojn v sovremennom mire. Sbornik statej (Globalization and the Problem of War in the Modern World. Digest of Articles). Ed. Barabash V.V. Moscow, 2011. C. 29-35.]; Бойко С.М. Группа правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности: взгляд из прошлого в будущее // Международная жизнь. – 2016. – № 8. – С. 53-71. [Boiko, S.M. Gruppa pravitel'stvennyh ehkspertov OON po dostizheniyam v sfere informatizacii i telekommunikacij v kontekste mezhdunarodnoj bezopasnosti: vzglyad iz proshlogo v budushchee (UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: a View from the Past to the Future) // *Mezhdunarodnaya zhizn*', 2016, No. 8, pp. 53-71.]

[9] Док. Генеральной Ассамблеи ООН A/55/40, 10 июля 2000; A/55/140/Add. 1, 3 октября 2000 // Информационные вызовы национальной и международной безопасности. – М., 2001. – С. 315. [Doc. UN General Assembly A/55/40, 10 July 2000; A/55/40 / Add. 1, October 3. Informacionnye vyzovy nacional'noj i mezhdunarodnoj bezopasnosti (Information

В соответствии с Доктриной информационной безопасности РФ (2000) информационная безопасность – это безопасность национальных интересов в информационной сфере. Национальные интересы в информационной сфере определяются совокупностью сбалансированных интересов личности (реализация конституционных прав человека и гражданина на доступ к информации), общества (упрочение демократии, создание правового социального государства, достижение и поддержание общественного согласия), и государства (создание условий для развития информационной инфраструктуры, для реализации конституционных прав и свобод человека, обеспечение незыблемости конституционного строя, суверенитета и территориальной целостности, политической, экономической и социальной стабильности, в обеспечении законности и правопорядка, в развитии равноправного и взаимовыгодного международного сотрудничества)[10].

Однако существуют различия в подходах к определению понятия «информационная безопасность». В российском законодательстве понятие «информационная безопасность» сводится к «состоянию защищённости информационной среды общества, обеспечивающему её формирование, использование и развитие в интересах граждан, организаций, государства»[11]. В зарубежных правовых актах (в частности, американских) информационная безопасность определяется не просто как состояние защищённости информационной среды, а как «способность сети или системы противостоять с нужным уровнем надёжности авариям или злонамеренным действиям, которые могут нарушить доступность, целостность и конфиденциальность хранимой и передаваемой информации»[12].

Научные исследования и открытые дискуссии по этим вопросам привели к тому, что значительная часть работ за последние годы разделена на два основных полюса. Представители первого полюса (технологического), такие, как Р. Хандли и Р. Андерсон, в своих работах обсуждают проблемы информационной безопасности и защиты информации в компьютерах и сетях; принципы, лежащие в основе угроз информационной инфраструктуры США[13]. Другой полюс (в частности, Дж. Най, У. Оуэнс) составляют работы, связанные с политическим и идеологическим контекстом происходящих процессов информатизации – информационная стратегия рассматривается как способ выражения «мягкой силы» американских идеалов с целью распространения своего влияния на руководство и население зарубежных стран[14].

Можно выделить два подхода к информационной безопасности в международных отношениях, условно называемые «реалистическим» и «либеральным».

«Реалистический» подход делает акцент на:

1. Увеличение уровня безопасности информационных систем внутри страны,

2. Создание большого количества внутренних сетей, независимых друг от друга и от глобальных сетей,

3. Постоянный мониторинг уровня информационной безопасности потенциальных противников, целенаправленный поиск уязвимостей в их программном обеспечении,

Challenges to National and International Security). Moscow, 2001. P. 315.]

[10] Доктрина информационной безопасности РФ (2000) // Развитие информационного общества в России. Том 2. Концепции и программы: Сб. документов и материалов / СПб., 2001. – 228с. [Doktrina informacionnoj bezopasnosti RF (Doctrine of Information Security of the Russian Federation), 2000 // Razvitie informacionnogo obshchestva v Rossii. Tom 2. Koncepcii i programmy: Sb. dokumentov i materialov (Development of an Information Society in Russia. Vol 2. Concepts and Applications: Coll. documents and materials). St. petersburg, 2001. 228 p.]

[11] Федеральный Закон РФ от 05.03.1992 № 2446-1 «О безопасности». [Federal'nyj Zakon RF "O bezopasnosti" (Federal Law "On Security") (1992), № 2446-1.]

[12] US Federal Information Security Management Act of 2002. Mode of access: http://www.findarticles.com/p/articles/mi_m0OBA/is_1_22/ai_n6134858

[13] Hundley, R.; Anderson, R. Security in Cyberspace: An Emerging Challenge for Society, 1994.

[14] Nye, J.; Owens, W. America's Information Age: The Nature of Power // *Foreign Affairs,* March-April 1996.

4. Контроль над распространением информации и соответствующих технологий,

5. Разработка средств ведения «информационной войны»,

6. Уменьшение взаимозависимости и открытости государств в информационной сфере.

«Реалистический» подход, по сути, отражает современную политику обеспечения информационной безопасности, проводимую в Китае, США и, в какой-то мере, в России. Принятые в США концепции «информационного превосходства» и «информационного сдерживания» выступают наглядной иллюстрацией применения подобного подхода.

«Либеральный» поход более идеалистичный, и его можно свести к следующему:

1. Увеличение взаимозависимости государств в информационной сфере,

2. Обеспечение общей безопасности через создание сети международных структур и договоров,

3. Либерализация информационных отношений и информационного рынка[15].

Данная концепция предполагает, что отношения между государствами должны строиться в первую очередь на основе взаимного доверия и неуклонного следования заключенным договорам. Априорно предполагается снижение ограничений на распространение информации. К либеральному подходу можно отнести и принятие международных соглашений по проблемам информационной безопасности, в том числе Окинавскую хартию.

Исследование: основная часть

В настоящее время на территории России действует более 40 федеральных законов в области информации, более 80 актов президента, около 200 актов правительства Российской Федерации. Однако у России пока что отсутствует отдельная киберстратегия в виде официального документа. Одним из ключевых документов в данной сфере является Доктрина информационной безопасности, первая версия которой была принята в 2000 г., а новая версия – в декабре 2016.

Принятию данной доктрины предшествовал ряд событий на протяжении 1990-х гг. До 2000-х гг. в России практически не существовало ясной государственной позиции по проблеме информационной безопасности. В отличие от подхода, обозначенного США, в российской Доктрине на первое место ставится обеспечение информационной безопасности индивидуального, группового и общественного сознания. В начале 1990-х гг. в России сложилась довольно сложная ситуация с обеспечением информационной безопасности. С одной стороны, либерально настроенные СМИ постоянно критиковали информационную безопасность как таковую, приводя аналогии оруэлловского «Большого Брата». Другая крайность – некоторые политики и эксперты стали придерживаться обскурантистских позиций, полагая, что для обеспечения национальных интересов России в информационном пространстве необходим отказ от открытого общества и от участия в глобализации.

Можно выделить два этапа, предшествовавшие принятию Доктрины информационной безопасности:

1) 1991-1996 гг. – формирование предпосылок и законодательной базы. В этот период был принят Федеральный закон «Об информации, информатизации и защите информации» от 20.02.1995 и ряд других документов. Так же происходит накопление положительного опыта взаимодействия с участием России на международной арене, связанного с обретением новой идентичности участника международных отношений и носителя интересов в информационном пространстве. Для данного этапа характерна разноголосица в оценках роли и места России в информационном пространстве, заметная в высказываниях разных политических партий, ведомств и групп интересов. Доминировало утопическое представление

[15] Болгов Р.В., Васильева Н.А., Виноградова С.М., Панцерев К.А. Информационное общество и международные отношения / Отв. Ред. Панцерев К.А. – СПб, 2014. – 384 с. [Bolgov, R.V.; Vasilyeva, N.A.; Vinogradova, S.M.; Pantserev, K.A. Informacionnoe obshchestvo i mezhdunarodnye otnosheniya (Information Society and International Relations) / Ed. Pantserev K.A. St. Petersburg, 2014. 384 p.];

о перспективе врастания России в мировое информационное пространство. Также здесь характерна политика уступок со стороны России, в т.ч. в сфере национальных интересов в информационной сфере. Была поставлена под сомнение необходимость защиты информационных ресурсов России и с технологической точки зрения, и как формы национальной идентичности (традиции, обычаи, менталитет). Происходило неадаптированное копирование западного опыта в сфере информационной политики. Пиковым событием стали президентские выборы 1996 г., запомнившиеся войной компроматов в информационном пространстве и после которых всё чаще стали говорит об угрозах конституционному строю и угрозах в духовной сфере (что впоследствии вошло в текст Доктрины). В конце данного периода был заменен ряд ключевых фигур, отвечавших за вопросы информационной безопасности. В этот же период началась военная операция в Чечне, в ходе которой российские войска терпели поражения в информационном противоборстве.

2) 1996-2000 гг. – формирование структур обеспечения информационной безопасности. В этот период была сформирована межведомственная комиссия по обеспечению информационной безопасности (в составе Совета безопасности с участием МВД, ФСБ и др.). Благодаря деятельности этих структур к 1997 году был подготовлен проект Доктрины информационной безопасности, однако властный вакуум и обострение противоречий внутри правящих элит не позволили принять данный документ. Финансово-экономический кризис 1998 г. также отсрочил принятие Доктрины.

Наконец в 2000 году Доктрина была утверждена. Данный документ представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации. Она служит основой для формирования государственной политики в области обеспечения информационной безопасности Российской Федерации, подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации, а также разработки целевых программ обеспечения информационной безопасности Российской Федерации.

Под информационной безопасностью понимается состояние защищенности национальных интересов государства в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

В доктрине прописаны угрозы, источники угроз интересы, методы обеспечения и мероприятия, а также международное сотрудничество в сфере информационной безопасности.

Но с 2000 года многое изменилось. Появились технологии *Web 2.0* и связанные с ними социальные медиа, влияние которых на национальную безопасность нельзя недооценивать, что продемонстрировали протесты в арабских странах в 2011 г. (их некоторые СМИ поспешили назвать «твиттерными революциями»). Санкции в отношении России показали необходимость «импортозамещения» в сфере ИТ. Всё чаще говорят об опасности кибератак для жизнеобеспечивающей инфраструктуры. Появились новые документы, связанные с вопросами развития информационных технологий в России. Доктрина 2016 г. стала попыткой более адекватного отражения тех изменений, которые произошли за 16 лет[16].

Намерение России выработать правила поведения в сфере международной информационной безопасности именно под эгидой ООН нашло отражение в Концепции внешней политики РФ (2013)[17]. Кроме того, в докумен-

[16] Доктрина информационной безопасности РФ (утв. Президентом РФ 05.12.2016 № 646) // Российская газета, 06.12.2016. [Doktrina informacionnoj bezopasnosti RF (Doctrine of Information Security of the Russian Federation) (approved by The President of the Russian Federation 05/12/2016 number 646) // *Rossijskaya gazeta,* 12/06/2016.]

[17] Концепция внешней политики Российской Федерации, 2013. Режим доступа: http://mid.ru/bdomp/ns-osndoc.nsf/e2f289bea62097f9c325787a0034c255/c32577ca0017434944257b160051bf7f!OpenDocument[The Concept of Russia's Foreign Policy, 2013. Mode of access:

те «Основы государственной политики РФ в области международной информационной безопасности на период до 2020 г.» в качестве одного из направлений противодействия угрозам в информационной сфере указано «содействие подготовке и принятию в рамках ООН международных правовых актов, регламентирующих применение принципов и норм международного гуманитарного права в сфере использования ИКТ»[18].

Результаты исследования

Поскольку Россия последовательно делает акцент на нормативно-правовом регулировании вопросов кибербезопасности на внутринациональном уровне (особенно в последние годы, если посмотреть на количество принятых документов), этого же подхода она придерживается и на международном уровне: вопросы кибербезопасности нужно регулировать, причем как можно скорее и как можно более детально. Этого подхода Россия придерживалась на протяжении 15 лет, предлагая свои проекты в рамках ООН (в частности, предложение о создании специального международного суда по преступлениям в информационной сфере). Россию поддерживали Китай, Индия и Бразилия. Однако это наталкивалось на противоположную позицию США, ЕС и Японии, считающих, что вопросы кибербезопасности не нужно излишне «перерегулировать» в ущерб свободам граждан и бизнеса. Некоторое сближение позиций по данным вопросам наметилось на конференции по безопасности в Мюнхене в феврале 2011 г., где большинство политиков и экспертов высказалось за необходимость международно-правового регулирования киберпространства. Несмотря на то, что был подготовлен совместный российско-американский доклад, конкретных решений обязательного характера принято не было.

Сейчас применение информационного оружия регулируется следующими договорами: Международное Телекоммуникационное Соглашение Малага-Торремолинос (1973) и Международное Соглашение о Морских Спутниках (ИНМАРСАТ) (1976), принятые под эгидой специализированных учреждений ООН – соответственно, Международного союза электросвязи и Международной морской организацией. Международное Телекоммуникационное Соглашение[19] в статье 35 определяет, что «все станции, вне зависимости от их цели, должны быть установлены и управляемы так, чтобы не причинить вред радиослужбам или коммуникациям других членов». Таким образом, соглашение запрещает использование спутниковой станции для разрушения или столкновения с коммуникациями других государств. Но те же самые государства в статье 38 согласились, что они «сохраняют полную свободу относительно военных радиостанций их армии, военно-морских и воздушных сил». Таким образом, соглашение признает, что возможно использование в военных целях спутниковой системы. Однако большая часть потоков информации военного характера развитых стран проходят через гражданские системы коммуникаций. Таким образом, в этом документе имеется противоречие между 35 и 38 статьями.

В то же время, в рамках обсуждения обозначились по крайней мере два различных подхода к проблеме. Ряд развитых стран во главе с США исходил из приоритета разработки мер информационной безопасности применительно к угрозам террористического и криминального характера. При этом угроза создания информационного оружия и

http://mid.ru/bdomp/ns-osndoc.nsf/e2f289bea62097f9c325787a0034c255/c32577ca0017434944257b160051bf7f]

[18] Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (утв. Президентом РФ 24.07.2013 № Пр-1753). [Osnovy gosudarstvennoj politiki Rossijskoj Federacii v oblasti mezhdunarodnoj informacionnoj bezopasnosti na period do 2020 goda (Fundamentals of the Russian Federation's State Policy in the Field of International Information Security for the Period up to 2020). Approved by the President of the Russian Federation, 24/7/2013, Pr-1753.]

[19] International Telecommunication Convention (Malaga-Torremolinos, 25 October 1973). Mode of access: http://www.itu.int/en/history/HistoryDigitalCollectionDocLibrary/constitutionsConventions/5.10.61.en.100.pdf

возникновения информационных войн сторонниками такого подхода рассматривалась скорее как теоретическая. Соответственно, сходил на нет и разоруженческий аспект проблемы международной информационной безопасности. Дальнейшее обсуждение этой проблематики предлагалось рассредоточить по региональным и тематическим форумам (Европейский Союз, Группа Семи и т. д.), а в рамках ООН перевести обсуждение из военно-политического в правовой и экономический комитеты. США считают, что вопрос международно-правового регулирования военно-политических аспектов информационной безопасности пока не приобрёл достаточной актуальности и видят необходимым сначала накопить достаточный практический опыт регулирования подобных проблем[20].

С другой стороны, представители России, Китая, развивающихся стран поддерживали концепцию рассмотрения проблемы международной информационной безопасности в комплексе, с выделением в качестве приоритетной задачи ограничение потенциальной угрозы развязывания информационной войны. При этом подчеркивалась необходимость немедленно приступить к обсуждению и практической разработке международно-правовой основы режима международной информационной безопасности. Выдвигалось, в частности, предложение о создании специального международного суда по преступлениям в информационной сфере. Эти подходы проявились при принятии Окинавской Хартии глобального информационного общества (2000). В ходе 53-й сессии Генеральной Ассамблеи ООН Россией был выдвинут проект резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», консенсусом принятый в 1998 г.[21] Еще один успех, но более поздний – Резолюция Генеральной Ассамблеи ООН A/RES/64/211 «Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур»[22].

Некоторое сближение позиций по данным вопросам наметилось на конференции по безопасности в Мюнхене в феврале 2011 г., где большинство политиков и экспертов высказалось за необходимость международно-правового регулирования киберпространства. Хотя конкретных решений обязательного характера принято не было, был подготовлен совместный российско-американский доклад «К выработке правил поведения в киберконфликтах: применимость Женевских и Гаагских конвенций в современном информационном пространстве». В докладе выделены следующие проблемные вопросы, по которым до сих нет единой позиции у США и России, но по которым стороны обязуются договариваться: можно ли законодательно и технически «выделить» защищенные объекты инфраструктуры из «облака» незащищенных объектов в киберпространстве, наподобие того, как гражданские объекты пользуются защитой международных соглашений во время вой-

[20] Информационные вызовы национальной и международной безопасности / И.Ю. Алексеева и др.; Под общ. ред. А.В. Федорова, В.Н. Цыгичко. – М.: ПИР-Центр, 2001. [Informacionnye vyzovy nacional'noj i mezhdunarodnoj bezopasnosti (Information Challenges to National and International Security). Alekseev I.Y. etc.; Ed. Fedorov, A.V., Tsygichko, V.N. Moscow, PIR-Center, 2001.]

[21] Резолюция Генеральной Ассамблеи ООН A/RES/53/70, 4 декабря 1998 г. «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». Режим доступа: http://www.un.org/ru/documents/ods.asp?m=A/RES/53/70 [UN General Assembly Resolution A/RES/53/70, December 4, 1998 «Developments in the field of information and telecommunications in the context of international security». Mode of access: http://www.un.org/ru/documents/ods.asp?m=A/RES/53/70]

[22] Резолюция Генеральной Ассамблеи ООН A/RES/64/211 «Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур», 2010. Режим доступа: http://www.un.org/ru/documents/ods.asp?m=A/RES/64/211 [UN General Assembly Resolution A/RES/64/211 «Creating a global culture of cybersecurity and the assessment of national efforts to protect critical information infrastructures,» 2010. Mode of access: http://www.un.org/ru/documents/ods.asp?m=A/RES/64/211]

ны. Также стороны должны решить, является ли кибероружие (вирусы, «черви» и т.д.) аналогичными вооружениям, запрещенным Женевским протоколом (например, ядовитые газы). На конференции также были достигнуты договоренности разработать международную конвенцию о кибервойне и создать международный трибунал по преступлениям в киберпространстве. В рамках этих структур стороны должны будут решать вышеназванные вопросы[23].

Неудачи России в проведении своих инициатив по кибербезопасности через ООН (с 1998 г.) подстегнули актуализацию Россией этих вопросов в повестке дня Шанхайской организации сотрудничества (ШОС). Китай и Казахстан с 2011 г. также рассматривают данную организацию как инструмент для контроля киберпространства. Во время председательства России в 2014 г. в Шанхайской организации сотрудничества кибербезопасность была одним из приоритетов повестки дня, определенных Россией в этой организации. К числу основных проектов и инициатив по кибербезопасности в рамках ШОС стоит отметить:

– Обсуждение усиления государственного контроля над интернетом как следствие протестов в арабских странах.

– Создание киберполиции (2011, данная инициатива не была реализована).

– Усиление сотрудничества по безопасности в интернете.

– Борьба с финансированием терроризма через интернет.

– Проект Кодекса поведения в сфере международной информационной безопасности (в письме ШОС в ООН 12.09.2011)

Еще одним инструментом продвижения интересов России в сфере кибербезопасности становится формат БРИКС. В рамках этой структуры борьба с киберугрозами названа одном из четырех сфер перспективного сотрудничества. Обсуждаются идеи создания Центра киберугроз БРИКС, а также «горячей линии» для информирования и предупреждения о киберинцидентах наподобие той, которая уже существует между Россией и США.

[23] Working Towards Rules for Governing Cyber Conflict. Rendering the Geneva and Hague Conventions in Cyberspace. Advanced Edition Prepared by Russia-U.S. Bilateral on Critical Infrastructure Protection for the 2011 Munich Security Conference. NY: EastWest Institute, February 2011.

Заключение

Таким образом, главной правовой проблемой можно назвать отсутствие единого и целостного международного законодательства в сфере регулирования киберпространства. Сегодня действуют только отдельные нормы международного права или национальных законодательств. Проблемой можно также назвать противоречивость отдельных положений внутри источников международного права (в частности, в Международном телекоммуникационном соглашении 1973 г.), которые могут использоваться акторами в своих интересах.

Что касается направлений для дальнейших исследований, то на данный момент имеют место лакуны в отношении того, какие критерии нужно применять для оценки эффективности кибервойны. При этом необходимо различать оценку потенциальной мощи для ведения кибервойны и эффективности политики кибервойны. Существующие индексы / рейтинги потенциала кибервойны редко учитывают вышеупомянутую разницу.

Литература:

Бойко С.М. Группа правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности: взгляд из прошлого в будущее // Международная жизнь. – 2016. – № 8. – С. 53-71.

Болгов Р.В. Информационные технологии в современных вооруженных конфликтах и военных стратегиях (политические аспекты). Диссертация на соискание ученой степени кандидата политических наук / Санкт-Петербургский государственный университет. – СПб, 2011.

Болгов Р.В., Васильева Н.А., Виноградова С.М., Панцерев К.А. Информационное общество и международные отношения / Отв. Ред. Панцерев К.А. – СПб, 2014. – 384 с.

Демидов О.В. Обеспечение международной информационной безопасности и российские национальные интересы // Индекс безопасности. – 2013. – № 1 (104). – С. 129-168.

Зиновьева Е.С. Анализ внешнеполитических инициатив РФ в области международной информационной безопасности // Вестник МГИМО-Университета. – 2014. – № 6 (39). – С. 47-52.

Информационные вызовы национальной и международной безопасности / И.Ю. Алексеева и др.; Под общ. ред. А.В. Федорова, В.Н. Цыгичко. – М.: ПИР-Центр, 2001.

Квантaлиани И.Э. Роль международных организаций в деле обеспечения безопасности информационного пространства // Актуальные проблемы современного международного права. Материалы X ежегодной Всероссийской научно-практической конференции. 2012. – С. 26-30.

Лобанова Е.Н. Некоторые инициативы РФ в ООН по решению проблемы международной информационной безопасности // Глобализация и проблема войн в современном мире. Сборник статей. Под общ. ред. В.В. Барабаша. – М., 2011. – С. 29-35.

Международная информационная безопасность: дипломатия мира. Сборник материалов / Под общ. ред. Комова С.А. – М., 2009. – 272 с.

Ромашкина Н.П. ООН и международная информационная безопасность // Безопасность и контроль над вооружениями 2015-2016. Международное взаимодействие в борьбе с глобальными угрозами. – Москва, 2016. – С. 273-286.

Томилова Ю.Н. ООН и проблема обеспечения международной информационной безопасности // Международная жизнь. – 2015. – № 8. – С. 73-85.

Ширин С.С. Российские инициативы по вопросам управления Интернетом // Вестник МГИМО Университета. – 2014. – № 6 (39). – С. 73-81.

Clarke, R.; Knake, R. Cyberwar. The Next Threat to National Security and What to Do about It. HarperCollins Publishers New York, 2010.

Hundley, R.; Anderson, R. Security in Cyberspace: An Emerging Challenge for Society, 1994.

Hurwitz, R. The Play of States: Norms and Security in Cyberspace // *American Foreign Policy Interests*, 2014, Vol. 36, Issue 5, pp. 322-331. DOI: 10.1080/10803920.2014.969180

Kane, A. The Rocky Road to Consensus: The Work of UN Groups of Governmental Experts in the Field of ICTs and in the Context of International Security, 1998–2013 // *American Foreign Policy Interests*, 2014, Vol. 36, Issue 5, pp. 314-321. DOI: 10.1080/10803920.2014.969175

Maurer, T. Cyber Norm Emergence at the United Nations: An Analysis of the Activities of the UN Regarding Cybersecurity. Cambridge, MA: Harvard Kennedy School's Belfer Center for Science and International Affairs, 2011. P. 22.

Nye, J.; Owens, W. America's Information Age: The Nature of Power // *Foreign Affairs*, March-April 1996.

Working Towards Rules for Governing Cyber Conflict. Rendering the Geneva and Hague Conventions in Cyberspace. Advanced Edition Prepared by Russia-U.S. Bilateral on Critical Infrastructure Protection for the 2011 Munich Security Conference. NY: EastWest Institute, February 2011.

References:

Boiko, S.M. Gruppa pravitel'stvennyh ehkspertov OON po dostizheniyam v sfere informatizacii i telekommunikacij v kontekste mezhdunarodnoj bezopasnosti: vzglyad iz proshlogo v budushchee (UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: a View from the Past to the Future) // *Mezhdunarodnaya zhizn'*, 2016, No. 8, pp. 53-71.

Bolgov, R.V. Informacionnye tekhnologii v sovremennyh vooruzhennyh konfliktah i voennyh strategiyah (politicheskie aspekty) (Information Technology in Contemporary Armed Conflicts and Military Strategies (Political Aspects)). Thesis for a PhD degree in Political Science / Saint Petersburg State University. St. Petersburg, 2011.

Bolgov, R.V.; Vasilyeva, N.A.; Vinogradova, S.M.; Pantserev, K.A. Informacionnoe obshchestvo i mezhdunarodnye otnosheniya (Information Society and International Relations) / Ed. Pantserev K.A. St. Petersburg, 2014. 384 p.

Clarke, R.; Knake, R. Cyberwar. The Next Threat to National Security and What to Do about It. HarperCollins Publishers New York, 2010.

Demidov, O.V. Obespechenie mezhdunarodnoj informacionnoj bezopasnosti i rossijskie nacional'nye interesy (Ensuring International Information Security and National Interests of Russia) // *Indeks bezopasnosti*, 2013, No. 1 (104), pp. 129-168.

Hundley, R.; Anderson, R. Security in Cyberspace: An Emerging Challenge for Society, 1994.

Hurwitz, R. The Play of States: Norms and Security in Cyberspace // *American Foreign Policy Interests,* 2014, Vol. 36, Issue 5, pp. 322-331. DOI: 10.1080/10803920.2014.969180

Kane, A. The Rocky Road to Consensus: The Work of UN Groups of Governmental Experts in the Field of ICTs and in the Context of International Security, 1998–2013 // *American Foreign Policy Interests*, 2014, Vol. 36, Issue 5, pp. 314-321. DOI: 10.1080/10803920.2014.969175

Kvantaliani, I.E. Rol' mezhdunarodnyh organizacij v dele obespecheniya bezopasnosti informacionnogo prostranstva [The Role of International Organizations in the Security of Information Space]. Aktual'nye problemy sovremennogo mezhdunarodnogo prava. Materialy X ezhegodnoj Vserossijskoj nauchno-prakticheskoj konferencii (Actual Problems of Modern International Law. Materials of the 10th All-Russian Annual Scientific Conference), 2012. Pp. 26-30.

Lobanova, E.N. Nekotorye iniciativy RF v OON po resheniyu problemy mezhdunarodnoj informacionnoj bezopasnosti (Some Russian Initiatives in the United Nations to Address the Issue of International Information Security). Globalizaciya i problema vojn v sovremennom mire. Sbornik statej (Globalization and the Problem of War in the Modern World. Digest of Articles). Ed. Barabash V.V. Moscow, 2011. C. 29-35.

Maurer, T. Cyber Norm Emergence at the United Nations: An Analysis of the Activities of the UN Regarding Cybersecurity. Cambridge, MA: Harvard Kennedy School's Belfer Center for Science and International Affairs, 2011. P. 22.

Mezhdunarodnaya informacionnaya bezopasnost': diplomatiya mira (International Information Security: Diplomacy around the World). Collection of materials, Ed. Komov S.A. Moscow, 2009, 272 p.

Informacionnye vyzovy nacional'noj i mezhdunarodnoj bezopasnosti (Information Challenges to National and International Security). Alekseev I.Y. etc.; Ed. Fedorov, A.V., Tsygichko, V.N. Moscow, PIR-Center, 2001.

Nye, J.; Owens, W. America's Information Age: The Nature of Power // *Foreign Affairs,* March-April 1996.

Romashkina, N.P. OON i mezhdunarodnaya informacionnaya bezopasnost' (The UN and the International Information Security). Bezopasnost' i kontrol' nad vooruzheniyami 2015-2016. Mezhdunarodnoe vzaimodejstvie v bor'be s global'nymi ugrozami (Security and

Arms Control 2015-2016. International Cooperation in the Fight Against Global Threats). Moscow, 2016, pp. 273-286.

Shirin S.S. Rossijskie iniciativy po voprosam upravleniya Internetom (Russian Initiatives on Internet Governance) // *Vestnik MGIMO Universiteta*, 2014, No. 6(39), pp. 73-81.

Tomilova, Y.N. OON i problema obespecheniya mezhdunarodnoj informacionnoj bezopasnosti (The UN and the Problem of Ensuring International Information Security) // *Mezhdunarodnaya zhizn'*, 2015, No. 8, pp. 73-85.

Working Towards Rules for Governing Cyber Conflict. Rendering the Geneva and Hague Conventions in Cyberspace. Advanced Edition Prepared by Russia-U.S. Bilateral on Critical Infrastructure Protection for the 2011 Munich Security Conference. NY: EastWest Institute, February 2011.

Zinovieva, E.S. Analiz vneshnepoliticheskih iniciativ RF v oblasti mezhdunarodnoj informacionnoj bezopasnosti (Analysis of Russian Foreign Policy Initiatives in the Field of International Information Security) // *Vestnik MGIMO-Universiteta*, 2014, No. 6(39), pp. 47-52.

DOI: 10.24411/2221-3279-2019-10004

UN ACTIVITIES IN THE FIELD OF INFORMATION AND INTERNATIONAL ASPECTS OF RUSSIAN INFORMATION SECURITY

Radomir V. Bolgov

Saint Petersburg State University, Saint Petersburg, Russia

Article history:

Received:

11.12.2017

Accepted:

24.08.2018

About the author:
Candidate of Political Science,
Associate Professor, World Politics Department, Saint Petersburg State University

e-mail: rbolgov@yandex.ru

Key words:
international information security;
cyber security; Internet; United Nations;
Russia's foreign policy;
international organizations

Abstract: The study focuses on the policy of Russia in the UN on issues of information security. We analyze basic doctrines and documents regulating information security policy in Russia, as well as international legal Russian initiative. In addition, we present the work of the UN in this realm as a context for the Russian initiatives on international information security. We argue the necessity of joint actions of Russia and the United Nations to fight information security threats.

Acknowledgements: The article is prepared with the financial support of the Russian Science Foundation, project No. 16-18-10315

Для цитирования: Болгов Р.В. Деятельность ООН в области информации и международные аспекты информационной безопасности России // *Сравнительная политика*. – 2019. – № 1. – С. 59-69.

DOI: 10.24411/2221-3279-2019-10004

For citation: Bolgov, Radomir V. Deyatel'nost' OON v oblasti informatsii i mezhdunarodnye aspekty informatsionnoj bezopasnosti Rossii (UN Activities in the Field of Information and International Aspects of Russian Information Security) // *Comparative Politics Russia,* 2019, No. 1, pp. 59-69.

DOI: 10.24411/2221-3279-2019-10004