https://doi.org/10.17816/RJLS19126

Роль международного права в обеспечении международной информационной безопасности

Костенко Николай Иванович,
доктор юридических наук, профессор,
член-корреспондент РАЕ, заслуженный деятель науки и образования,
заслуженный работник науки и образования,
старший научный сотрудник Научно-исследовательского центра
Краснодарского высшего военного училища
имени генерала армии С.М. Штеменко Министерства обороны РФ,
член международной ассоциации ученых, преподавателей и специалистов,
член Всемирной ассоциации международного права
E-mail: prof_48kost@mail.ru

Аннотация. *Целью исследования является формирование основных подходов к обеспечению государствами международной информационной безопасности. Рассматривается роль Российской Федерации и других государств в достижениях в сфере информатизации и телекоммуникаций в рамках международной безопасности. Обращается внимание на то, что быстрое формирование и активное использование технологий привели к сильной зависимости от них государств и, как следствие, появлению новых угроз.*

Исследуется роль Российской Федерации в целенаправленной деятельности по формированию доктрины Организации Объединенных Наций о мировой информационной кибербезопасности.

Обращается внимание на Резолюцию A/RES/56/19 Генеральной Ассамблеи ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», принятую 7 января 2002 г., в которой одобрено проведение исследований нынешних и возможных угроз в сфере информационной безопасности и рассматриваются вероятные коллективные меры по их ликвидации.

Анализируется предложение Российской Федерации об образовании группы экспертов, которая смогла бы рассматривать вопросы, изложенные в Резолюции Генеральной Ассамблеи ООН от 8 декабря 2003 г. № 58/32 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». Особое внимание в статье обращается на документ Генеральной Ассамблеи ООН A/55/140, в котором указаны пять принципов, касающихся обеспечения международной информационной безопасности.

В статье подробно анализируются принятые в период с 4 декабря 1998 г. по 22 октября 2018 г. резолюции Генеральной Ассамблеи Организации Объединенных Наций на тему «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности».

Новизной исследования являются выводы и предложения по проблемным вопросам в области обеспечения международной информационной безопасности, которые бы способствовали принятию единой международной Конвенции ООН, содержащей понятийный аппарат, цели, задачи, виды угроз, приоритетные направления и механизмы их реализации, а также положения об ответственности государств в международном информационном пространстве.

Ключевые слова*: информатизация, телекоммуникация, международная, информация, безопасность, угроза, резолюция, принципы, нормы, государства.*

Международная информационная безопасность зависит от информационного пространства. Информационное пространство — это сфера деятельности, которая связана с хранением информации, ее созданием, применением, модифицированием, передачей и оказывает воздействие как на индивидуальное, так и общественное сознание.

Формирование современного общества связано с процессами информатизации, совершенствованием информационных технологий и возникновением глобального информационного пространства. Тем не менее, как любое явление, кроме положительных сторон, оно имеет и свои неблагоприятные. Развитые государства с высоким уровнем компьютеризации различных сфер жизнедеятельности общества то и дело испытывают сложности, связанные с развитием технологий. Чем чаще осуществляется массовое использование ими информационных технологий и применение глобальных сетей, чем сложнее их информационная инфраструктура, тем ниже защищенность от кибератак и выше причиняемый вред. Так,

в США убытки от несанкционированного проникновения в подобные системы и последующей утечки информации оцениваются в десятки миллионов долларов [Маслакова, 2015, с. 75–77]. Быстрое формирование и активное использование технологий привели к тому, что государства оказались зависимы от них, а это повлекло за собой вероятность появления новых угроз. Чаще всего такие угрозы связаны с объективной возможностью применения информационно-коммуникационных технологий с целью создания конфликтов. В первую очередь обеспокоенность вызывают применение и распространение информационного оружия и возникающая в этой связи угроза информационных войн и информационного терроризма, которые могут нарушить международный мир и кибербезопасность.

Российская Федерация в лице Министерства иностранных дел в 1998 г. направила Генеральному секретарю ООН доктрину о мировой информационной кибербезопасности, которая получила свое практическое развитие в виде Резолюции под наименованием «Достижения в сфере информатизации и телекоммуникаций в связи с международной безопасностью», одобренной консенсусом 4 декабря 1998 г. Данная Резолюция подразумевала под собой возвращение к обсуждению проблемы информационной безопасности, так как для этого требовалось предложить необходимую формулировку киберугроз и принципов международного взаимодействия по этой проблеме[1].

Обеспечение международной информационной безопасности не представляется целью единственного, отдельно взятого, суверенного государства. Международная проблема всего мирового сообщества впервые была озвучена в Резолюции ООН от 1 декабря 1999 г. «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»[2], в которой обращалось внимание на киберугрозы применительно не только к гражданской, но и к армейской обстановке. С того времени практически ежегодно проводятся съезды представителей разных государств в рамках международных институтов для общего обсуждения и внесения изменений в программу по борьбе с информационной опасностью.

Генеральной Ассамблеей ООН 20 сентября 2000 г. на 55-й сессии был одобрен текст документа ООН A/RES/55/28 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»[3], который определяет программу сдерживания в области информационной безопасности и обращен на укрепление кибербезопасности в мировых гиперинформационных режимах. Министерством иностранных дел Российской Федерации в соответствии с документом ООН 55/28 разработан и рекомендован ООН текст «Общая оценка проблем информационной безопасности. Угрозы международной информационной безопасности». В тексте подчеркнуты и описаны одиннадцать основных ситуаций, влекущих за собой угрозу нуждам человека и государствам в информационном пространстве. К таким ситуациям относятся создание и применение способов неразрешенного вмешательства в деятельность вновь образованных государств и направленное информационное влияние на важные органы и госструктуры таких государств и население; операции, направленные на преобладание в информационном пространстве, стимулирование терроризма, в конечном счете овладение информационными войнами и т.д.[4].

В Резолюции A/RES/56/19 Генеральной Ассамблеи ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»[5], принятой 7 января 2002 г., были одобрены идеи в отношении исследования нынешних и возможных угроз в сфере информационной безопасности и вероятные коллективные меры по их ликвидации[6].

Важными являются резолюции Генеральной Ассамблеи ООН от 30 декабря 2002 г. A/RES/57/53 «Достижения в сфере информатизации и телекоммуникаций в контексте

[1] См.: Проект документа Министерства иностранных дел РФ «Общая оценка проблем информационной безопасности. Угрозы международной информационной безопасности». URL: http://esa-conference.ru/wp-content/uploads/files/pdf/SHirin-Sergej-Sergeevich.pdf (дата обращения: 12.11.2019).

[2] См.: Резолюция Генеральной Ассамблеи от 29 ноября 2001 г. A/RES/56/19. URL: https:// www.un.org/ga/search/view_ doc.asp? symbol=A/RES/56/19 (дата обращения: 12.11.2019).

[3] См.: Резолюция ООН от 20 сентября 2000 г. A/RES/55/28 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». URL: https://www. un.org/ga/search/ view_ doc.asp?symbol=A/RES/55/28 (дата обращения: 12.11.2019).

[4] См.: Проект документа Министерства иностранных дел РФ «Общая оценка проблем информационной безопасности. Угрозы международной информационной безопасности». URL: http://esa-conference.ru/wp-content/uploads/files/pdf/SHirin-Sergej-Sergeevich.pdf (дата обращения: 12.11.2019).

[5] См.: Резолюция Генеральной Ассамблеи от 29 ноября 2001 г. A/RES/56/19. URL: https:// www.un.org/ga/search/view_doc.asp? symbol= A/RES/56/19 (дата обращения: 12.11.2019).

[6] См.: Резолюция Генеральной Ассамблеи от 7 января 2002 г. A/RES/56/19 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N01/476/30/PDF/N0147630.pdf (дата обращения: 12.11.2019).

международной безопасности»[7] и от 8 декабря 2003 г. A/RES/58/321 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»[8]. Первая отмечает невозможность применения информационно-телекоммуникационных технологий ради дестабилизации обстановки в отдельно взятом регионе. Вторая же резолюция открывает поиск практических решений проблемы. В общем, две эти резолюции продолжают развивать предыдущие, таким образом, за это время была выработана единая теоретическая база, которая позволила в рамках международного права искать решение сложной проблемы. Российская Федерация в апреле 2003 г. направила в Секретариат ООН доклад «Вопросы, связанные с работой Группы правительственных экспертов по проблеме информационной безопасности»[9], в котором содержалась российская позиция по работе указанной Группы и отмечалась необходимость стремиться к выработке многостороннего, взаимоприемлемого, основанного на праве международного документа, нацеленного на закрепление универсального правового порядка международной информационной безопасности.

По решению Российской Федерации состав правительственных экспертов смог бы сконцентрировать обсуждение на следующих важных стадиях:

— регулирование предмета исследования в области международной информационной безопасности;

— поиск обстоятельств, воздействующих на международную информационную безопасность с учетом присутствия угроз как уголовно-правового, так и военного характера;

— установление приемлемых мер, предупреждающих применение информационных кибертехнологий и систем в террористических и других преступных намерениях;

— исследование средств международного сотрудничества правоохранительных органов по предупреждению и пресечению злодеяний в информационном пространстве и установлению причин информационной агрессии;— исследование предоставления международного сотрудничества государствам, пострадавшим от информационных нападений, с целью облегчить результаты несоблюдения соответствующих действий в первую очередь для объектов критических инфраструктур государств[10].

Данные стадии нацеливают субъектов международного права на участие в Резолюции Генеральной Ассамблеи ООН от 8 декабря 2003 г. № 58/32 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»[11], в которой выражается обеспокоенность тем, что эти технологии и средства, вероятно, могут быть применены для задач, несоответствующих обеспечению международной устойчивости и безопасности, а также могут критически влиять на единство механизма государств, нарушая их безопасность как в гражданской, так и в военной сферах. Тем самым составители Резолюции считают должным предупредить применение информационных возможностей или кибертехнологий в криминальных или террористических планах.

Кроме того, Российская Федерация подготовила проект «Принципов, касающихся международной информационной безопасности» и опубликовала документ Генеральной Ассамблеи ООН A/55/140 о вкладе России в дальнейшее обсуждение темы: «Обеспечение международной информационной безопасности».

В документе Генеральной Ассамблеи ООН A/55/140 были изложены пять принципов, касающихся обеспечения международной информационной безопасности.

Принцип I. Участие любого государства и других субъектов международного права в международном информационном пространстве. Такая работа должна стать совместимой с правом каждого государства искать, получать и распространять информацию и идеи, как это зафиксировано в соответствующих документах Организации Объединенных Наций, с учетом того, что такое право может быть ограничено международной нормой в целях защиты интересов безопасности. При этом каждое

[7] См.: Резолюция Генеральной Ассамблеи ООН от 30 декабря 2002 г. A/RES/57/53 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N02/541/47/PDF/N0254147.pdf (дата обращения: 12.11.2019).

[8] См.: Резолюция Генеральной Ассамблеи ООН от 8 декабря 2003 г. A/RES/58/32 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N03/454/85/PDF/N0345485.pdf (дата обращения: 12.11.2019).

[9] См.: Стрельцов А.Л., Крутских Л.В. Право в обеспечении международной информационной безопасности // URL: http://www.zhenilo.narod.ru//main/ ips/2007_common_problems.pdf (дата обращения: 15.11.2019).

[10] См.: Продвижение российских инициатив в области обеспечения международной информационной безопасности. URL: https://studme.org/78414/pravo/prodvizhenie_rossiyskih_ initsiativ_oblasti_ obespecheniya_mezhdunarodnoy_informatsionnoy_bezopasnosti (дата обращения: 15.11.2019).

[11] См. Резолюция Генеральной Ассамблеи ООН от 8 декабря 2003 г. № 58/32 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». URL: https://www.un.org/ga/search/view_doc.asp?symbol= A/RES/58/32 (дата обращения: 15.11.2019).

государство и другие субъекты международного права должны иметь равные права на защиту своих информационных ресурсов и критически важных структур от незаконного применения и несанкционированного информационного вмешательства и могут рассчитывать на поддержку мирового сообщества в реализации этих прав.

Принцип II. Государства должны стремиться к ограничению угроз в сфере международной информационной безопасности и с этой целью воздерживаться от:

— применения способов влияния и причинения вреда информационным источникам и режимам другого государства;

— целевого информационного воздействия на критически важные структуры другого государства;

— информационного воздействия с целью разрушения политической, экономической и социальной системы других государств;

— психологической обработки населения с целью дестабилизации общества;

— несанкционированного вмешательства в информационно-телекоммуникационные режимы, а также их незаконного применения;

— изучения условий технологической привязанности в области информатизации в ущерб другим государствам;

— поощрения международных террористических, экстремистских и преступных сообществ, организаций, групп и отдельных злоумышленников, осуществляющих угрозу информационным источникам и критически важным государственным структурам;

— утверждения планов, доктрин, предполагающих вероятность ведения информационных войн и способных спровоцировать гонку вооружений, а также создающих напряженность в отношениях между государствами с целью возникновения информационных войн;

— применения информационных технологий и средств в ущерб существенным правам и свободам человека, созданным в информационной сфере;

— трансграничного распространения информации, запрещенной международными принципами и нормами международного права;

— манипуляции информационными потоками, обмана и укрывательства информации с целью искажения психологической и духовной среды общества, эрозии традиционных культурных, нравственных, этических и эстетических ценностей.

Принцип III. Организация Объединенных Наций и соответствующие учреждения системы ООН обязаны способствовать международному сотрудничеству, целью чего должно являться сдерживание угроз в области международной информационной безопасности и создание международно-правовой основы для:

— установления доказательств и систематизации информационных войн;

— установления доказательств и спецификации информационного оружия и его состояний, которые возможно отнести к информационному оружию;

— ограничения оборота информационного оружия;

— недопущения создания, распространения и использования информационного оружия;

— предотвращения угрозы возникновения информационных войн;

— признания опасности применения информационного оружия в отношении критически важных госструктур, сопоставимой с угрозой применения оружия массового поражения;

— создания ситуации для равного положения и надежного международного информационного обмена на основании общепринятых норм и принципов международного права;

— устранения исчерпанных информационных технологий и условий в террористических и криминальных целях;

— устранения исчерпанных информационных технологий и средств для влияния на общественную психику с целью расшатывания общества и государства;

— разработки процедуры взаимного уведомления и предотвращения трансграничного несанкционированного информационного воздействия;

— образования структуры международного наблюдения для мониторинга угроз, обнаруживающихся в информационной сфере: создания устройства проверки реализации положений системы международной информационной безопасности;

— завершения спорных ситуаций в сфере информационной безопасности;

— формирования международного режима аттестации кибертехнологий и состояния информатизации и телекоммуникации (в том числе программно-технических) в отношении обеспечения их информационной безопасности;

— формирования структуры международного сотрудничества правоохранительных органов по устранению и предупреждению злодеяний в информационном пространстве;

— унификации на основании отсутствия необходимости государственного законодательства в части обеспечения информационной безопасности.

Принцип IV. Государства и другие субъекты международного права обязаны нести международную ответственность за функционирование в киберпространстве, находящееся под юрисдикцией либо в рамках международных

организаций, членами которой они являются, и соблюдать принципы, имеющиеся в документе Генеральной Ассамблеи ООН A/55/140 проект «Принципов, касающихся международной информационной безопасности».

Принцип V. Любой спор между государствами и другими субъектами международного права, возникающий из-за применения настоящих принципов, разрешается с помощью установленных процедур мирного урегулирования споров[12].

Из изложенного выше усматривается, что принципы являются своего рода рабочей версией кодекса поведения государств в информационном пространстве, они обеспечивают для них как минимум моральные обязательства и формируют основные положения для международных переговоров под эгидой ООН и других международных организаций по рассматриваемой проблематике.

Представляется, что в указанных принципах содержится существенная понятийная база по предмету «Право международной информационной безопасности», цитируются основополагающие формулировки: права международной информационной безопасности, угроз международной информационной безопасности, информационного оружия, информационной войны, международного информационного терроризма и международной преступности.

Указанные пять базовых принципов международной информационной безопасности выделяют роль права, обязательства и ответственность государств в информационном пространстве, намечают конкретные задачи, решение которых было бы направлено на ограничение угроз в сфере международной информационной безопасности, а также прописывают роль ООН в контексте общих усилий в этой области.

В 2011 г. очередным шагом России стало внесение в ООН конвенции, которая несла в себе цель закрепить на уровне международного права такие понятия, как информационная война, информационная безопасность, информационное оружие, терроризм в информационном пространстве и другие категории, которые не имели статуса общепринятых.

Таким же образом в конвенции предполагалось прописать статус суверенитета государства над его информационным пространством. Данная конвенция выступает в роли противовеса Европейской конвенции по киберпреступлениям (преступлениям в киберпространстве) от 23 ноября 2001 г.[13], Российская Федерация ее не подписывала по причине ряда разногласий. В частности, это касалось пункта о «трансграничном доступе», который напрямую нарушает целостность информационного поля отдельно взятого государства.

Первый комитет 69-й сессии Генеральной Ассамблеи ООН консенсусом 2 декабря 2014 г. принял очередную выдвинутую Российской Федерацией Резолюцию от 2 декабря 2014 г. A/RES/69/28 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»[14], в которой сохранены положения одноименной Резолюции от 3 декабря 2012 г. A/RES/67/27[15] о важности уважения прав человека и основных свобод в сфере информационно-коммуникационных технологий. В связи с этим с каждым годом все больше государств становятся соавторами этого документа. В 2014 г. таковыми стали более 50 стран. Документ обрел глобальный характер, так как его география охватила практически все регионы земного шара. В этом же году в четвертый раз была созвана Группа правительственных экспертов, в работе приняли участие более 50 стран. Приоритетным направлением исследований Группы являлись обнаружение угроз в сфере информационно-коммуникационных технологий и выработка совместного противодействия им. В результате работы Группы удалось достичь консенсуса по целому ряду вопросов. В частности, на первое место были поставлены угрозы международной информационной безопасности на современном этапе. К ним отнесли наращивание потенциала информационно-коммуникационных технологий в военных целях, рост их влияния в будущих конфликтах, подрыв деятельности стратегически важных объектов с помощью информационно-коммуникационных технологий и др.

В 2016 г. Россия предложила новый проект резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», которая была подготовлена

[12] См.: Доклад Генерального секретаря ООН «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности». URL: https://documents-dds-ny. un.org/doc/UNDOC/ GEN/N00/535/04/PDF/N0053504.pdf (дата обращения: 16.11.2019).

[13] См.: Европейская конвенция по киберпреступлениям (преступлениям в киберпространстве), 23 ноября 2001 г. URL: http://mvd.gov.by/ main.aspx? guid=4603 (дата обращения: 16.11.2019).

[14] См.: Резолюция от 2 декабря 2014 г. A/RES/69/28 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». URL: https://documentsdds-ny.un.org/doc/UNDOC/ GEN/N14/662/43/PDF/N1466243.pdf (дата обращения: 16.11.2019).

[15] См.: Резолюция от 3 декабря 2012 г. A/RES/67/27 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». URL: https://documentsdds-ny.un.org/doc/UNDOC/ GEN/N12/480/24/PDF/N1248024.pdf (дата обращения: 16.11.2019).

в соавторстве с 84 государствами. Среди них страны БРИКС, ШОС, СНГ, латиноамериканские и азиатские государства. Впервые соавторами этого документа стали также США, Япония и многие члены ЕС, включая Великобританию, Германию, Испанию, Нидерланды и Францию. Упомянутая Резолюция положила начало новому уровню международного сотрудничества в рамках ООН. Важно отметить тот факт, что инициативу по поводу участия в работе Группы правительственных экспертов 2016 г. проявили около 80 стран, что можно считать дипломатической победой Российской Федерации в этой сфере.

22 октября 2018 г. на 73-й сессии Генеральной Ассамблеи ООН в очередной раз была принята Резолюция ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», в которой отмечается, что, «хотя главная ответственность за обеспечение безопасности и мирной информационно-коммуникационной среды лежит на государствах, выявление механизмов вовлечения при необходимости организаций гражданского общества, частного сектора и научных кругов могло бы способствовать повышению эффективности международного сотрудничества, принять проект международного кодекса поведения для обеспечения международной информационной безопасности»[16].

Из Резолюции усматривается, что именно международные институты должны стать базой для обеспечения информационной безопасности в мире, а также сдерживающим механизмом в информационной войне. С помощью международных институтов появляется возможность оказывать влияние на субъекты международного права по возникающим вопросам, которые относятся к международному обеспечению информационной безопасности.

Изложенная позиция России рассматривалась ранее во многих международных организациях. В рамках ОДКБ 14 октября 2016 г. была утверждена Стратегия коллективной безопасности до 2025 г.[17] В ней была также рассмотрена и информационная безопасность. Ключевые позиции, выделенные в данном договоре, следующие:

— применение информационных и коммуникационных технологий в целях оказания деструктивного воздействия на общественно-политическую и социально-экономическую обстановку, а также манипулирования общественным сознанием в государствах — членах ОДКБ;

— формирование системы информационной безопасности государств-членов, развитие сотрудничества государств-членов в этой области, проведение совместных мероприятий по противодействию, создание условий для реализации совместных мероприятий.

Стратегической целью ОДКБ является обеспечение коллективной безопасности путем консолидации усилий и ресурсов государств — членов ОДКБ на основе стратегического партнерства, общепризнанных норм и принципов международного права. В основу реализации стратегической цели ОДКБ положен принцип обеспечения коллективной безопасности государств — членов ОДКБ через укрепление национальной безопасности каждого из них.

Государства Шанхайской организации сотрудничества (ШОС), выступившие союзниками в продвижении идеи обеспечения международной информационной безопасности, подготовили и подписали 16 июня 2009 г. в Екатеринбурге межправительственное соглашение о совместной деятельности в области обеспечения международной информационной безопасности, ставшее первым в международной практике документом, направленным на ограничение всего комплекса угроз международной информационной безопасности, включая их военно-политические, криминальные и террористические аспекты. Важным элементом этого Соглашения являются включенные в него согласованные, выработанные группой экспертов «Перечень основных понятий в области международной информационной безопасности» и «Перечень основных видов угроз в области международной информационной безопасности, их источников и признаков»[18].

2 июня 2011 г. вступило в силу Соглашение между правительствами государств — членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности[19]. В документе прописаны основные угрозы

[16] См.: Резолюция ООН от 5 декабря 2018 г. A/RES/73/27 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». URL: https://www.un.org/ ga/search/view_ doc.asp? symbol=A/RES/73/27 (дата обращения: 16.11.2019).

[17] См.: Стратегия коллективной безопасности ОДКБ на период до 2025 года. URL: http://www.odkb-csto.org/documents/detail.php?ELEMENT_ ID=8382 (дата обращения 16.11.2019).

[18] См.: Главная угроза человечества XXI века. На первое место в списке угроз человечеству Всемирная федерация ученых поставила информационную безопасность. URL: https://www. sb.by/articles/glavnaya-chelovechestva-xxi-veka-na-pervoe-mesto-v-spiske-ugroz- chelovechestvuvsemirnaya-federatsiya-uchenykh-postavila-informatsionnuyu-bezopasnost.html (дата обращения: 16.11.2019).

[19] См.: Соглашение между правительствами государств — членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности: заключено 16 июня 2009 г., вступило в силу 2 июня 2011 г. : URL: http://docs.cntd.ru/document/902289626 (дата обращения: 16.11.2019).

в области обеспечения международной информационной безопасности, основные направления, принципы и формы сотрудничества. Стоит отметить, что проработка данной проблематики в рамках ШОС остается на повестке дня и по сей день. Страны БРИКС воздержались от подписания соглашений о сотрудничестве по обеспечению информационной безопасности, однако данная проблема неоднократно прорабатывалась на заседаниях организации. Как уже отмечалось, в основном это связано с высокой вовлеченностью населения стран-участниц в телекоммуникационные информационные сети и высоким уровнем вредоносной активности внутри них. Также отмечается двойственный характер данной проблемы, потому как есть и страны — инициаторы хакерской активности, и их жертвы. Помимо этого, указанная проблема затрагивалась и в других международных организациях, таких как СНГ, Организация американских государств, АТЭС, АСЕАН, Африканский Союз, ЕС, ОБСЕ, Совет Европы, а также в рамках двухстороннего сотрудничества между странами. Следует отметить важность развития международно-правовых отношений в данной сфере с Китайской Народной Республикой. 8 мая 2015 г., согласно положениям Договора о добрососедстве, дружбе и совместной деятельности между Российской Федерацией и Китайской Народной Республикой 2001 г., заключено Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности. В Соглашении государства определили особое значение совместной работы в рамках ШОС, а также необходимость дальнейшего углубления доверия и развития взаимодействия в области использования информационно-коммуникационных технологий, отметили стремление формировать многостороннюю, демократическую и прозрачную международную систему управления информационно-коммуникационной сетью Интернет в целях реальной интернационализации управления сетью Интернет и обеспечения равных прав государств на участие в этом процессе, включая демократическое управление основными ресурсами информационно-коммуникационной сети Интернет и их справедливое распределение. Важным шагом международно-правового сотрудничества в области формирования общих подходов к проблематике международной информационной безопасности стало заключенное между Правительством Российской Федерации и Правительством Республики Куба двустороннее Соглашение о сотрудничестве в области обеспечения международной информационной безопасности (Гавана, 11 июля 2014 г.), вступившее в силу 2 января 2015 г., а также аналогичное Соглашение с Правительством Республики Беларусь (Москва, 25 декабря 2013 г.), вступившее в силу 27 февраля 2015 г. Государствами-участниками обозначены основные угрозы международной информационной безопасности, определены главные направления, общие принципы, формы и механизмы сотрудничества, что, несомненно, выводит на новый уровень отношения государств в данной сфере и вместе с тем создает нормативно-правовую базу для практического взаимодействия.

В завершение необходимо отметить, что в настоящее время существуют проблемные вопросы в области обеспечения международной информационной безопасности, на которые следовало бы обратить внимание.

Во-первых, в связи с тем, что Российская Федерация и ее западные партнеры активно разрабатывают собственные проекты конвенций в области обеспечения международной информационной безопасности (кибербезопасности), положения которых конкурируют между собой, до сих пор нет единой международной конвенции ООН, содержащей понятийный аппарат, цели, задачи, виды угроз, приоритетные направления и механизмы их реализации, а также положения об ответственности государств в международном информационном пространстве.

Во-вторых, западные государства рассматривают обеспечение защиты информационного пространства через понятие «кибербезопасность», Российская Федерация — через дефиницию «международная информационная безопасность». Однако в целях мирного сотрудничества и сосуществования в Российской Федерации разработан проект концепции Стратегии обеспечения кибербезопасности Российской Федерации[20].

В-третьих, в настоящее время имеет место стремление ряда стран к доминированию в мировом информационном пространстве. Такая деятельность не способствует эффективному сотрудничеству Российской Федерации с другими государствами, а также несет в себе угрозы конституционным правам и свободам человека и гражданина, информационному обеспечению государственной политики Российской Федерации, развитию отечественной индустрии информации, безопасности информационных средств и систем.

[20] См.: Проект концепции Стратегии кибербезопасности Российской Федерации. URL: cea8a73.pdf (дата обращения: 16.11.2019). В проекте концепции обосновываются необходимость и своевременность разработки Стратегии кибербезопасности Российской Федерации, определяются ее принципы и направления, а также ее место в системе нормативных актов государства.

В-четвертых, в Российской Федерации на законодательном уровне требуется закрепить эффективные гарантии защиты прав и свобод человека и гражданина от информационных угроз, связанных с негативным информационным воздействием на сознание как отдельных граждан, так и общества в целом.

В-пятых, в Российской Федерации необходимо «переориентировать» законодателя на то, чтобы выработка понятийного аппарата, определение основных видов угроз, целей, задач, наиважнейших направлений в области обеспечения международной информационной безопасности осуществлялась на уровне федерального закона, а не только через международные соглашения Российской Федерации и проекты международных конвенций.

В-шестых, для эффективного осуществления совместной деятельности в сфере обеспечения информационной безопасности необходимо гарантировать активное участие Российской Федерации во всех международных организациях, работающих в области информационной безопасности, а также защиты информации, стандартизации и сертификации средств информации.

Список литературы

1. Доклад Генерального секретаря ООН «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности». URL: https:// documents-dds-ny. un.org/doc/UNDOC/GEN/N00/535/04/ PDF/N0053504.pdf (дата обращения: 16.11.2019).
2. Европейская конвенция по киберпреступлениям (преступлениям в киберпространстве), 23 ноября 2001 г. URL: http://mvd.gov.by/main.aspx? guid=4603 (дата обращения: 16.11.2019).
3. Маслакова Е.А. К вопросу о международном сотрудничестве в сфере обеспечения информационной безопасности / Маслакова Е.А., Жилкин М.Г., Качалов В.В. // Вестник Московского университетата МВД России. 2015. № 9. С. 75-77.
4. Проект документа Министерства иностранных дел РФ «Общая оценка проблем информационной безопасности. Угрозы международной информационной безопасности». URL: http://esa-conference.ru/ wp-content/uploads/files/pdf/SHirin-Sergej-Sergeevich. pdf (дата обращения: 16.11.2019).
5. Проект концепции Стратегии кибербезопасности Российской Федерации. URL: http://council.gov.ru/ media/files/41d4b3dfbdb 25cea8a 73.pdf (дата обращения: 16.11.2019).
6. Резолюция Генеральной Ассамблеи от 29 ноября 2001 г. A/RES/56/19. URL: https:// www.un.org/ga/ search/view_ doc.asp? symbol=A/RES/56/19 (дата обращения: 16.11.2019).
7. Резолюция ООН от 20 сентября 2000 г. A/RES/55/28 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». URL: https://www. un.org/ga/search/view_doc.asp? symbol=A/RES/55/28 (дата обращения: 16.11.2019).
8. Резолюция Генеральной Ассамблеи от 29 ноября 2001 г. A/RES/56/19. URL: https:// www.un.org/ga/ search/view_doc.asp?symbol=A/RES/56/19 (дата обращения: 16.11.2019).
9. Резолюция Генеральной Ассамблеи от 7 января 2002 г. A/RES/56/19 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. URL: https:// documents-dds-ny.un.org/ doc/UNDOC/GEN/N01/476/30/PDF/N0147630.pdf (дата обращения: 16.11.2019).
10. Резолюция Генеральной Ассамблеи ООН от 30 декабря 2002 г. A/RES/57/53 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». URL: https:// documents-dds-y.un.org/doc/UNDOC/GEN/N02/541/47/ PDF/ N0254147. pdf (дата обращения: 16.11.2019).
11. Резолюция Генеральной Ассамблеи ООН от 8 декабря 2003 г. A/RES/58/32 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». URL: https:// documents-dds-ny. un.org/doc/UNDOC/GEN/N03/454/85/PDF/N0345485. pdf (дата обращения: 16.11.2019).
12. Резолюция от 2 декабря 2014 г. A/RES/69/28 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». URL: https://documentsdds-ny.un.org/doc/UNDOC/ GEN/N14/662/43/PDF/N1466243.pdf (дата обращения: 16.11.2019).
13. Резолюция от 3 декабря 2012 г. A/RES/67/27 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». URL: https://documentsdds-ny.un.org/doc/UNDOC/ GEN/N12/480/24/PDF/N1248024.pdf (дата обращения: 16.11.2019).
14. Резолюция ООН от 5 декабря 2018 г. A/RES/73/27 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». URL: https://www.un.org/ ga/search/view_ doc.asp? symbol=A/RES/73/27 (дата обращения: 16.11.2019).
15. Соглашение между правительствами государств — членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. 16 июня 2009 г. URL: http://docs.cntd.ru/document/902289626 (дата обращения: 16.11.2019).
16. Стрельцов А.Л., Крутских Л.В. Право в обеспечении международной информационной безопасности // Информация и звук: сайт. URL: http://www.zhenilo. narod.ru//main/ ips/2007_common_problems.pdf (дата обращения: 16.11.2019).

The Role of International Law in International Information Security

Nikolai Kostenko,
Doctor of Law, Professor, Distinguished Worker of Science and Education, Senior Researcher, Research Center of the Krasnodar Higher Military School named after Army General S.M. Stemenko of the Russian Ministry of Defense, member of the International Association of Scientists, Teachers and Professionals, member of the World Association of International Law
E-mail: prof_48kost@mail.ru

Abstract. *The aim of the study is to develop the main approaches to providing states with international information security. The role of the Russian Federation and other states in advances in information and telecommunications within the framework of international security is being investigated. Attention is drawn to the rapid formation and use of information and communication technologies, which have made up a large and lasting dependence of adverse government mechanisms on real cyber technologies and has been the reason new threats.*
The role of the Russian Federation in the purposeful work of shaping the United Nations doctrine on world information international security is being investigated. The UN General Assembly's Resolution A/RES/56/19, "Advances in Information and Telecommunications in the Context of International Security" adopted on 7 January 2002, endorsed the idea of researching current and possible threats to information security and drawing attention to the likely collective measures to eliminate them.
The Russian Federation's proposal for education, the composition of government experts, which could concentrate and discuss the most important stages that aim the subjects of international law to participate in the UN General Assembly Resolution of December 8, 2003 No. 58/32 "Achievements in the field of information and telecommunications in the context of international security" are analyzed.
The article draws particular attention to the document of the UN General Assembly A/55/140 which outlined five principles on international information security. The article examines in detail the resolutions of the United Nations General Assembly "Advances in Information and Telecommunications in the context of International Security" from December 4, 1998 to October 22, 2018 to ensure international information security.
The novelty of the study is the conclusions and proposals on problematic issues in the field of international information security, which would contribute to the adoption of a single international UN Convention, which would contain a conceptual apparatus, objectives, objectives, types of threats, priorities and mechanisms for their implementation, as well as provisions on the responsibility of States in the international information space.
Key words*: information, telecommunications, international, information, safety, threat, resolution, principles, standards, state.*

References

1. Draft document of the Russian Ministry of Foreign Affairs "General assessment of information security problems. Threats to international information security". URL: http://esa-conference.ru/wp-content/uploads/files/pdf/SHirin-Sergej-Sergeevich.pdf (Accessed: 16.11.2019).
2. Draft concept of the cybersecurity strategy of the Russian Federation. URL: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a 73.pdf (Accessed: 16.11.2019).
3. European Convention on Cybercrime (Crimes in Cyberspace), November 23, 2001. URL: http://mvd.gov.by/main.aspx?guid'4603 (Accessed: 16.11.2019).
4. General Assembly Resolution of November 29, 2001 A/RES/56/19. URL: https:// www.un.org/ga/search/view_ doc.asp?symbol/RES/56/19 (Accessed: 16.11.2019).
5. General Assembly Resolution of 29 November 2001 A/RES/56/19. URL: https:// www.un.org/ga/search/view_doc.asp?symbol=A/RES/56/19 (Accessed: 16.11.2019).
6. General Assembly Resolution of 7 January 2002 A/RES/56/19 "Advances in Information and Telecommunications in the Context of International Security". URL: https:// documents-dds-ny.un.org/doc/UNDOC/GEN/N01/476/30/PDF/N0147630.pdf (Accessed: 16.11.2019).
7. Maslakova E.A. To the issue of international cooperation in the field of information security / Maslakova E.A., Yilkin M.G., Kachalov V.V. // Herald of the Moscow Un-T of the Russian Interior Ministry. 2015. № 9. P. 75–77.
8. Resolution of December 2, 2014 A/RES/69/28 "Advances in Information and Telecommunications in the Context of International Security". URL: https://documentsdds-ny.un.org/doc/UNDOC/GEN/N14/662/43/ PDF/ N1466243.pdf (Accessed: 16.11.2019).

9. Resolution of December 3, 2012 A/RES/67/27 "Advances in Information and Telecommunications in the Context of International Security". URL: https://documentsdds-ny.un.org/doc/UNDOC/GEN/N12/ 480/24/PDF/ N1248024.pdf (Accessed: 16.11.2019).
10. Streltsov A.L., Krutsky L.V. Right in Providing International Information Security / Information and Sound: Site. URL: http://www.zhenilo.narod.ru//main/ ips/2007_common_problems.pdf (Accessed: 16.11.2019).
11. The agreement between the governments of the member states of the Shanghai Cooperation Organization for Cooperation in International Information Security. June 16, 2009. URL: http://docs.cntd.ru/document/902289626 (Accessed: 16.11.2019).
12. UN Resolution of 20 September 2000 A/RES/55/28 "Advances in Information and Telecommunications in the Context of International Security". URL: https://www. un.org/ga/search/view_doc.asp? symbol/RES/55/28.
13. UN General Assembly Resolution of December 30, 2002 A/RES/57/53 "Advances in information and telecommunications in the context of international security". URL: https:// documents-dds-y.un.org/doc/UNDOC/GEN/N02/541/47/ PDF/ N0254147.pdf (Accessed: 16.11.2019).
14. UN General Assembly Resolution of December 8, 2003 A/RES/58/32 "Advances in Information and Telecommunications in the Context of International Security". URL: https:// documents-dds-ny.un.org/doc/ UNDOC/GEN/N03/454/85/PDF/ N0345485.pdf (Accessed: 16.11.2019).
15. UN Secretary-General's Report on "Advances in Information and Telecommunications in the Context of International Security". URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/ N00/535/04/PDF/ N0053504.pdf (Accessed: 16.11.2019).
16. UN Resolution of December 5, 2018 A/RES/73/27 "Advances in information and telecommunications in the context of international security". URL: https://www.un.org/ ga/search/view_ doc.asp? symbol/RES/73/27 (Accessed: 16.11.2019).