DOI: 10.7256/2454-0633.2017.1.20710
При цитировании этой статьи сноска на doi обязательна

НОРМОТВОРЧЕСКАЯ И ПРАВОПРИМЕНИТЕЛЬНАЯ ДЕЯТЕЛЬНОСТЬ МЕЖДУНАРОДНЫХ ОРГАНИЗАЦИЙ

Ефремов А.А.

РАЗВИТИЕ РЕГУЛИРОВАНИЯ ИНФОРМАЦИОННОЙ ИЛИ «ЦИФРОВОЙ» БЕЗОПАСНОСТИ В ДОКУМЕНТАХ МЕЖДУНАРОДНЫХ ОРГАНИЗАЦИЙ

Аннотация. *Объектом исследования в данной статье являются современные тенденции развития международной информационной или «цифровой» безопасности. Автором рассмотрены доклад Группы правительственных экспертов Организации Объединенный Наций по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности 2015 г., документы Шанхайской организации сотрудничества, Организации договора о коллективной безопасности, а также Рекомендация Организации экономического сотрудничества и развития по управлению рисками цифровой безопасности для экономического и социального процветания 2015 г. Автором проведен сравнительный анализ моделей информационной безопасности, закрепленных в российском законодательстве и продвигаемых Россией в ООН, ШОС, ОДКБ, и концепции управления рисками цифровой безопасности ОЭСР. С учетом интеграционных процессов в Евразийском экономическом союзе, формированием единого цифрового пространства Евразийской экономической комиссии, а также стремлением государств – членов ЕАЭС к вступлению в ОЭСР, необходимо обеспечить согласование действующих механизмов обеспечения информационной безопасности и концепции управления рисками цифровой безопасности. В этой связи автором разработаны предложения по возможным изменениям российского законодательства об информационной безопасности.*

Ключевые слова: *ОДКБ, международные организации, международное право, информационное право, информационная безопасность, интеграция, Организация Объединенных Наций, ОЭСР, управление рисками, цифровая безопасность.*

Abstract: *The object of this article is the modern trends in development of the international information or digital security. The author considers the report of the United Nations Group of Governmental Experts on achievements in the field of information and telecommunications in 2015, documents of the Shanghai Cooperation Organization, the Collective Security Treaty Organization, as well as the Organization for Economic Cooperation and Development Recommendation on digital security risk management for economic and social prosperity in 2015. The author conducts a comparative analysis of the information security models established in Russian legislation and advanced by Russia in the UN, SCO, OCSTO, and the concept of digital security risk management of OECD. Taking into account the integration processes in the Eurasian Economic Union, formation of a unified digital space of the Eurasian Economic Commission, as well as the desire the EAEU member states to enter the OECD, it is necessary to ensure coordination between the existing mechanisms of information security and the OECD concept on digital security risk management. On the basis*

DOI: 10.7256/2454-0633.2017.1.20710
При цитировании этой статьи сноска на doi обязательна

of comparative analysis, the author has developed proposals pertaining to the possible changes in the Russian information security legislation.
Keywords: *United Nations, Collective Security Treaty Organization, international organisations, international law, information law, information security, integration, OECD, risk management, digital security.*

В настоящее время в рамках различных международных организаций идет активное формирование [1, с. 133-138] модельного регулирования вопросов информационной или «цифровой» безопасности [2, с. 120]. По своей юридической природе принимаемые документы органов международных организаций носят в значительной мере рекомендательный характер и относятся к так называемому «мягкому праву» (англ. – soft law). Вместе с тем, указанные рекомендации и декларации активно имплементируются в национальное законодательство государств – участников соответствующих международных организаций.

Формирование моделей правового регулирования информационной безопасности идет как на универсальном уровне (в рамках ООН), так и на региональном – в рамках таких международных организаций, как Шанхайская организация сотрудничества (ШОС), Организация Договора о коллективной безопасности (ОДКБ), Организация экономического сотрудничества и развития (ОЭСР). При этом данные модели имеют серьезные различия концептуального порядка, и для полноценной интеграции РФ в деятельность указанных организаций необходимо определение возможностей согласования различных подходов к регулированию информационной или «цифровой» безопасности [3].

В настоящее время можно выделить две тенденции развития права международной информационной безопасности.

Первая, традиционная, основана на концепции угроз информационной безопасности, а также признания ключевой роли государств в регулировании данной сферы и «многостороннего» (*англ. – multi-lateral*) регулирования (мультилатерализма). Данное направление развития осуществляется в рамках работы периодически формируемых групп правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, а также в рамках таких международных организаций, как Шанхайская организация сотрудничества (ШОС) и Организация Договора о коллективной безопасности (ОДКБ).

Вторая тенденция основывается на концепции управления рисками цифровой безопасности в рамках ОЭСР и так называемого много-субъектного регулирования (*англ. – multi-stakeholder regulation*).

Концепцию «мультистейкхолдеризма» (*англ. – multistakeholderism*) следует определять именно как «много-субъектное регулирование» (*англ. – multi-stakeholder regulation*) [4, с. 29-49]. Ее ключевым отличием от мультилатерализма является включение в число субъектов-регуляторов не только государств, но и граждан, бизнеса и институтов гражданского общества. Следует отметить, что противостояние двух подходов – мультистейкхолдерной модели, основанной на участии всех заинтересованных сторон, и мультилатеральной, которая отдает приоритет международной дипломатии и международным организациям, было рассмотрено 7 апреля 2016 г. на 7 Российском форуме по управлению Интернетом. У. Дрейк высказал мнение, что две эти модели следует рас-

DOI: 10.7256/2454-0633.2017.1.20710
При цитировании этой статьи сноска на doi обязательна

сматривать не как взаимоисключающие, а как взаимодополняющие, а мультистейкхолдерной модели следует заимствовать у мультилатерализма более строгое следование законам и правилам [5].

В рамках ООН еще в 1998 г. по инициативе РФ была принята резолюция «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» (A/RES/53/70), предусматривающая подготовку периодических докладов Генерального секретаря ООН по данной теме, содержащих позиции государств-членов ООН по таким вопросам, как:

– общая оценка проблем информационной безопасности;

– усилия, предпринимаемые на национальном уровне для укрепления информационной безопасности и содействия международному сотрудничеству в этой области;

– содержание концепций (информационная безопасность, несанкционированное вмешательство, неправомерное использование);

– возможные меры, которые могли бы быть приняты международным сообществом для укрепления информационной безопасности на глобальном уровне.

С 2010 г. Генеральным секретарем ООН представлялись доклады, содержащие позиции государств по вопросам информационной безопасности (2010 г. – A/65/154, 2011 г. – A/66/152, 2013 г. – A/68/156, 2014 – A/69/112).

Кроме того, в период 2004-2015 г.г. были созданы 4 группы правительственных экспертов, представлявшие свои доклады соответственно, на 60-й, 65-й, 68-й и 70-й сессиях Генеральной ассамблеи ООН.

В последнем докладе Группы правительственных экспертов, представленной на 70-й сессии Генеральной ассамблеи ООН в 2015 г. [6], отражены рекомендации в отношении правил или принципов ответственного поведения государств, призванных способствовать обеспечению открытой, безопасной, стабильной, доступной и мирной ИКТ-среды:

а) в соответствии с целями Устава ООН, в том числе касающимися поддержания международного мира и безопасности, государства должны сотрудничать в разработке и осуществлении мер по укреплению стабильности и безопасности в использовании ИКТ и предупреждению совершения действий в сфере ИКТ, признанных вредоносными или способных создать угрозу международному миру и безопасности;

б) в случае инцидентов в сфере ИКТ государства должны изучить всю соответствующую информацию, в том числе более общий контекст события, проблемы присвоения ответственности в ИКТ-среде, а также характер и масштабы последствий;

в) государства не должны заведомо позволять использовать их территорию для совершения международно-противоправных деяний с использованием ИКТ;

г) государства должны рассмотреть вопрос о наилучших путях сотрудничества в целях обмена информацией, оказания взаимопомощи, преследования лиц, виновных в террористическом и преступном использовании ИКТ, а также осуществлять другие совместные меры по противодействию таким угрозам;

д) в процессе обеспечения безопасного использования ИКТ государства должны соблюдать положения резолюций 20/8 и 26/13 Совета по правам человека о поощрении, защите и осуществлении прав человека в Интернете и резолюций 68/167 и 69/166 Генеральной Ассамблеи о праве на неприкосновенность личной жизни в эпоху цифровых технологий, чтобы обеспечить всестороннее уважение прав человека, включая право свободно выражать свое мнение;

DOI: 10.7256/2454-0633.2017.1.20710
При цитировании этой статьи сноска на doi обязательна

е) государство не должно осуществлять или заведомо поддерживать деятельность в сфере ИКТ, если такая деятельность противоречит его обязательствам по международному праву, наносит преднамеренный ущерб критически важной инфраструктуре или иным образом препятствует использованию и функционированию критически важной инфраструктуры для обслуживания населения;

и) государства должны принимать надлежащие меры для защиты своей критически важной инфраструктуры от угроз в сфере ИКТ, принимая во внимание резолюцию 58/199 Генеральной Ассамблеи о создании глобальной культуры кибербезопасности и защите важнейших информационных инфраструктур и другие соответствующие резолюции;

к) государства должны удовлетворять соответствующие просьбы об оказании помощи, поступающие от других государств, критически важная инфраструктура которых становится объектом злонамеренных действий в сфере ИКТ. Государства должны также удовлетворять соответствующие просьбы о смягчении последствий злонамеренных действий в сфере ИКТ, направленных против критически важной инфраструктуры других государств, если такие действия проистекают с их территории, принимая во внимание должным образом концепцию суверенитета;

л) государства должны принимать разумные меры для обеспечения целостности каналов поставки, чтобы конечные пользователи могли быть уверены в безопасности продуктов ИКТ. Государства должны стремиться предупреждать распространение злонамеренных программных и технических средств в сфере ИКТ и использование пагубных скрытых функций;

м) государства должны способствовать ответственному представлению информации о факторах уязвимости в сфере ИКТ и делиться соответствующей информацией о существующих методах борьбы с такими факторами уязвимости, чтобы ограничить, а по возможности и устранить возможные угрозы для ИКТ и зависящей от ИКТ инфраструктуры;

н) государства не должны осуществлять или заведомо поддерживать деятельность, призванную нанести ущерб информационным системам уполномоченных групп экстренной готовности к компьютерным инцидентам (также именуемым группами готовности к компьютерным инцидентам или группам готовности к инцидентам в сфере кибербезопасности) другого государства. Государство не должно использовать уполномоченные группы экстренной готовности к компьютерным инцидентам для осуществления злонамеренной международной деятельности.

Концепция международной информационной безопасности, основанная на определении угроз информационной безопасности, получила свое развитие в документах ШОС и ОДКБ.

В рамках ШОС 16 июня 2009 г. было подписано межправительственное Соглашение между правительствами государств—членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности, согласно которому каждое государство имеет равное право на защиту своих информационных ресурсов и критически важных структур от неправомерного использования и несанкционированного вмешательства, в том числе от информационных атак на них. Данное соглашение вступило в силу 2 июня 2011 г.

Вопросы международной информационной безопасности рассматриваются и в других документах ШОС. В частности, ряд положений содержит Уфимская декларация

DOI: 10.7256/2454-0633.2017.1.20710
При цитировании этой статьи сноска на doi обязательна

глав государств-членов Шанхайской организации сотрудничества 9-10 июля 2015 г. [7]:

– Государства-члены будут наращивать согласованные усилия по укреплению международной информационной безопасности;

– Государства-члены активизируют совместные усилия по созданию мирного, безопасного и открытого информационного пространства, основанного на принципах сотрудничества, уважения государственного суверенитета, территориальной целостности и невмешательства во внутренние дела других стран. С этой целью они и далее будут укреплять взаимодействие в вопросах формирования комплексной системы обеспечения безопасности информационного пространства, активно бороться с распространением террористических, сепаратистских, экстремистских и других радикальных идей посредством информационно-коммуникационных сетей;

– Государства-члены поддерживают выработку универсального кодекса правил, принципов и норм ответственного поведения государств в информационном пространстве и рассматривают новую редакцию «Правил поведения в области обеспечения международной информационной безопасности», распространенную в январе 2015 года от лица государств-членов ШОС в качестве официального документа ООН, как важный шаг в этом направлении.

В рамках Парламентской Ассамблеи Организации Договора о коллективной безопасности также приняты Рекомендации по сближению и гармонизации национального законодательства государств – членов ОДКБ в сфере обеспечения информационно-коммуникационной безопасности от 27 ноября 2014 г. №7-6 [8].

Документы, разработанные по инициативе РФ в вышеуказанных международных организациях, явились основой и для формирования международно-договорных норм – 11 июля 2014 г. было подписано межправительственное Соглашение между Правительством Российской Федерации и Правительством Республики Куба о сотрудничестве в области обеспечения международной информационной безопасности, а 8 мая 2015 г. – аналогичное соглашение с Правительством Китайской Народной Республики. Документ вступил в силу 10 августа 2016 г.

Вторым направлением международно-правового регулирования в указанной сфере является развитие управления рисками «цифровой» безопасности, разрабатываемого в рамках Организации экономического сотрудничества и развития.

17 сентября 2015 г. Совет ОЭСР принял Рекомендацию и сопроводительный документ по управлению рисками цифровой безопасности для экономического и социального процветания (Digital security risk management for economic and social prosperity. OECD Recommendation and Companion Document. 17 September 2015 – C (2015) 115) [9].

Нацеливая государства на принятие стратегий цифровой безопасности, данная Рекомендация не содержит упоминаний о суверенитете государств в цифровом пространстве. Однако при этом неоднократно подчеркивается значимость вовлечения всех заинтересованных субъектов (*англ. – all stakeholders*), т.е. Рекомендация ориентирована на так называемое много-субъектное регулирование (*англ. – multi-stakeholder regulation*), и разработку соответствующих стратегий всеми субъектами [10, с. 180-191].

Рекомендация уже начинает активно рассматриваться в странах-членах ОЭСР (Италия [11, с. 168-174], Австралия [12, с. 177-198]).

DOI: 10.7256/2454-0633.2017.1.20710
При цитировании этой статьи сноска на doi обязательна

Концепция управления рисками цифровой безопасности развивается и в принятой 23 июня 2016 г. Канкунской Декларации ОЭСР о цифровой экономике 2016 г [13]. В п. 5 данной Декларации указывается на необходимость продвижения управления рисками цифровой безопасности и защиты неприкосновенности частной жизни на самом высоком уровне для укрепления доверия, а также на необходимость разработки с этой целью совместных стратегий, которые имеют решающее значение для экономического и социального процветания, осуществления поддержки цифровой безопасности и практики управления рисками.

Несмотря на приостановку переговорного процесса о присоединении России к ОЭСР, темпы экспертного сотрудничества сохраняются и даже наращиваются, продолжается процесс гармонизации российского законодательства с документами ОЭСР. Интерес к вступлению в ОЭСР имеют и российские партнеры по Евразийскому экономическому союзу (Армения, Казахстан). В этой связи и процессы интеграции цифрового пространства ЕАЭС, которые идут под эгидой Евразийской экономической комиссии [14, с. 18-21], также будут учитывать концепцию управления рисками цифровой безопасности.

Ключевыми проблемами реализации данной концепции в российском законодательстве в настоящее время являются:

1) Ни действующий Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ, ни Доктрина информационной безопасности РФ, утв. Президентом РФ 09.09.2000 № Пр-1895, ни проект новой Доктрины, размещенный на официальном сайте Совета безопасности РФ в июле 2016 г. [15, с. 62-66], вообще не используют термины «риск» и «управление рисками». Российская модель информационной безопасности, развиваемая в том числе в документах ШОС и ОДКБ, ориентирована на отражение угроз информационной безопасности, а не оценку и управление рисками. В этой связи возможная реализации концепции управления рисками цифровой безопасности потребует серьезных изменений понятийного аппарата и механизмов обеспечения информационной безопасности, закрепленных в российском законодательстве.

2) Согласно Рекомендации ОЭСР, цифровые риски, вместо того, чтобы рассматриваться в качестве технической проблемы, которая требует технических решений, рассматриваются как экономические риски. Поэтому управление рисками цифровой безопасности должно быть составной частью общего процесса управления рисками и принятия решений в каждой организации. Реализация данного похода потребует разработок методик оценок рисков вместо существующих моделей угроз информационной безопасности.

3) Рекомендация ориентирует государства на формирование целостной публичной политики управления рисками цифровой безопасности, включающую новые координационные механизмы правительства с неправительственными заинтересованными субъектами и повышение эффективности государственно-частного сотрудничества на национальном, региональном и международном уровнях. Реализация данного положения требует разработки в РФ механизмов государственно-частного партнерства в сфере информационной безопасности.

Решение данных проблем позволит согласовать имеющиеся концептуальные различия в подходах к правовому регулированию международной информационной безопасности и «цифровой» безопасности в условиях интеграции региональных «цифровых» пространств.

DOI: 10.7256/2454-0633.2017.1.20710
При цитировании этой статьи сноска на doi обязательна

Библиография:

1. Bello, P. Security and international cooperation dominate today's cyber policy landscape // Journal of Cyber Policy, 2016. Vol. 1. No. 1. P. 133-138. URL: http://dx.doi.org/10.1080/23738871.2016.1166255
2. Ellison, D., Venter, H. An ontology for digital security and digital forensics investigative techniques (Conference Paper) // Proceedings of The 11th International Conference on Cyber Warfare and Security (ICCWS2016). Boston, 2016. P. 120-128.
3. Ефремов А. Анализ текущего состояния и перспектив гармонизации российского законодательства в области научно-технической и инновационной политики с нормами ОЭСР // Информационный бюллетень «Новости ОЭСР». 2016. Вып. 3(6). С. 6-10. URL: https://oecdcentre.hse.ru/nletter6.4
4. Hofmann, J. Multi-stakeholderism in Internet governance: putting a fiction into practice // Journal of Cyber Policy. 2016. Vol. 1. Is. 1. P. 29-49. URL: http://dx.doi.org/10.1080/23738871.2016.1158303
5. Разные модели управления интернетом дополняют друг друга // Координационный центр национального домена сети Интернет. URL https://cctld.ru/ru/press_center/news/news_detail.php?ID=9661
6. Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. A/70/174. Официальный сайт ООН. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/37/PDF/N1522837.pdf?OpenElement
7. Уфимская декларация глав государств-членов Шанхайской организации сотрудничества 9-10 июля 2015 г. URL: http://sco-russia.ru/load/1013640909
8. Рекомендации по сближению и гармонизации национального законодательства государств-членов ОДКБ в сфере обеспечения информационно-коммуникационной безопасности от 27 ноября 2014 г. № 7-6 // Парламентская Ассамблея Организации Договора о коллективной безопасности. URL: http://www.paodkb.ru/upload/iblock/c07/rekomendatsii-po-sblizhen.-i-garmoniz.-natsion.-zak_va-gos._chlenov-odkb-v-sfere-obesp.-inf._kommunik.-bezop..pdf
9. OECD (2015), Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, Paris, 2015. 74 p.
10. Yilmaz, R., Yalman, Y. A Comparative Analysis of University Information Systems within the Scope of the Information Security Risks // TEM Journal. 2016. Vol 5. No.2 P.180–191. URL: https://dx.doi.org/10.18421/TEM52-10
11. Baldoni, R. Montanari, L. Italian National Cyber Security Framework // Proceedings of the International Conference on Security and Management (SAM' 2016). Athens, 2016. P. 168-174.
12. Ng J. International cybercrime, transnational evidence gathering and the challenges in Australia: finding the delicate balance //International Journal of Information and Communication Technology. 2016. Vol. 9. Issue 2. P. 177-198. URL: http://dx.doi.org/10.1504/IJICT.2016.078879
13. Cancún Ministerial Declaration on the Digital Economy // OECD URL: http://www.oecd.org/sti/ieconomy/Digital-Economy-Ministerial-Declaration-2016.pdf
14. Ефремов А.А. Формирование единого цифрового пространства Евразийского экономического союза и обеспечение государственного суверенитета в информационной сфере // Евразийский юридический журнал. 2016. № 5. С. 18-21.
15. Минбалеев А.В. Доктрина информационной безопасности Российской Федерации: современное состояние и перспективы развития // Вестник УрФО. Безопасность в информационной сфере. 2016. № 3. С. 62-66.

References (transliterated):

1. Bello, P. Security and international cooperation dominate today's cyber policy landscape // Journal of Cyber Policy, 2016. Vol. 1. No. 1. P. 133-138. URL: http://dx.doi.org/10.1080/23738871.2016.1166255
2. Ellison, D., Venter, H. An ontology for digital security and digital forensics investigative techniques (Conference Paper) // Proceedings of The 11th International Conference on Cyber Warfare and Security (ICCWS2016). Boston, 2016. P. 120-128.

DOI: 10.7256/2454-0633.2017.1.20710
При цитировании этой статьи сноска на doi обязательна

3. Efremov A. Analiz tekushchego sostoyaniya i perspektiv garmonizatsii rossiiskogo zakonodatel'stva v oblasti nauchno-tekhnicheskoi i innovatsionnoi politiki s normami OESR // Informatsionnyi byulleten' "Novosti OESR". 2016. Vyp. 3(6). S. 6-10. URL: https://oecdcentre.hse.ru/nletter6.4
4. Hofmann, J. Multi-stakeholderism in Internet governance: putting a fiction into practice // Journal of Cyber Policy. 2016. Vol. 1. Is. 1. P. 29-49. URL: http://dx.doi.org/10.1080/23738871.2016.1158303
5. Raznye modeli upravleniya internetom dopolnyayut drug druga // Koordinatsionnyi tsentr natsional'nogo domena seti Internet. URL https://cctld.ru/ru/press_center/news/news_detail.php?ID=9661
6. Yilmaz, R., Yalman, Y. A Comparative Analysis of University Information Systems within the Scope of the Information Security Risks // TEM Journal. 2016. Vol 5. No.2 P.180–191. URL: https://dx.doi.org/10.18421/TEM52-10
7. Baldoni, R. Montanari, L. Italian National Cyber Security Framework // Proceedings of the International Conference on Security and Management (SAM' 2016). Athens, 2016. P. 168-174.
8. Ng J. International cybercrime, transnational evidence gathering and the challenges in Australia: finding the delicate balance //International Journal of Information and Communication Technology. 2016. Vol. 9. Issue 2. P. 177-198. URL: http://dx.doi.org/10.1504/IJICT.2016.078879
9. Cancún Ministerial Declaration on the Digital Economy // OECD URL: http://www.oecd.org/sti/ieconomy/Digital-Economy-Ministerial-Declaration-2016.pdf
10. Efremov A.A. Formirovanie edinogo tsifrovogo prostranstva Evraziiskogo ekonomicheskogo soyuza i obespechenie gosudarstvennogo suvereniteta v informatsionnoi sfere // Evraziiskii yuridicheskii zhurnal. 2016. № 5. S. 18-21.
11. Minbaleev A.V. Doktrina informatsionnoi bezopasnosti Rossiiskoi Federatsii: sovremennoe sostoyanie i perspektivy razvitiya // Vestnik UrFO. Bezopasnost' v informatsionnoi sfere. 2016. № 3. S. 62-66.