Международные процессы, Том 19, № 4 (67), сс. 6–25
DOI 10.17994/IT.2021.19.4.67.4

ПОЛИТИКО-ПРАВОВЫЕ ПРЕДПОСЫЛКИ СИСТЕМЫ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РОССИЙСКИЕ ПОДХОДЫ И ИНИЦИАТИВЫ

СЕРГЕЙ БОЙКО
Аппарат Совета Безопасности Российской Федерации, Москва, Россия

Резюме

В фокусе статьи – государственная политика Российской Федерации в области международной информационной безопасности. Цель исследования состоит в определении основных направлений укрепления международного сотрудничества в сфере обеспечения информационной безопасности на различных уровнях международных отношений. Автор даёт оценку профильному двустороннему сотрудничеству на примере Соглашения между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности. Автором обобщаются российские инициативы, выдвигаемые в многосторонних институтах: особое внимание уделяется взаимодействию в рамках БРИКС, ШОС, ОДКБ и АСЕАН. Региональное и межрегиональное взаимодействие в данной сфере позволяет обеспечить стабильность и безопасность соответствующих регионов с учётом национальных интересов. В статье также рассматриваются российские проекты, продвигаемые на глобальном уровне, – резолюции Генеральной Ассамблеи ООН: благодаря России и её партнерам удалось закрепить свод международных правил, принципов и норм ответственного поведения государств в информационном пространстве. Помимо этого, ощутимым российским вкладом в институционализацию профильного дискуссионного механизма в ООН стал созыв новой Рабочей группы открытого состава – инклюзивной площадки для непрерывного и транспарентного диалога по проблематике международной информационной безопасности. Автор приходит к выводу, что реализация российских инициатив и достигнутые договорённости о сотрудничестве содействуют развитию политико-правовых основ системы обеспечения международной информационной безопасности. Нацеленность России на содействие формированию такой системы подтверждают обновлённые Основы государственной политики Российской Федерации в области международной информационной безопасности. Однако предпринимаемые Россией практические шаги в указанной области не являются достаточными, поскольку для формирования системы обеспечения международной информационной безопасности необходимы усилия всего мирового сообщества.

Ключевые слова:

международная информационная безопасность; внешняя политика Российской Федерации; государственная политика Российской Федерации; международное сотрудничество.

Дата поступления рукописи в редакцию: 15.01.2021
Дата принятия к публикации: 09.02.2022

Для связи с автором / Corresponding author:
Email: boiko_sm@gov.ru

DOI 10.17994/IT.2021.19.4.67.4

Стремительно нарастающие угрозы в информационной сфере требуют адекватного ответа со стороны государства, общества и граждан. Противостоять противоправному воздействию на информационную инфраструктуру со стороны государств, преследующих деструктивные военно-политические, террористические, экстремистские и криминальные цели, становится возможным только на основе комплексного подхода к выстраиванию системы обеспечения международной информационной безопасности (далее – МИБ) – системы, функционирующей на двустороннем, многостороннем, региональном и глобальном уровнях.

На содействие формированию такой системы нацелена государственная политика Российской Федерации в области МИБ, основы которой закреплены в 2021 году в профильном документе стратегического планирования – Основах государственной политики Российской Федерации в области международной информационной безопасности[1]. В обновлённой редакции понятие «система обеспечения МИБ» определяется как совокупность международных и национальных институтов, регулирующих деятельность в глобальном информационном пространстве в целях предотвращения (минимизации) угроз МИБ[2].

Проблемы создания системы обеспечения МИБ, подходы к выстраиванию международного сотрудничества с целью формирования соответствующих правовых механизмов и выработки практических мер рассматривались в работах ряда отечественных и зарубежных авторов.

Российские исследователи особое внимание традиционно уделяют политическим аспектам данной проблемы, среди которых перспективы формирования международной системы информационной безопасности сквозь призму инициатив России и США в ООН [Себекин, 2020]; формирование международных режимов информационной безопасности на различных уровнях [Зиновьева 2019, 2021]; состояние и возможности разработки политико-правовой базы сотрудничества в обеспечении МИБ [Крутских 2007, 2014]; применимость норм права международной ответственности к поведению государств в киберпространстве [Красиков 2018]; потенциальные направления российско-американского сотрудничества в области МИБ в условиях прогрессивного развития международного права и его адаптации к особенностям ИКТ-среды как новой сферы международного сотрудничества [Смирнов, Стрельцов 2017].

Зарубежные авторы, в свою очередь, делают больший акцент на правовой составляющей исследуемой проблематики. Они освещают вопросы ответственности государств за совершение международно-противоправных деяний в киберпространстве и выработки правил отнесения таких деяний к определённому государству [Antonopoulos 2015]; анализируют принципы ответственности государств и состояние выработки основных правил поведения в международном праве применительно к киберпространству [Jensen 2017]; оценивают как роль ООН в регулировании вопросов обеспечения кибербезопасности, так и необходимость дальнейших согласованных действий вообще [Henderson 2015]; рассматривают вопросы создания норм поведения государств в целях обеспечения стабильности в киберпространстве [Nye 2018, 2019]; исследуют правовой статус киберпространства и его суверенитета, а также потенциальные проблемы при разработке всеобъемлющего и согласованного на глобальном уровне договора, устанавливающего правила поведения, запрещающего отдельные виды деятельности и устанавливающего правила юрисдикции [Tsagourias 2016].

Анализ литературы по рассматриваемой проблематике свидетельствует о том, что исследования проблем формирования системы обеспечения МИБ, проводимые

[1] Основы государственной политики Российской Федерации в области международной информационной безопасности. URL: http://publication.pravo.gov.ru/Document/View/ 0001202104120050

[2] Там же.

представителями отечественных и зарубежных научных и экспертных сообществ, носят комплексный характер, подчёркивают необходимость сотрудничества заинтересованных сторон в целях противодействия всему спектру вызовов и угроз в информационной сфере.

При этом, если ранее приоритетное внимание уделялось так называемой триаде угроз (угрозам использования информационно-коммуникационных технологий (ИКТ) в деструктивных военно-политических целях, направленных на подрыв суверенитета государств, их территориальной целостности, в террористических и иных преступных целях), то в настоящее время российские и зарубежные авторы чаще исследуют «новые угрозы», нарастающие в последние годы и непосредственно влияющие на формирование системы обеспечения МИБ.

К таким, относительно новым, угрозам относят использование ИКТ для нанесения экономического ущерба, в том числе посредством деструктивного воздействия на объекты информационной инфраструктуры, а также для пропаганды экстремизма, терроризма и сепаратизма, вовлечения новых сторонников в ряды экстремистских и террористических организаций. Представители научного и экспертного сообществ отмечают нарастание угрозы использования ИКТ для вмешательства во внутренние дела государств, нарушения общественного порядка, разжигания межнациональной, межрасовой и межконфессиональной вражды, пропаганды расистских и ксенофобских идей и теорий, дестабилизации внутриполитической и социально-экономической обстановки, нарушения системы управления государством. Всё более серьёзной становится угроза распространения информации, наносящей вред общественно-политической и социально-экономической системе, духовно-нравственной и культурной среде государств.

Перечисленные угрозы МИБ подробно представлены в работах отечественных авторов, таких как Е.В. Батуева, В.А. Васенин, Е.С. Зиновьева, О.В. Казарин, В.Ю. Скиба, Р.А. Шаряпов, А.Я. Капустин, А.И. Смирнов, А.В. Крутских [Батуева 2014; Васенин 2004; Зиновьева 2019; Казарин, Скиба, Шаряпов 2016; Капустин 2015; 2017; Смирнов 2016; Крутских 2021]. Они также освещаются в публикациях зарубежных специалистов [Ambos 2015; Buchan 2018; Weimann 2015; Jensen, Watts 2017; Kastner, Megret 2015; Kerschischnig 2012; Lewis, Stewart 2013; Saul, Heath 2014; Hua, Bapna 2013]. Глобальный характер данных угроз и масштаб возможных последствий их реализации актуализирует необходимость формирования многоуровневой системы обеспечения МИБ.

Правовую основу каждого уровня упомянутой системы могут составить международные договоры о сотрудничестве в области обеспечения МИБ. Такие договоры позволяют не только зафиксировать единство подходов сотрудничающих сторон, но и гарантировать их взаимную безопасность от угроз в информационной сфере. Формат договоров может быть различным, что обусловлено особенностями правовых систем государств, достигающих договоренностей о сотрудничестве. Например, согласно Федеральному закону от 15 июля 1995 года № 101-ФЗ «О международных договорах Российской Федерации» международные договоры заключаются с иностранными государствами, международными организациями и иными образованиями от имени государства (межгосударственные договоры), от имени правительства (межправительственные договоры) и от имени органов власти или уполномоченных организаций (договоры межведомственного характера)[3]. Российское законодательство, равно как и законодательства других государств, предусматривает различные виды международных договоров: договоры, соглаше-

[3] Федеральный закон от 15 июля 1995 года № 101-ФЗ «О международных договорах Российской Федерации» (с дополнениями и изменениями). URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=370228&dst=1000000001%2C0#04556996730220404

ния, конвенции, протоколы, обмены письмами или нотами, а также иные виды и наименования международных договоров.

При достижении государствами с различными правовыми системами договорённостей о сотрудничестве в области обеспечения МИБ подобная вариативность позволяет находить взаимоприемлемые подходы к организационно-правовому оформлению сотрудничества. В целом международные договоры образуют многоуровневую правовую основу межгосударственных отношений в области обеспечения МИБ, которая содействует поддержанию мира, безопасности и стабильности в глобальном информационном пространстве, а также развитию международного сотрудничества в соответствии с целями и принципами Устава Организации Объединённых Наций.

Двустороннее сотрудничество как фундамент системы обеспечения МИБ

Правовую основу двустороннего уровня системы обеспечения МИБ составляют международные договоры, заключённые между двумя государствами. Подобные договоры позволяют наладить практическое взаимодействие заинтересованных сторон, поскольку чётко очерчивают основные направления сотрудничества.

Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности от 8 мая 2015 года[4], например, предусматривает создание механизма сотрудничества между уполномоченными органами в целях обмена информацией и совместного использования информации о существующих и потенциальных рисках, угрозах и уязвимостях в области информационной безопасности, их выявления, оценки, изучения, взаимного информирования о них, а также предупреждения их возникновения. Прикладной характер носят направления, связанные с совместным реагированием на угрозы в области обеспечения МИБ и созданием соответствующих каналов связи и контактов.

В практической плоскости лежит сотрудничество компетентных органов России и Китая в сфере обеспечения безопасности критической информационной инфраструктуры государств, обмена технологиями, а также взаимодействие уполномоченных органов в области реагирования на компьютерные инциденты. Большое значение для защиты от информационных угроз имеют обмен информацией и сотрудничество в правоохранительной области при расследовании дел, связанных с использованием ИКТ в террористических и криминальных целях.

Интересам формирования системы обеспечения МИБ на двустороннем уровне подчинены разработка и осуществление необходимых совместных мер доверия в рассматриваемой области, а также взаимодействие в разработке и продвижении норм международного права в целях обеспечения национальной и международной информационной безопасности. Кроме того, в числе основных направлений сотрудничества – содействие научным исследованиям, проведение совместных научно-исследовательских работ, подготовка специалистов, обмен студентами, аспирантами и преподавателями профильных высших учебных заведений. Наряду с решением поставленных задач большое значение придаётся сотрудничеству России и Китая и координации их деятельности в рамках международных организаций и форумов, а также проведению рабочих встреч, конференций, семинаров уполномоченных представителей и экспертов. Перечисленные направления российско-китайского сотрудничества во многом обеспечивают взаимодействие сторон в борьбе с угрозами МИБ.

Аналогичные межправительственные соглашения Россией заключены с Белорус-

[4] Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности от 8 мая 2015 г. URL: http://publication.pravo.gov.ru/Document/View/0001201608100001

сией, Бразилией, Вьетнамом, Индией, Индонезией, Ираном, Киргизией, Кубой, Никарагуа, Туркменистаном, Узбекистаном и ЮАР. Взаимные договорённости позволяют обеспечить эффективное системообразующее сотрудничество на двустороннем уровне. Наличие обязательств гарантирует, по меньшей мере, информационную безопасность от возможных деструктивных воздействий со стороны партнёра. Достижение всё большего числа двусторонних договорённостей способствует созданию разветвлённой паутины безопасности – фундамента для построения глобальной системы обеспечения МИБ.

В первую очередь межправительственные соглашения были подписаны Российской Федерацией со своими союзниками по СНГ, ШОС и БРИКС, с государствами, традиционно поддерживающими с Россией отношения стратегического партнёрства, а также со странами, разделяющими российские подходы к формированию системы обеспечения МИБ. Соглашения носят преимущественно рамочный характер, определяя основные направления сотрудничества сторон и фиксируя процедурные вопросы; практическое же взаимодействие строится на основе планов реализации указанных направлений. Круг государств, сотрудничающих с Россией в рассматриваемой области, не ограничивается упомянутыми странами. Более того, построение указанной системы только по блоковому признаку невозможно: необходимо взаимодействие на взаимовыгодной основе без политических пристрастий и блоковой принадлежности.

Именно такой подход России – государства, обладающего весомым потенциалом в области ИКТ и занимающего лидирующие позиции в мировой «табели о рангах», – обусловливает стремление многих государств выстраивать с ней прагматичные двусторонние отношения. Приоритеты для российских партнёров: обеспечение информационной безопасности, взаимодействие в наиболее чувствительных областях, связанных с защитой критической инфраструктуры, а также с противодействием использованию ИКТ в преступных целях. Наличие в отдельных случаях политических разногласий, различия в подходах не стали препятствием и для многих стран Запада, включая США, Францию, ФРГ, Нидерланды, Республику Корея, Японию, для налаживания профильного диалога с Россией. Проведение регулярных межведомственных консультаций способствует более полному пониманию и сближению позиций сторон, укреплению доверия и урегулированию потенциально опасных ситуаций.

Практическим результатом такого сотрудничества становится снижение числа компьютерных атак на информационные ресурсы взаимодействующих сторон, а также организация совместных усилий в борьбе с киберпреступниками.

Наглядным примером реализации указанных подходов стало Совместное заявление президентов Российской Федерации и Соединённых Штатов Америки о новой области сотрудничества в укреплении доверия от 17 июня 2013 года[5], которое дало старт взаимодействию профильных российских и американских ведомств. Кроме того, главы государств достигли договорённости о создании двусторонней рабочей группы по вопросам угроз в сфере использования ИКТ и самим ИКТ в контексте международной безопасности для проведения на регулярной основе консультаций по вопросам, представляющим взаимный интерес и вызывающим взаимную озабоченность.

Спустя восемь лет, в июне 2021 года, аналогичный процесс был запущен лидерами России и США в ходе встречи на высшем уровне в Женеве. Регулярный диалог экспертов по вопросам информационной безопасности в формате «Кремль–

[5] Совместное заявление президентов Российской Федерации и Соединённых Штатов Америки о новой области сотрудничества в укреплении доверия от 17 июня 2013 г. URL: http:// www.kremlin.ru/supplement/1479

Белый дом» позволил активизировать сотрудничество сторон в борьбе с преступным использованием ИКТ.

Таким образом, развитие двустороннего взаимодействия на прагматичной основе уже стало тенденцией в рассматриваемой области.

Многостороннее взаимодействие как выражение единства подходов и готовности к совместным действиям

Над двусторонним фундаментом располагается следующий уровень системы обеспечения МИБ – уровень многостороннего взаимодействия, скрепляющий узами сотрудничества несколько стран, объединённых общими подходами к противодействию угрозам в информационной сфере.

Примером такого взаимодействия является Шанхайская организация сотрудничества, в рамках которой заложены как политические, так и правовые основы сотрудничества в области обеспечения МИБ.

Первым шагом стало Заявление глав государств–членов Шанхайской организации сотрудничества по международной информационной безопасности от 15 июня 2006 года[6], в котором лидеры выразили озабоченность появлением реальной опасности использования ИКТ в целях, способных нанести серьёзный ущерб безопасности человека, общества и государства в нарушение основополагающих принципов равноправия и взаимного уважения, невмешательства во внутренние дела суверенных государств, мирного урегулирования конфликтов, неприменения силы, соблюдения прав человека. Также обращалось внимание на то, что угрозы использования ИКТ в преступных, террористических и военно-политических целях, не совместимых с обеспечением международной безопасности, могут реализовываться как в гражданской, так и в военной сфере и привести к тяжёлым политическим и социально-экономическим последствиям в отдельных странах, регионах и в мире в целом, к дестабилизации общественной жизни государств. В связи с этим главами государств–членов ШОС было достигнуто решение о принятии скоординированных и взаимодополняющих мер для адекватного ответа современным вызовам и угрозам безопасности в информационной сфере.

Ключевым стало решение о создании профильной группы экспертов для выработки плана действий по обеспечению МИБ и определению возможных путей и средств решения в рамках ШОС актуальных проблем в рассматриваемой области. Начиная с 2006 г. данная экспертная группа активно включилась в формирование политико-правовой основы сотрудничества государств Организации в многостороннем формате. Результатом трёхлетней деятельности экспертов стал проект профильного межправительственного соглашения о сотрудничестве, подписанного 16 июня 2009 г. в Екатеринбурге.

Соглашение между правительствами государств–членов ШОС о сотрудничестве в области обеспечения МИБ[7] стало первым в мировой практике многосторонним соглашением в упомянутой области. Подписание Соглашения подтвердило возможность достижения договорённостей о сотрудничестве стран, имеющих значительные различия в национальных законодательствах и используемой терминологии. Данные отличия тем не менее не стали препятствием на пути к подписанию документа, поскольку подходы к обеспечению национальной безопасности в информационной сфере, а также к формированию системы обеспечения МИБ основывались на принципах, единых для стран-подписантов.

Сотрудничество в ШОС отличают предметный характер и практическая ориенти-

[6] Заявление глав государств–членов Шанхайской организации сотрудничества по международной информационной безопасности от 15 июня 2006 г. URL: http://www.infoshos.ru/ru/?id=94

[7] Соглашение между правительствами государств–членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности от 16 июня 2009 г. URL: https://base.garant.ru/2571379/

рованность. Государства ставят целями определение, согласование и осуществление совместных мер в области обеспечения МИБ, создание системы мониторинга и совместного реагирования на возникающие угрозы, обеспечение информационной безопасности критически важных структур, а также противодействие угрозам использования ИКТ в террористических целях и информационной преступности. Соглашением предусматриваются обмен опытом, подготовка специалистов, проведение рабочих встреч, конференций, семинаров и форумов уполномоченных представителей и экспертов в области информационной безопасности.

В целях сближения подходов сторон к унификации профильных национальных законодательств в качестве одного из направлений сотрудничества указан обмен информацией о законодательном регулировании. Взаимодействие по правовым вопросам подразумевает совершенствование международно-правовой базы и практических механизмов сотрудничества в обеспечении МИБ. На данном направлении конкретной задачей стала выработка совместных мер по развитию норм международного права в области ограничения распространения и применения информационного оружия, создающего угрозы обороноспособности, национальной и общественной безопасности. Также большое значение придаётся содействию обеспечению безопасного, стабильного функционирования и интернационализации управления глобальной сетью Интернет.

Координация действий сторон в рассматриваемой области вот уже на протяжении более 12 лет остаётся прерогативой профильной группы экспертов государств–членов Шанхайской организации сотрудничества. Результатом её работы стали согласованные действия членов Организации на различных международных площадках, прежде всего в Организации Объединённых Наций, свидетельством чего служит резолюция A/RES/73/27 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», принятая 5 декабря 2018 г. 73-й сессией Генеральной Ассамблеи ООН[8]. В данном документе был очерчен свод международных правил, норм и принципов ответственного поведения государств, которые ранее были закреплены в докладах групп правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности от 2013[9] и 2015[10] годов.

Основу данных правил, норм и принципов составили не только результаты исследований профильных групп правительственных экспертов ООН, но и «Правила поведения в области обеспечения международной информационной безопасности», внесённые государствами–членами ШОС 12 сентября 2011 г. и 9 января 2015 г. в качестве официальных документов соответственно 66-й (A/66/359)[11] и 69-й (A/69/723)[12] сессий Генеральной Ассамблеи ООН.

Вклад ШОС справедливо подчёркивался в обоих упомянутых докладах. В 2013 г. Группа отметила документ A/66/359, рас-

[8] Резолюция A/RES/73/27 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». Принята Генеральной Ассамблеей ООН 5 декабря 2018 г. URL: https://undocs.org/ru/A/RES/73/27

[9] Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности 2013 г. URL: https://undocs.org/pdf?symbol=ru/A/68/98

[10] Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности 2015 г. URL: https://undocs.org/ru/A/70/174

[11] Правила поведения в области обеспечения международной информационной безопасности. URL: https://undocs.org/ru/A/66/359

[12] Правила поведения в области обеспечения международной информационной безопасности. URL: http://undocs.org/ru/A/69/723

пространённый Генеральным секретарем ООН по просьбе постоянных представителей Китая, Российской Федерации, Таджикистана и Узбекистана и содержащий проект правил поведения в области обеспечения МИБ, к числу авторов которого впоследствии присоединились Казахстан и Кыргызстан[13]. В 2015 г. Группа приняла к сведению Правила поведения в области обеспечения международной информационной безопасности, предложенные Казахстаном, Китаем, Кыргызстаном, Российской Федерацией, Таджикистаном и Узбекистаном[14].

Общность подходов стран ШОС к обеспечению МИБ и готовность к консолидации усилий по противодействию угрозам в информационной сфере в очередной раз подтвердило заявление Совета глав государств-членов о сотрудничестве в области обеспечения международной информационной безопасности от 10 ноября 2020 года[15]. В документе чётко обозначена нацеленность государств Организации на совершенствование механизма и мер по предотвращению межгосударственных конфликтов и преодоление дефицита доверия между государствами, который может возникать вследствие противоправного использования ИКТ.

Ключевым посылом заявления лидеров стал обращённый к международному сообществу призыв к тесному взаимодействию, в том числе по предотвращению конфликтов, возникающих в результате применения ИКТ, обеспечению их использования в интересах социального и экономического развития и повышения благосостояния народов. Основная цель – формирование общего будущего в информационном пространстве на основе международного сотрудничества в области обеспечения информационной безопасности путём активизации усилий на национальном, двустороннем и многостороннем уровнях.

Политическая воля глав государств–членов ШОС к созданию правовой основы системы обеспечения МИБ выражается в нацеленности на выработку правил, норм и принципов ответственного поведения государств в информационном пространстве, разработку под эгидой ООН универсальных юридически обязывающих инструментов, совершенствование управления Интернетом, обеспечение равных прав государств и повышения роли Международного союза электросвязи в данном контексте.

Достигнутые в рамках ШОС договорённости помогли наладить эффективное взаимодействие в области обеспечения информационной безопасности, позволяя значительно сократить число компьютерных атак на критическую информационную инфраструктуру государств–членов Организации, а также укрепить их национальную безопасность в информационной сфере.

В многостороннем формате развивается сотрудничество государств–участников БРИКС. Создана Рабочая группа экспертов по вопросам безопасности в сфере использования ИКТ, координирующая действия сторон в указанной области и содействующая расширению сотрудничества в рамках «пятёрки», в том числе посредством рассмотрения соответствующих инициатив и реализации Дорожной карты практического сотрудничества стран БРИКС в обеспечении безопасности в сфере использования ИКТ.

[13] Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности 2013 г. URL: https://www.un.org/disarmament/ru/достижения-в-сфере-информатизации-и-т/

[14] Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности 2015 г. URL: https://www.un.org/disarmament/ru/достижения-в-сфере-информатизации-и-т/

[15] Заявление Совета глав государств–членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности от 10 ноября 2020 г. URL: http://ru.china-embassy.org/rus/zgxw/t1831178.htm

В Московской декларации XII саммита БРИКС от 17 ноября 2020 г.[16] в контексте формирования системы обеспечения МИБ подчёркивается ведущая роль ООН в развитии диалога по достижению общего понимания безопасности ИКТ и их использования, а также разработка под эгидой Организации общепризнанных норм, правил и принципов ответственного поведения государств в сфере ИКТ.

Нацеленность лидеров Бразилии, России, Индии, Китая и ЮАР на многостороннее сотрудничество выражается в работе по рассмотрению и подготовке предложений о разработке межправительственного соглашения БРИКС о сотрудничестве в области обеспечения безопасности в сфере использования ИКТ и двусторонних соглашений между странами объединения.

Многостороннее взаимодействие, таким образом, позволяет гармонизировать национальные подходы сотрудничающих государств и способствовать укреплению системы обеспечения МИБ.

Региональное сотрудничество во имя достижения общих целей обеспечения МИБ

Третий уровень системы обеспечения МИБ представлен региональными объединениями, к которым относятся, например, Организация Договора о коллективной безопасности (ОДКБ) и Содружество Независимых Государств (СНГ), действующие на постсоветском пространстве.

Правовую основу взаимодействия на данном уровне составляют профильные соглашения о сотрудничестве; при этом такое сотрудничество, как правило, является наиболее практико-ориентированным и реализуется по многочисленным направлениям, предполагающим активное взаимодействие сторон.

Например, Соглашение о сотрудничестве государств–членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности от 30 ноября 2017 г.[17] предусматривает развитие региональной системы информационной безопасности на основе межгосударственного сотрудничества и укрепления межведомственного взаимодействия. Во главу угла ставится совершенствование механизмов противодействия угрозам в информационной сфере, проведение совместных мероприятий, направленных на укрепление информационной безопасности и противодействие противоправной деятельности в информационном пространстве государств-членов, взаимная помощь в целях развития технологической основы обеспечения информационной безопасности государств Организации, выявление, предупреждение и нейтрализация угроз информационной безопасности. Приоритетными задачами стали планирование и проведение скоординированных мероприятий по обеспечению информационной безопасности, взаимодействие в вопросах защиты критически важных структур, а также противодействие деструктивному информационному воздействию, противоправной деятельности в информационном пространстве, созданию и распространению вредоносного программного обеспечения, выработка критериев определения информационных ресурсов, используемых в противоправных целях, их выявление и блокировка.

Приоритетное значение придаётся предотвращению использования третьей стороной территории и/или информационной инфраструктуры, находящейся под юрисдикцией государства–члена ОДКБ, для оказания деструктивного информационного воздействия, в том числе компьютерных атак, на другое государство Организации. В связи с этим на передний план выступает определение источника компьютерных атак, проведённых с их территории, проти-

[16] Московская декларация XII саммита БРИКС от 17 ноября 2020 г. URL: http://www.kremlin.ru/supplement/5581.

[17] Соглашение о сотрудничестве государств–членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности от 30 ноября 2017 г. URL: http://docs.cntd.ru/document/542645728

водействие этим атакам и ликвидация их последствий.

Обязательным условием обеспечения скоординированных действий сторон стала подготовка кадров в области обеспечения информационной безопасности, выделенная в самостоятельное направление сотрудничества в рамках объединения.

В связи с тем что члены ОДКБ осознают необходимость встраивания региональной компоненты в формирующуюся глобальную систему, государства нацелены на выработку согласованной позиции в вопросах обеспечения МИБ, а также на участие в продвижении этой позиции на международной арене.

Такой перечень практико-ориентированных направлений сотрудничества позволяет сделать вывод о том, что региональная составляющая многоуровневой системы обеспечения МИБ играет важную роль в её стабильном и устойчивом функционировании. Вместе с тем в интересах дальнейшего развития глобальной системы обеспечения МИБ требуется не только устойчивое функционирование вышеперечисленных уровней взаимодействия, но и развитие интеграционных процессов, позволяющих объединить усилия различных региональных объединений или наладить их сотрудничество с отдельными ведущими государствами (группами государств), являющимися лидерами в сфере информационной безопасности.

Основой для такого взаимодействия, как правило, становятся политические заявления на высшем уровне, а также другие форматы волеизъявления заинтересованных сторон. Например, 14 ноября 2018 г. было принято Заявление Российской Федерации и АСЕАН о сотрудничестве в области обеспечения безопасности использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий[18], давшее старт консолидации усилий заинтересованных сторон.

Заявление подтвердило близость подходов России и стран АСЕАН к формированию системы обеспечения МИБ, отмечая, что сотрудничество и координация усилий государств на двустороннем, региональном и международном уровнях являются императивом для своевременного и эффективного реагирования на угрозы и вызовы, связанные с использованием ИКТ с учётом их трансграничной природы. При этом в тексте документа подчёркивается практический характер сотрудничества России и стран–членов АСЕАН, важность активизации усилий по сокращению цифрового разрыва, значимость мер по наращиванию национальных потенциалов, запуску образовательных программ и тренингов по вопросам безопасности в сфере использования ИКТ и самих ИКТ. Особое внимание уделяется укреплению практического сотрудничества на таких направлениях, как борьба с использованием ИКТ в террористических целях и для иной преступной деятельности.

Согласие принявших Заявление сторон содействовать укреплению и оптимизации существующих региональных механизмов по безопасности в сфере использования ИКТ и самих ИКТ, а также поддержка российской инициативы об учреждении профильного диалога Россия–АСЕАН свидетельствуют о нацеленности государств объединения на формирование во взаимодействии с Россией качественно нового регионального уровня системы обеспечения МИБ.

Важным дополнением такого взаимодействия стало развитие двусторонних отношений между Россией и странами АСЕАН, создание необходимой правовой базы сотрудничества в области обеспечения безопасности в сфере использования ИКТ. В 2018 г. было подписано профильное российско-вьетнамское межправительственное соглашение о сотрудничестве[19], в 2021 г. – аналогичное соглашение с Индо-

[18] Заявление Российской Федерации и АСЕАН о сотрудничестве в области обеспечения безопасности использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий от 14 ноября 2018 г. URL: http://www.kremlin.ru/supplement/5361

[19] Соглашение между Правительством Российской Федерации и Правительством Социалистической Республики Вьетнам о сотрудничестве в области обеспечения международной информационной безопасности от 6 сентября 2018 г. URL: http://docs.cntd.ru/document/554398783.

незией[20]. Активно развивается конструктивный диалог в рассматриваемой области с Сингапуром и Малайзией. Нацеленность на двустороннее сотрудничество с Россией подтвердили Таиланд и Камбоджа.

Подобное региональное взаимодействие, а также достижение внутри- и межрегиональных договорённостей, в том числе и в двустороннем формате, позволяют укреплять региональный уровень системы обеспечения МИБ – гаранта стабильности и безопасности в информационной сфере всех заинтересованных сторон.

Развитие нормативных правовых и политических основ сотрудничества на вышеперечисленных уровнях не может стать стопроцентным барьером угрозам в информационной сфере. Тем не менее такое сотрудничество и политическое волеизъявление значительно снижает количество новых вызовов и угроз и, самое главное, масштабы их последствий.

Глобальный уровень системы обеспечения МИБ

Вершиной пирамиды системы обеспечения МИБ является глобальный уровень – взаимодействие государств на основе принятых под эгидой ООН международно-правовых актов, регулирующих деятельность в информационном пространстве.

Первым шагом на пути создания политико-правовой основы на данном уровне стало принятие 5 декабря 2018 г. 73-й сессией Генеральной Ассамблеи ООН российского проекта резолюции A/RES/73/27 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», впервые закрепившей свод из 13 международных правил, норм и принципов ответственного поведения государств[21].

Одновременно с этой резолюцией для придания переговорному процессу по безопасности в сфере использования ИКТ более демократического, инклюзивного и транспарентного характера в 2019 г. была создана рабочая группа открытого состава, приоритетной задачей которой стала дальнейшая выработка упомянутых норм, правил и принципов ответственного поведения государств.

Поддержанная большинством государств–членов ООН резолюция дала старт регулярному институциональному диалогу с широким кругом участников под эгидой Организации, ставшему качественно новым форматом экспертного обсуждения ключевых проблем в области обеспечения МИБ всеми заинтересованными сторонами, включая деловые круги, неправительственные организации и научное сообщество.

31 декабря 2020 г. на 75-й сессии Генеральной Ассамблеи ООН по инициативе России большинством голосов была принята резолюция A/RES/75/240 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»[22], которая предусматривала созыв на период 2021–2025 годов новой рабочей группы открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ. Таким образом, в ООН сохранились непрерывность и преемственность демократического, инклюзивного и транспарентного переговорного процесса по безопасности.

[20] Распоряжение Правительства Российской Федерации от 28 декабря 2018 г. № 2984-р «О подписании Соглашения между Правительством Российской Федерации и Правительством Республики Индонезии о сотрудничестве в области обеспечения международной информационной безопасности». URL: http:/docs.cntd.ru/document/552051443; Россия и Индонезия заключили межправительственное соглашение о сотрудничестве в области обеспечения международной информационной безопасности. 14 декабря 2021 г. URL: http://www.scrf.gov.ru/news/allnews/3151/.

[21] Резолюция A/RES/73/27 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». URL: https://www.un.org/disarmament/ru/достижения-в-сфере-информатизации-и-т/.

[22] Резолюция A/RES/75/240 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». Принята Генеральной Ассамблеей ООН 31 декабря 2020 г. URL: https://undocs.org/ru/A/RES/75/240

Новая рабочая группа открытого состава, заработавшая в июне 2021 года, продолжит дальнейшую выработку норм, правил и принципов ответственного поведения государств и путей их имплементации, а также, при необходимости, внесение в них изменений или формулирование дополнительных правил.

Впервые площадка Группы будет использована для рассмотрения инициатив, направленных на обеспечение безопасности в сфере использования ИКТ, что позволит всесторонне обсуждать проблемы в указанной области и искать пути их решения, в том числе возможные совместные меры по предотвращению существующих и потенциальных угроз в сфере информационной безопасности и противодействию им.

Несмотря на то что доклады Рабочей группы открытого состава, равно как и доклады Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (2010, 2013, 2015 годов), носят рекомендательный характер, изложенные в них положения в перспективе могут стать основой для подготовки под эгидой ООН профильных правовых актов, регулирующих отношения в области обеспечения МИБ.

В числе потенциальных основных регулятивных актов – Конвенция ООН об обеспечении международной информационной безопасности, концепцию которой Россия представила в сентябре 2011 г. на международной встрече высоких представителей, курирующих вопросы безопасности[23]. Данный документ по замыслу его разработчиков мог стать основой для базового многостороннего договора с участием всех государств–членов ООН, открытым для участия международного сообщества в целом и нацеленным на достижение провозглашённой 8 сентября 2000 г. в Декларации тысячелетия ООН[24] необходимости укрепления международного правопорядка, в том числе в информационной сфере.

В 2011 г. была обозначена цель данной конвенции – противодействие использованию ИКТ для нарушения международного мира и безопасности, а также установление мер, способствующих тому, чтобы деятельность государств в информационном пространстве: 1) способствовала общему социальному и экономическому развитию; 2) осуществлялась таким образом, чтобы быть совместимой с задачами поддержания международного мира и безопасности; 3) соответствовала общепризнанным принципам и нормам международного права, включая принципы мирного урегулирования споров и конфликтов, неприменения силы, невмешательства во внутренние дела, уважения прав и основных свобод человека; 4) была совместимой с правом каждого искать, получать и распространять информацию и идеи, как это зафиксировано в документах ООН, с учётом того, что такое право может быть ограничено законодательством для защиты интересов национальной и общественной безопасности каждого государства, а также для предотвращения неправомерного использования информационных ресурсов; 5) гарантировала свободу технологического обмена и свободу обмена информацией с учётом уважения суверенитета государств и их политических, исторических и культурных особенностей[25].

За десятилетний период, прошедший со дня первого представления концепции, изменилась оценка современного состояния информационного пространства, существующих и потенциальных угроз МИБ,

[23] Конвенция ООН об обеспечении международной информационной безопасности (концепция). URL: http://www.scrf.gov.ru/security/information/document112/.

[24] Декларация тысячелетия Организации Объединённых Наций. Принята резолюцией 55/2 Генеральной Ассамблеи ООН от 8 сентября 2000 г. URL: https://www.un.org/ru/documents/ decl_conv/declarations/summitdecl.shtml.

[25] Конвенция ООН об обеспечении международной информационной безопасности (концепция). URL: http://www.scrf.gov.ru/security/information/document112/

а также возможных мер противодействия этим угрозам. Эти изменения нашли своё отражение в обновлённой редакции упомянутой концепции Конвенции ООН, представленной в июле 2021 г.[26]

В качестве главной цели документа обозначено содействие формированию системы обеспечения МИБ, позволяющей противодействовать угрозам международному миру, безопасности и стабильности в информационной сфере. Предусматривается, что данная система должна способствовать: а) равноправному стратегическому партнёрству в глобальном информационном пространстве на основе суверенного равенства государств; б) общему социальному и экономическому развитию на основе равноправного и безопасного доступа всех государств к достижениям современных ИКТ; в) реализации общепризнанных принципов и норм международного права, включая принципы мирного урегулирования споров и конфликтов, неприменения силы, невмешательства во внутренние дела, уважения прав и основных свобод человека; г) реализации права каждого искать, получать и распространять всякого рода информацию и идеи с учётом того, что такое право может быть сопряжено с ограничениями, установленными законом и являющимися необходимыми для уважения прав и репутации других лиц, а также для охраны государственной безопасности, общественного порядка, здоровья или нравственности населения; д) свободному технологическому обмену и свободному обмену информацией с учётом уважения суверенитета государств и их существующих политических, правовых, исторических и культурных особенностей[27].

Несмотря на актуализацию содержания документа, принципиальные подходы к формированию системы обеспечения МИБ, заложенные в 2011 году, остались неизменными.

При этом российская инициатива о разработке упомянутой Конвенции не нашла поддержки у стран Запада, отдающих предпочтение необязательности исполнения правил и норм ответственного поведения государств. Подобная позиция просматривается и в работах ряда зарубежных учёных. В частности, Дж.С. Най отмечает, что «обязательный международно-правовой договор был бы преждевременным в качестве следующего шага. Нормы ожидаемого поведения могут обеспечить гибкую золотую середину между жёсткими договорами и отсутствием каких-либо действий вообще» [Nye 2017].

Тем не менее есть и другие учёные, с одной стороны, подтверждающие трудности, с которыми в настоящее время Россия сталкивается при продвижении своей инициативы, а с другой – дающие оценку необходимости достижения всеобъемлющих договорённостей.

По мнению Н. Цагориаса, «киберпространство – это область, которая предлагает возможности, но также содержит риски и опасности; это система регулирования, основанная на общих ценностях, принципах и правилах поведения, что необходимо для укрепления сотрудничества <...> в киберпространстве. Для этого может потребоваться всеобъемлющий и согласованный на глобальном уровне договор, устанавливающий правила юрисдикции и поведения. Однако достижение соглашения о всеобъемлющей правовой базе для киберпространства сопряжено с огромными проблемами». Учёный утверждает, что «перспективы такого всеобъемлющего режима не являются благоприятными». При этом делает вывод, что «международное право определяет поведение и интересы государств в киберпространстве и, возможно, рационализирует их...» [Tsagourias 2016].

Российская инициатива о принятии под эгидой ООН Конвенции об обеспечении международной информационной безо-

[26] Концепция Конвенции ООН об обеспечении международной информационной безопасности (2021 г.). URL: http://www.scrf.gov.ru/security/information/document112/

[27] Там же.

пасности является не единственной на глобальном уровне. Стремительный рост противоправного использования ИКТ актуализировал потребность в борьбе с этой проблемой. Правовой основой для консолидации усилий мирового сообщества под эгидой ООН, по мнению России, может стать всеобъемлющая международная конвенция о противодействии использованию информационно-коммуникационных технологий в преступных целях.

Для разработки данной конвенции согласно резолюции Генеральной Ассамблеи ООН от 27 декабря 2019 г. A/RES/74/247 «Противодействие использованию информационно-коммуникационных технологий в преступных целях»[28] в ООН учреждён специальный межправительственный комитет экспертов открытого состава, представляющий все регионы мира.

При подготовке конвенции планируется в полной мере учесть существующие международные правовые документы и предпринимаемые на национальном, региональном и международном уровнях усилия по борьбе с использованием ИКТ в преступных целях, а также итоги работы Межправительственной группы экспертов открытого состава для проведения всестороннего исследования проблемы киберпреступности[29].

Базовым документом в этой работе может стать инициативный российский проект Конвенции ООН о сотрудничестве в сфере противодействия информационной преступности, распространённый в октябре 2017 г. в ООН в качестве документа 72-й сессии Генассамблеи[30] (по пункту 107 повестки дня «Предупреждение преступности и уголовное правосудие»).

Данный проект, учитывающий современные реалии и основывающийся на принципах суверенного равенства сторон и невмешательства во внутренние дела других государств, стал результатом многолетней работы экспертов по созданию универсального всеобъемлющего документа, нацеленного на противодействие преступлениям в сфере использования ИКТ.

Несомненным достоинством документа стало использование его разработчиками опыта подобных международно-правовых актов. В их числе Конвенция ООН против коррупции от 31 октября 2003 г.[31], Конвенция ООН против транснациональной организованной преступности от 15 ноября 2000 г.[32], Конвенция Совета Европы о преступности в сфере компьютерной информации (ETS № 185) от 23 ноября 2001 г. (так называемая Будапештская конвенция о киберпреступности)[33], а также универсальные антитеррористические конвенции ООН.

Актуализированный проект Конвенции ООН о противодействии использованию

[28] Резолюция A/RES/74/247 «Противодействие использованию информационно-коммуникационных технологий в преступных целях». Принята Генеральной Ассамблеей ООН 27 декабря 2019 г. URL: https://undocs.org/ru/A/RES/74/247

[29] Всестороннее исследование проблемы киберпреступности (проект, февраль 2013 г.). URL: https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Russian.pdf

[30] Проект Конвенции Организации Объединённых Наций о сотрудничестве в сфере противодействия информационной преступности // Письмо Постоянного представителя Российской Федерации при Организации Объединённых Наций от 11 октября 2017 г. на имя Генерального секретаря. A/C.3/72/12 от 16 октября 2017 г. URL: http://www.mid.ru/documents/10180/3024875/Проект+конвенции+по+преступности+с+правками+секр+ООН.pdf/c93e68c9-9994-4769-951d-057c4881b8fd

[31] Конвенция Организации Объединённых Наций против коррупции. Принята резолюцией 58/4 Генеральной Ассамблеи ООН от 31 октября 2003 г. URL: http://www.un.org/ru/ documents/decl_conv/conventions/corruption.shtml

[32] Конвенция Организации Объединённых Наций против транснациональной организованной преступности. Принята резолюцией 55/25 Генеральной Ассамблеи ООН от 15 ноября 2000 г. URL: http://www.un.org/ru/documents/decl_conv/conventions/orgcrime

[33] Конвенция о преступности в сфере компьютерной информации (ETS N 185) (Будапешт, 23 ноября 2001 г.). URL: http://base.garant.ru/4089723/

ИКТ в преступных целях[34] был внесён Россией в июле 2021 г. в специальный межправительственный комитет. Разработку итогового проекта планируется завершить в 2023–2024 годах в ходе 78-й сессии Генеральной Ассамблеи ООН.

Ещё одним важным шагом к формированию на глобальном уровне системы обеспечения МИБ может стать принятие конвенционального документа ООН в области обеспечения безопасности сети Интернет. За основу такого документа может быть взята представленная в апреле 2017 г. российская концепция конвенции (концепция безопасного функционирования и развития сети Интернет)[35].

Ключевыми идеями концепции являются содействие дальнейшему развитию Интернета, повышению его безопасности и обеспечению гарантий прав и свобод пользователей, а также установление режима равноправного международного сотрудничества в управлении сетью, повышение его эффективности и действенности.

Реализация инициативы России даст возможность каждому государству защищать свой национальный сегмент глобальной сети, включая критическую информационную инфраструктуру, а также гарантировать соблюдение прав и свобод пользователей и защиту граждан в Интернете. Кроме того, исключается возможность создавать помехи для функционирования сети Интернет и манипулировать доступом в сеть для влияния на другие суверенные государства.

В своей основе концепция опирается на Тунисскую программу для информационного общества от 15 декабря 2005 г.[36] и Итоговый документ совещания высокого уровня Генеральной Ассамблеи, представляющий собой обзор хода осуществления решений Всемирной встречи на высшем уровне по вопросам информационного общества от 16 декабря 2015 г.[37] В российской концепции отражён ключевой лейтмотив данных базовых документов: каждое государство имеет суверенное право самостоятельно решать вопросы государственной политики в Интернете.

Такой подход имеет как сторонников, так и оппонентов, расценивающих инициативу России как попытку контроля глобальной информационной сети, ущемления прав её пользователей. В связи с этим уместно напомнить положения ст. 19 Международного пакта о гражданских и политических правах 1966 г.: «Каждый человек имеет право на свободное выражение своего мнения; это право включает свободу искать, получать и распространять всякого рода информацию и идеи, независимо от государственных границ. Пользование <...> правами налагает особые обязанности и особую ответственность. Это может быть, следовательно, сопряжено с некоторыми ограничениями, которые, однако, должны быть установлены законом и являться необходимыми для уважения прав и репутации других лиц, для охраны государственной безопасности, общественного порядка, здоровья или нравственности населения»[38].

[34] Конвенция Организации Объединённых Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях (проект). URL: https://www. kommersant.ru/docs/2021/RF_28_July_2021_-_R.pdf

[35] Минкомсвязь представляет проект новой концепции конвенции ООН. URL: http://minsvyaz.ru/ru/events/36739/

[36] Тунисская программа для информационного общества. Документ WSIS-05/TUNIS/DOC/6(Rev.1)-R от 15 ноября 2005 г. URL: http://www.un.org/ru/events/pastevents/pdf/agenda_wsis.pdf

[37] Итоговый документ совещания высокого уровня Генеральной Ассамблеи, посвящённого общему обзору хода осуществления решений Всемирной встречи на высшем уровне по вопросам информационного общества. Принят резолюцией A/70/125 Генеральной Ассамблеи ООН от 16 декабря 2015 г. URL: http://workspace.unpan.org/sites/Internet/Documents/UNPAN96090.pdf

[38] Международный пакт о гражданских и политических правах. Принят резолюцией 2200 A (XXI) Генеральной Ассамблеи ООН от 16 декабря 1966 г. URL: https:// www.un.org/ru/documents/decl_conv/conventions/pactpol.shtml

* * *

Формирование системы обеспечения МИБ на всех рассмотренных уровнях – сложный и многогранный процесс, в который должны быть вовлечены государства, негосударственные субъекты, научное и экспертное сообщество, деловые круги и простые граждане. Ответственность за безопасность в информационной сфере, защиту от новых вызовов и угроз тем не менее лежит на государствах. От их активности на данном направлении зависит будущее мирового сообщества, социально-политическая стабильность и благополучие населения.

Понимание сложности данных процессов, масштабов возможных последствий деструктивной деятельности в информационном пространстве предопределило содержание российских подходов и инициатив, направленных на содействие формированию системы обеспечения МИБ на всех уровнях – от двустороннего до глобального.

Приведённый перечень инициатив России, нацеленных на построение системы обеспечения МИБ, не является исчерпывающим и достаточным для решения данной глобальной задачи. На этом пути потребуется преодолеть множество разногласий, сблизить подходы к ключевым проблемам, укрепить взаимопонимание и доверие в рассматриваемой области, наладить на различных уровнях и в различных форматах взаимодействие в интересах обеспечения МИБ и, наконец, достичь договорённостей о сотрудничестве, чтобы консолидировать усилия мирового сообщества в противодействии стремительно нарастающим вызовам и угрозам в информационной сфере.

В контексте поиска стратегических решений перечисленных проблем рассмотренные в статье российские подходы и инициативы могут служить ориентиром для создания необходимых политико-правовых основ формирования системы обеспечения МИБ – гаранта стабильности и равноправного стратегического партнёрства в глобальном информационном пространстве.

Список литературы

Батуева Е.В. Американская концепция угроз информационной безопасности и её международно-политическая составляющая: Дис. … канд. полит. наук. М., 2014. 207 с.

Васенин В.А. Информационная безопасность и компьютерный терроризм // Научные и методологические проблемы информационной безопасности / Под ред. В.П. Шерстюка. М.: МЦНМО, 2004. С. 67–83.

Зиновьева Е.С. Международная информационная безопасность: проблемы двустороннего и многостороннего сотрудничества. М.: МГИМО МИД России, 2021. 250 с.

Зиновьева Е.С. Международное сотрудничество по обеспечению информационной безопасности: субъекты и тенденции эволюции: Дис. … канд. полит. наук. М., 2019. 362 с.

Казарин О.В., Скиба В.Ю., Шаряпов Р.А. Новые разновидности угроз международной информационной безопасности // История и архивы. 2016. № 1. С. 54–72.

Капустин А.Я. К вопросу о международно-правовой концепции угроз международной информационной безопасности // Журнал зарубежного законодательства и сравнительного правоведения. 2017. № 6. С. 44–51.

Капустин А.Я. Угрозы международной информационной безопасности: формирование концептуальных подходов // Журнал российского права. 2015. № 8. С. 89–100.

Красиков Д.В. Международно-правовая ответственность государств в киберпространстве // Государство и право в новой информационной реальности: Сб. науч. трудов ИНИОН РАН / Отв. ред. Е.В. Алфёрова, Д.А. Ловцов. М., 2018. С. 235–247.

Красиков Д.В. Территориальный суверенитет и делимитация юрисдикций в киберпространстве // Государство и право в новой информационной реальности / Отв. ред. Е.В. Алфёрова, Д.А. Ловцов. М., 2018. С. 99–111.

Крутских А.В., Бирюков А.В. Новая геополитика международных научно-технологических отношений // Международные процессы. 2017. Т. 15. № 2 (49). С. 6–26.

Крутских А.В. К политико-правовым основаниям глобальной информационной безопасности // Международные процессы. 2007. Т. 5. № 1 (13). С. 28–37.

Международная информационная безопасность: Теория и практика: В 3 т. Т. 1 / Под общ. ред. А.В. Крутских. 2-е изд., доп. М.: Аспект Пресс, 2021. 384 с.

Международная информационная безопасность: Теория и практика: В 3 т. Т. 2: Сб. документов (на русском языке) / Под общ. ред. А.В. Крутских. М.: Аспект Пресс, 2021. 784 с.

Себекин С.А. Будущее международной системы информационной безопасности в условиях кризиса архитектуры стратегической стабильности. РСМД, 16 ноября 2020 г. URL: https://russiancouncil.ru/analytics-and-comments/columns/cybercolumn/budushchee-mezhdunarodnoy-sistemy-informatsionnoy-bezopasnosti-v-usloviyakh-krizisa-arkhitektury-str/ (дата обращения: 01.01.2022).

Смирнов А.И., Стрельцов А.А. Российско-американское сотрудничество в области международной информационной безопасности: предложения по приоритетным направлениям // Международная жизнь. 2017. № 11. С. 72–81.

Ambos K. International Criminal Responsibility in Cyberspace // Research Handbook on International Law and Cyberspace / ed. by N. Tsagourias, R. Buchan. Edward Elgar, 2015. URL: https://www.e-elgar.com/shop/gbp/research-handbook-on-international-law-and-cyberspace-9781782547389.html (accessed: 01.01.2022).

Antonopoulos C. State Responsibility in Cyberspace // Research Handbook on International Law and Cyberspace / ed. by N. Tsagourias, R. Buchan. Edward Elgar, 2015. URL: https://www.e-elgar.com/shop/gbp/research-handbook-on-international-law-and-cyberspace-9781782547389.html (accessed: 01.01.2022).

Buchan R. Cyber Espionage and International Law. Oxford, 2018. 248 p.

Henderson C. The United Nations and the Regulation of Cybersecurity // Research Handbook on International Law and Cyberspace / ed. by N. Tsagourias, R. Buchan. Edward Elgar, 2015. URL: https://www.e-elgar.com/shop/gbp/research-handbook-on-international-law-and-cyberspace-9781782547389.html (дата обращения: 01.01.2022).

Jensen E.T., Watts S. A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer? // Texas Law Review. URL: https://texaslawreview.org/wp-content/uploads/2017/11/Jensen.Watts_..pdf (accessed: 01.01.2022).

Jian H., Bapna S. The Economic Impact of Cyber Terrorism // The Journal of Strategic Information Systems. 2013. No. 2. P. 175–186.

Kastner P., Megret F. International Legal Dimensions of Cybercrime // Research Handbook on International Law and Cyberspace / ed. by N. Tsagourias, R. Buchan. Edward Elgar, 2015. URL: https://www.e-elgar.com/shop/gbp/research-handbook-on-international-law-and-cyberspace-9781782547389.html (дата обращения: 01.01.2022).

Kerschischnig G. Cyberthreats and International Law. Eleven International Publishing, 2012. 386 p.

Lewis J.A., Stewart B. The Economic Impact of Cybercrime and Cyber Espionage. Report. Center for Strategic and International Studies, 2013. URL: https://apo.org.au/node/35084 (accessed: 01.01.2022).

Nye J. Eight Norms for Stability in Cyberspace. URL: https://aftershock.news/?q=node/812028 &full (accessed: 01.01.2022).

Nye J. How Will New Cybersecurity Norms Develop? Project Syndicate, 2018. URL: https://www.project-syndicate.org/commentary/origin-of-new-cybersecurity-norms-by-joseph-s--nye-2018-03?barrier=accesspaylog (accessed: 01.01.2022).

Nye J. Rules of the Cyber Road for America and Russia. Project Syndicate, 2019. URL: https://www.project-syndicate.org/commentary/cyber-rules-for-america-and-russia-by-joseph-s--nye-2019-03?barrier=accesspaylog (accessed: 01.01.2022).

Saul B., Heath K. Cyber Terrorism. Sydney Law School Legal Studies Research Paper No. 14/11. January 2014. URL: https://ssrn.com/abstract=2387206 (accessed: 01.01.2022).

Tsagourias N. The Legal Status of Cyberspace. // Research Handbook on International Law and Cyberspace / ed. by N. Tsagourias, R. Buchan. St. Louis: Edward Elgar publ., 2016. P. 13–29.

Weimann G. Terrorism in Cyberspace: The Next Generation. New York, 2015. 344 p.

POLITICAL AND LEGAL FRAMEWORK OF THE INTERNATIONAL INFORMATION SECURITY SYSTEM

RUSSIAN APPROACHES AND INITIATIVES

SERGEY BOYKO
Security Council of the Russian Federation, Moscow, 103132, Russia

Abstract

The article covers the policy of the Russian Federation in the field of international information security. The purpose of the study is to identify the key directions for strengthening international cooperation in the area of information security. The article examines the state of bilateral cooperation on international information security issues in particular on the example of the Agreement between the Russian Federation and the People's Republic of China on cooperation in the field of international information security. The article analyzes Russian initiatives put forward in regional and multilateral organizations. Thus, special attention is paid to cooperation within BRICS, the SCO, the CSTO and ASEAN. Regional and interregional interaction in this area increases stability and security of the respective regions, taking into account the national interests of the parties involved. The article also studies the Russian projects promoted at the global level, namely, the UN General Assembly resolutions adopted by the initiative of the Russian Federation. Russia and its partners contributed to the adoption of a set of 13 international rules, principles and norms of responsible behavior of states in the information space. Convocation of an Open-Ended Working Group, whose mandate has been extended until 2025, has become an important contribution of Russia to institutionalization of the profile discussion mechanism within the UN. The author concludes that Russian projects and cooperation agreements reached can foster the development of political and legal framework of the international information security system. The focus on promoting the formation of such a system is confirmed by the updated Basic principles of the State Policy of the Russian Federation in the field of international information security. However, these initiatives are not exhaustive. Therefore, the formation of such a system requires the efforts of the entire world community.

Keywords:

international information security; foreign policy of the Russian Federation; state policy of the Russian Federation; international cooperation.

References

Ambos K. (2015). International Criminal Responsibility in Cyberspace. In: Tsagourias N., Buchan R. (eds). *Research Handbook on International Law and Cyberspace*. St. Louis: Edward Elgar. URL: https://www.e-elgar.com/shop/gbp/research-handbook-on-international-law-and-cyberspace-9781782547389.html (accessed: 01.01.2022).

Antonopoulos C. (2015). State Responsibility in Cyberspace. In Tsagourias N., Buchan R. (eds). *Research Handbook on International Law and Cyberspace*. St. Louis: Edward Elgar. URL: https://www.e-elgar.com/shop/gbp/research-handbook-on-international-law-and-cyberspace-9781782547389.html (accessed: 01.01.2022).

Batueva E.V. (2014). *Amerikanskaya kontseptsiya ugroz informatsionnoj bezopasnosti i ee mezhdunarodno-politicheskaya sostavlyayushchaya. Dissertatsiya na soiskanie uchenoj stepeni kandidata politicheskikh*

nauk [American Concept of Threats to Information Security and Its International Political Dimension. PhD in Political Science Thesis]. Moscow. 207 p.

Buchan R. (2018). Cyber Espionage and International Law. Oxford. 248 p.

Henderson C. (2015) The United Nations and the Regulation of Cybersecurity. In: Tsagourias N., Buchan R. (eds). *Research Handbook on International Law and Cyberspace*. St. Louis: Edward Elgar. URL: https://www.e-elgar.com/shop/gbp/research-handbook-on-international-law-and-cyberspace-9781782547389.html (accessed: 01.01.2022).

Jensen E.T., Watts S. (2017). A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer? *Texas Law Review*. URL: https://texaslawreview.org/wp-content/uploads/2017/11/Jensen.Watts_..pdf (accessed: 01.01.2022).

Jian H., Bapna S. (2013). The Economic Impact of Cyber Terrorism. *The Journal of Strategic Information Systems*. Vol. 22. No. 2. P. 175–186.

Nye J. (2019). *Eight Norms for Stability in Cyberspace.* URL: https://aftershock.news/?q=node/812028&full (accessed: 01.01.2022).

Nye J. (2018). *How Will New Cybersecurity Norms Develop*? Project Syndicate. URL: https://www.project-syndicate.org/commentary/origin-of-new-cybersecurity-norms-by-joseph-s--nye-2018-03?barrier=accesspaylog (accessed: 01.01.2022).

Nye J. (2019). *Rules of the Cyber Road for America and Russia*. Project Syndicate. URL: https://www.project-syndicate.org/commentary/cyber-rules-for-america-and-russia-by-joseph-s--nye-2019-03?barrier=accesspaylog (accessed: 01.01.2022).

Kapustin A.Y. (2015). Ugrozy mezhdunarodnoj informatsionnoj bezopasnosti: formirovanie kontseptual'nykh podkhodov [Threats to International Information Security: Formation of Conceptual Approaches]. *Zhurnal rossiiskogo prava*. No. 8. P. 89–100.

Kapustin A.Y. (2017). K voprosu o mezhdunarodno-pravovoj kontseptsii ugroz mezhdunarodnoj informatsionnoj bezopasnosti [With Regard to the International Legal Concept of Threats to International Information Security]. *Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedeniya.* No. 6. P. 44–51.

Kastner P., Megret F. (2015). International legal dimensions of cybercrime. In: Tsagourias N., Buchan R. (eds). *Research Handbook on International Law and Cyberspace*. St. Louis: Edward Elgar. URL: www.elgaronline.com/view/edcoll/9781782547389/9781782547389.00019.xml?rskey=oZCRWu&result=3 (accessed: 01.01.2022).

Kazarin O.V., Skiba V.Y., Sharyapov R.A. (2016). Novye raznovidnosti ugroz mezhdunarodnoj informatsionnoj bezopasnosti [New Kinds of Threats to International Information Security]. *Istoriya i arkhivy*. No. 1. P. 54–72.

Kerschischnig G. (2012). *Cyberthreats and International Law*. 344 p.

Krasikov D.V. (2018). Mezhdunarodno-pravovaya otvetstvennost' gosudarstv v kiberprostranstve [International Legal Responsibility of States in Cyberspace]. In: Alferova E.V., Lovtsov D.A. (eds). *Gosudarstvo i parvo v novoj informatsionnoj real'nosti: Sbornik nauchnykh trudov*. Moscow: INION. P. 235–247.

Krasikov D.V. (2018). Territorial'nyi suverenitet i delimitatsiya yurisdiktsij v kiberprostranstve [Territorial Sovereignty and Delimitation of Jurisdictions in Cyberspace]. In: Alferova E.V., Lovtsov D.A. (eds). *Gosudarstvo i parvo v novoj informatsionnoj real'nosti: Sbornik nauchnykh trudov*. Moscow: INION. P. 99–111.

Krutskikh A.V. (2007). K politiko-pravovym osnovaniyam global'noj informatsionnoj bezopasnosti [Towards the Political and Legal Foundations of Global Information Security]. *Mezhdunarodnye protsessy*. Vol. 5. No. 1 (13). P. 28–37.

Krutskikh A.V. (ed.) (2021a). *Mezhdunarodnaya informatsionnaya bezopasnost': Teoriya i praktika: V trekh tomakh. Tom 1* [International Information Security: Theory and Practice: In three volumes. Volume 1]. 2nd ed. Moscow: Aspekt Press. 384 p.

Krutskikh A.V. (ed.) (2021b). *Mezhdunarodnaya informatsionnaya bezopasnost': Teoriya i praktika: V trekh tomakh. Tom 2: Sbornik dokumentov* [International Information Security: Theory and Practice: In three volumes. Volume 2: Collection of documents]. Moscow: Aspekt Press. 784 p.

Krutskikh A.V., Biryukov A.V. (2017). Novaya geopolitika mezhdunarodnykh nauchno-tekhnologicheskikh otnoshenij [New Geopolitics of International Scientific and Technological Relations]. *Mezhdunarodnye protsessy*. Vol. 15. No. 2 (49). P. 6–26.

Lewis J.A., Stewart B. (2013). *The Economic Impact of Cybercrime and Cyber Espionage. Report*. Center for Strategic and International Studies. URL: https://apo.org.au/node/35084 (accessed: 01.01.2022).

Saul B., Heath K. (2014). *Cyber Terrorism.* Sydney Law School Legal Studies Research Paper. No. 14/11. URL: https://ssrn.com/abstract=2387206 (accessed: 01.01.2022).

Sebekin S.A. (2020). *Budushchee mezhdunarodnoj sistemy informatsionnoj bezopasnosti v usloviyakh krizisa arkhitektury strategicheskoj stabil'nosti* [The Future of International Information Security

System in Crisis of Strategic Stability Architecture]. URL: URL: https://russiancouncil.ru/analytics-and-comments/columns/cybercolumn/budushchee-mezhdunarodnoy-sistemy-informatsionnoy-bezopasnosti-v-usloviyakh-krizisa-arkhitektury-str/ (accessed: 01.01.2022).

Smirnov A.I., Strel'tsov A.A. (2017). Rossijsko-amerikanskoe sotrudnichestvo v oblasti mezhdunarodnoj informatsionnoj bezopasnosti: predlozheniya po prioritetnym napravleniyam [Russian-American Cooperation in the Field of International Information Security: Proposals in Priority Areas]. *Mezhdunarodnaya zhizn'*. No. 11. P. 72–81.

Tsagourias N. (2016). The legal status of cyberspace. In: Tsagourias N., Buchan R. (eds). *Research Handbook on International Law and Cyberspace*. St. Louis: Edward Elgar Publ. P. 13–29.

Vasenin V.A. (2004). Informatsionnaya bezopasnost' i komp'yuternyj terrorizm [Information Security and Computer Terrorism]. In: Sherstyuk V.P. (ed.) *Nauchnye i metodologicheskie problemy informatsionnoj bezopasnosti*. Moscow: MTsNMO. P. 67–83.

Weimann G. (2015). *Terrorism in Cyberspace: The next Generation*. New York. 344 p.

Zinovieva E.S. (2021). *Mezhdunarodnaya informatsionnaya bezopasnost': problemy dvustoronnego i mnogostoronnego sotrudnichestva* [International Information Security: Issues of Bilateral and Multilateral Cooperation]. Moscow: MGIMO University. 250 p.

Zinovieva E.S. (2019). *Mezhdunarodnoe sotrudnichestvo po obespecheniyu informatsionnoj bezopasnosti: sub"ekty i tendentsii evolyutsii. Dissertatsiya na soiskanie uchenoj stepeni doktora politicheskikh nauk*. [International Cooperation in the Field of Information Security: Actors and Trends of Evolution. Doctor of Political Sciences Thesis]. Moscow. 362 p.