

ДЕЯТЕЛЬНОСТЬ РОССИЙСКОЙ ФЕДЕРАЦИИ В ОБЛАСТИ РАЗВИТИЯ МЕЖДУНАРОДНО-ПРАВОВОГО РЕГУЛИРОВАНИЯ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

М.А. Родионов^{1,2}, д-р военных наук, канд. тех. наук, профессор

С.В. Гришко¹, магистрант

¹ Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации

² Московский государственный технический университет гражданской авиации (Россия, г. Москва)

DOI:10.24412/2411-0450-2025-9-132-137

Аннотация. В статье анализируются инициативы Российской Федерации в области международного регулирования использования информационно-коммуникационных технологий. Рассматриваются принципы и подходы, возможные направления сотрудничества в данной области. Раскрываются вопросы создания в рамках Организации Объединенных Наций постоянно действующей переговорной площадки по международной информационной безопасности.

Ключевые слова: информационно-коммуникационные технологии, киберпространство, киберпреступность, международная информационная безопасность, всемирный механизм, цифровизация.

В настоящее время информационно-коммуникационные технологии (ИКТ) играют ключевую роль в развитии всех сфер жизнедеятельности общества и государства. Они стали неотъемлемой частью глобальной инфраструктуры, обеспечивающей связь, обмен данными и доступ к информации в любой точке мира. При этом практика внедрения ИКТ, без увязки с обеспечением информационной безопасности (ИБ), существенно повышает вероятность проявления угроз в киберпространстве. Эти проблемы выходят за рамки национальных границ, требуют согласованных усилий государств и обществ в их решении. В связи с этим необходимость международного сотрудничества в области ИКТ становится все более критически значимой. Россия, как одна из ведущих мировых держав, активно участвует в формировании международных норм и стандартов в сфере ИБ. Актуальность рассматриваемой темы обусловлена

необходимостью обеспечения стабильного развития государств в условиях технологического прогресса в области ИКТ и противодействия возникающим при этом угрозам в информационной сфере.

В статье исследуется деятельность Российской Федерации по созданию при ООН постоянно действующей переговорной площадки по международной информационной безопасности (МИБ) – «Всемирного механизма по достижениям в области ИКТ в контексте международной безопасности и продвижению ответственного поведения государств в использовании ИКТ», а также изучение перспектив функционирования упомянутого выше Всемирного механизма (ВМ), его влияния на МИБ.

В современном киберпространстве имеется множество угроз, которые требуют скоординированных действий на международном уровне (табл. 1).

Таблица 1. Примеры угроз в киберпространстве

Угроза	Описание
Преступления против конфиденциальности	Нарушения, связанные с незаконным сбором и использованием персональных данных
Кибершпионаж	Несанкционированный доступ к конфиденциальной информации (корпоративной или государственной)
Кибератаки на критическую инфраструктуру	Нарушение работы систем жизнеобеспечения: энергетики, транспорта, здравоохранения и др.
Кибертерроризм и идеологически мотивированные атаки	Использование цифровых инструментов для воздействия на конкретного человека, общество в целом, бизнес и государство
Распространение дезинформации	Создание фейковых новостей для манипуляции общественным сознанием
Киберпреступления с использованием социальной инженерии	Манипуляции над людьми в целях получения доступа к данным

Отрицательные последствия вредоносного применения ИКТ могут иметь критические последствия, в том числе на геополитическом уровне. Одним из основных негативных факторов, влияющих на состояние ИБ, является наращивание рядом государств возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях. Нарушения и противоправные действия в информационной среде несут серьезную угрозу для экономической, политической и социальной стабильности и развития стран. Кибертерроризм направлен на разрушение критической инфраструктуры (энергетика, транспорт и здравоохранение) и с каждым днем становится все более актуальной проблемой. Различные террористические и экстремистские организации широко используют механизмы информационного воздействия на индивидуальное, групповое и общественное сознание в целях нагнетания межнациональной и социальной напряженности, разжигания этнической и религиозной ненависти либо вражды, пропаганды экстремистской идеологии, а также привлечения к террористической деятельности новых сторонников. Такими организациями в противоправных целях активно создаются средства деструктивного воздействия на объекты критической информационной инфраструктуры. Таким образом, создание новой постоянно действующей переговорной площадки по международной информационной безопасности укрепит сотрудничество России с другими государствами в области МИБ в целях формирования международного правового режима использования ИКТ.

Российская Федерация активно использует переговорные площадки ООН для продвижения разного рода инициатив, направленных на

объединение усилий по обеспечению МИБ. Так, еще в конце прошлого века одной из важных инициатив в области МИБ стала принятая Генеральной Ассамблеей ООН резолюция A/RES/53/70 от 1998 года: «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности» [1]. В соответствии с резолюцией Генеральной Ассамблеи ООН A/RES/54/49 от 1999 года международным сообществом была признана угроза негативного воздействия информационных технологий не только на гражданскую, но и на военную сферы [2]. Также в 1999 году нашей страной был разработан и внесен на обсуждение проект документа: «Принципы, касающиеся международной информационной безопасности». Этот проект предусматривал закрепление общих правил поведения государств в информационном пространстве. Данная инициатива была подвергнута критике со стороны США и их союзников, которые посчитали ее попыткой страны, проигравшей холодную войну, выйти из патовой для нее ситуации. Следует отметить исключительную значимость вопросов МИБ применительно к деятельности военно-политического руководства различных государств, особенно в условиях мировой финансово-экономической рецессии [3]. Из-за расхождения мнений США и России по вопросам обеспечения кибербезопасности и ответственного поведения государств в цифровой среде наша страна инициировала создание специализированной межправительственной экспертной площадки по вопросам безопасности в киберпространстве. В 2001 году была принята резолюция ООН A/RES/56/19 о создании Группы правительственных экспертов государств-членов ООН [4]. Однако эта деятельность вновь

столкнулась с неконструктивной позицией западных стран во главе с США.

Резолюция Генеральной Ассамблеи ООН A/RES/73/27 от 2018 года, предложенная Россией, закрепила порядок поведения государств в области применения ИКТ [5]. В связи со стремлением США сохранить лидерство в цифровой среде, разногласия в области обеспечения МИБ показали необходимость создания совершенно новой международной площадки для решения вопросов правового регулирования использования государствами ИКТ, противодействия возрастающим киберугрозам.

В 2019 году в рамках ООН начала свою деятельность Рабочая группа открытого состава (РГОС) по достижениям в сфере информатизации и телекоммуникации в контексте международной безопасности, полномочия которой истекли в июле 2025 г. [6]. Главным результатом ее деятельности стало принятие итогового доклада, одоббившего запуск в 2026 г. на смену РГОС постоянно действующей переговорной площадки по международной информационной безопасности – Всемирного механизма по достижениям в области информационно-коммуникационных технологий в контексте международной безопасности и продвижению ответственного поведения государств в использовании ИКТ. В своей деятельности РГОС удалось достичь понимания вызовов в сфере МИБ, согласовать инструменты сотрудничества в рамках подгрупп будущего механизма по наращиванию потенциала и общим вопросам. Закреплена главенствующая роль государств и строго совещательный статус неправительственных организаций. Также был выработан ряд мер, направленных на преодоление цифрового разрыва между государствами.

Участие в заседаниях международных организаций, таких как ООН, БРИКС, Шанхайская организация сотрудничества (ШОС), в саммитах Россия – Африка [7], демонстрирует приверженность Российской Федерации принципам укрепления доверия между странами в киберпространстве. Значимой площадкой для обсуждения вопросов ИБ выступает Содружество Независимых Государств (СНГ). В октябре 2019 г. государствами-участниками подписана «Стратегия обеспечения информационной безопасности госу-

дарств-участников СНГ» [8]. Важной инициативой России в рамках завершившей свою деятельности РГОС является продвижение «Правил поведения в области обеспечения международной информационной безопасности», которые устанавливают четкие нормы ответственного поведения в цифровой сфере.

К числу основных принципов, которыми руководствуется Российская Федерация при продвижении международных инициатив в области ИБ и правового регулирования в области применения ИКТ, являются: главенствующая роль международного права; обеспечение суверенитета государств в цифровой сфере; предотвращение использования технологий в военных целях, без соблюдения норм международного гуманитарного права; справедливое и равноправное сотрудничество всех заинтересованных сторон; поддержка новых форматов сотрудничества и др. Роль Российской Федерации в формировании ВМ проявляется в ее вкладе в разработку международных норм и стандартов, а также активном сотрудничестве с другими государствами и организациями, например, Международным союзом электросвязи, для борьбы с киберпреступностью и продвижения ответственного поведения в цифровой сфере. В обобщенном виде примеры успешного сотрудничества по обеспечению безопасности в области использования ИКТ приведены в таблице 2.

Российская Федерация поддерживает инициативы, направленные на создание механизмов взаимного контроля и предотвращения конфликтов в киберпространстве, а также разработку универсальных стандартов кибербезопасности, введение международных органов для расследования киберинцидентов и установление четких правил ответственности за такие нарушения. Роль России в разработке и реализации норм ответственного поведения в сфере использования ИКТ заключается в продвижении инициатив, направленных на предотвращение использования технологий в качестве инструмента вмешательства во внутренние дела государств. Российская Федерация также способствует созданию международных механизмов для мониторинга и контроля соблюдения норм безопасности в киберпространстве.

Таблица 2. Примеры двустороннего и международного сотрудничества России в области использования ИКТ

Двустороннее сотрудничество		
Страна	Наименование соглашения	Дата подписания
Бразилия	Соглашение о сотрудничестве в области обеспечения информационной и коммуникационной безопасности	14 мая 2010 г.
Беларусь	Соглашение о сотрудничестве в области обеспечения МИБ	25 декабря 2013 г.
Куба	Соглашение о сотрудничестве в области обеспечения МИБ	11 июля 2014 г.
Китай	Соглашение о сотрудничестве в области МИБ	8 мая 2015 г.
Индия	Соглашение о сотрудничестве в сфере использования ИКТ	15 октября 2016 г.
ЮАР	Соглашение о сотрудничестве в области обеспечения безопасности в сфере использования ИКТ	4 сентября 2017 г.
Международное сотрудничество		
Форма сотрудничества	Участники	Результаты деятельности
Инициативы РФ в рамках ООН	Страны-члены ООН	1. 2015 г. – «Правила поведения в области МИБ» [9]; 2. декабрь 2023 г. – Генеральной Ассамблеей ООН принята юбилейная резолюция, в которой признана значимость результатов работы за 25 лет в области МИБ; 3. 2023 г. – внесена на рассмотрение конвенция о правилах ответственного поведения государств в глобальном информационном пространстве; 4. 2024 г. – Конвенция ООН против киберпреступности [10]
Сотрудничество в рамках БРИКС (совместные проекты по кибербезопасности)	Страны-члены БРИКС	6 июля 2025 г. в Рио-де-Жанейро (Бразилия) подписана Декларация «Укрепление сотрудничества Глобального Юга для более инклюзивного и устойчивого управления» [11]
Второй саммит Россия – Африка	Приняли участие делегации 48 из 54 стран Африки	28 июля 2023 г. принята декларация «О сотрудничестве в области обеспечения МИБ»
Совместные учения по кибер-безопасности	Россия, Беларусь, Казахстан, Азербайджан, Пакистан, Вьетнам	В июне 2022 г. в России прошли Международные киберучения по предупреждению чрезвычайных ситуаций в результате хакерских атак
Создание платформ для обмена информацией	Международные организации и частный сектор	1. Взаимодействие с международным союзом электросвязи (ITU). 2. Двусторонние соглашения о сотрудничестве. 3. В 2009 г. подписано соглашение между правительствами государств-членов ШОС «О сотрудничестве в области обеспечения МИБ» [12].

Примеры инициатив России и других стран по обеспечению ответственного использования ИКТ включают: создание национальных стратегий кибербезопасности, развитие сотрудничества между странами в области обмена информацией о киберугрозах, проведение совместных учений и тренировок. Следует отметить совместное заявление президентов России и США в 2013 г. о взаимодействии по предотвращению киберинцидентов; разработку в ООН методик для сбора, обработки и хранения доказательств, имеющих отношение к преступному и террористическому использованию ИКТ и т.п.

Эти инициативы положительно сказываются на укреплении МИБ и развитии доверия между государствами. Влияние таких мер на глобальную безопасность заключается в снижении рисков кибератак, предотвращении

конфликтов в цифровой среде и создании условий для устойчивого развития.

Перспектива деятельности постоянно действующей переговорной площадки имеет стратегическое значение для обеспечения международной информационной безопасности. ВМ направлен на продвижение норм, правил и принципов, которые будут способствовать ответственному использованию ИКТ.

Создание ВМ представляет собой многогранный процесс, требующий скоординированных действий всех заинтересованных сторон. Важным аспектом функционирования ВМ является взаимодействие Российской Федерации и США в области МИБ. Взаимоотношения между государствами имеют периоды сближения и расхождения мнений. В целом, США стремятся к сохранению превос-

ходства в информационной области, возможности не быть связанными какими-то договорными ограничениями в военном использовании ИКТ.

Россия, как активный участник международного сообщества, продолжает продвигать инициативы, которые направлены на укрепление доверия между государствами в цифровой среде, на предотвращение конфликтов в киберпространстве и на обеспечение устойчивого экономического, социального и политического развития государств в современных реалиях. Применительно к рассматриваем в статье вопросам следует отметить особую значимость вопросов антикризисного менеджмента и эффективного управления стремительно обостряющимися информационны-

ми рисками. Здесь целесообразно применять при необходимой адаптации как существующие подходы в различных сферах, например, представленные в работах [13] и [14], так и создавать новые инновационные методологии и инструментарии.

В целом, подходы, которыми руководствуется и которые отстаивает Российская Федерация на международной арене в области ИКТ и МИБ имеют стратегическое значение для обеспечения безопасного и стабильного цифрового будущего как страны, так и всего международного сообщества. В будущем многополярном мире информационные технологии должны служить инструментом обеспечения безопасности и прогресса, а не источником угроз.

Библиографический список

1. Резолюция Генеральной Ассамблеи ООН A/RES/53/70 от 4 декабря 1998 года. «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности». – [Электронный ресурс]. – Режим доступа: <https://docs.un.org/ru/A/RES/53/70>.

2. Родионов М.А. Политические элиты в условиях мирового финансово-экономического кризиса / М.А. Родионов, Т.А. Волкова // Социально-гуманитарные знания. – 2016. – № 2. – С. 90-103. – EDN WDYACN.

3. Резолюция Генеральной Ассамблеи ООН A/RES/73/27 от 1 декабря 1999 года. «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». – [Электронный ресурс]. – Режим доступа: <https://docs.un.org/ru/A/RES/54/49>.

4. Резолюция Генеральной Ассамблеи ООН A/RES/56/19 от 29 ноября 2001 года. «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». – [Электронный ресурс]. – Режим доступа: <https://ifap.ru/ofdocs/un/5619.pdf>.

5. Резолюция Генеральной Ассамблеи ООН A/RES/73/27 от 5 декабря 2018 года. «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». – [Электронный ресурс]. – Режим доступа: <https://docs.un.org/ru/A/RES/73/27>.

6. Министерство иностранных дел Российской Федерации. Международная информационная безопасность. Сообщение для СМИ «О завершении деятельности Рабочей группы открытого состава ООН по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий». – [Электронный ресурс]. – Режим доступа: https://mid.ru/ru/foreign_policy/international_safety/mezdunarodnaa-informacionnaa-bezopasnost/2036185/.

7. Декларация второго саммита Россия – Африка о сотрудничестве в области обеспечения международной информационной безопасности. URL: <http://kremlin.ru/supplement/5975> (дата обращения: 17.09.2024).

8. Решение Совета глав правительства СНГ от 25 октября 2019 г. «О Стратегии обеспечения информационной безопасности государств-участников Содружества Независимых Государств». – [Электронный ресурс]. – Режим доступа: <https://base.garant.ru/73391721/?ysclid=mfnvn6s88n195844393>.

9. Министерство иностранных дел Российской Федерации. Заявление «Об инициативе стран-членов ШОС «Правила поведения в области обеспечения международной информационной безопасности». – [Электронный ресурс]. – Режим доступа: https://www.mid.ru/ru/foreign_policy/international_safety/mezdunarodnaa-informacionnaa-bezopasnost/1582268/?ysclid=mfnvy6d84781111594.

10. Конвенция Организации Объединенных Наций против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям (принята резолюцией 79/243 Генеральной Ассамблеей ООН от 24 декабря 2024 г.). – [Электронный ресурс]. – Режим доступа: <https://www.un.org/ru/documents/treaty/A-RES-79-243?ysclid=mfnxzqvzla142593998>.

11. БРИКС. Декларация Рио-де-Жанейро «Укрепление сотрудничества Глобального Юга для более инклюзивного и устойчивого управления». – [Электронный ресурс]. – Режим доступа: <https://static.kremlin.ru/media/events/files/ru/gvTArkWauqwuryk9xzLt3HuuI7EBmqrC.pdf>.

12. Министерство иностранных дел Российской Федерации. Многосторонние договоры. Соглашение между правительствами государств-членов Шанхайской организации о сотрудничестве в области обеспечения международной информационной безопасности. – [Электронный ресурс]. – Режим доступа: https://www.mid.ru/ru/foreign_policy/international_contracts/international_contracts/multilateral_contract/50243/.

13. Родионов М.А. Информационно-аналитическая поддержка принятия решений в антикризисном менеджменте / М.А. Родионов // Научный вестник Московского государственного технического университета гражданской авиации. – 2008. – № 131. – С. 126-130. – EDN KVVEMB.

14. Родионов М.А. Информационные аспекты антикризисного авиатранспортного риск-менеджмента // Управление финансовыми рисками. – 2020. – № 2 (62). – С. 120-128.

ACTIVITIES OF THE RUSSIAN FEDERATION IN THE FIELD OF DEVELOPMENT OF INTERNATIONAL LEGAL REGULATION OF THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES

M.A. Rodionov^{1,2}, *Doctor of Military Sciences, Candidate of Technical Sciences, Professor*
S.V. Grishko¹, *Graduate Student*

¹**Russian Presidential Academy of National Economy and Public Administration**

²**Moscow State Technical University of Civil Aviation**
(Russia, Moscow)

Abstract. *The article analyzes the initiatives of the Russian Federation in the field of international regulation of the use of information and communication technologies. The principles and approaches, possible directions of cooperation in this field are considered. The issues of creating a permanent negotiating platform on international information security within the framework of the United Nations are discussed.*

Keywords: *information and communication technologies, cyberspace, cybercrime, international information security, global mechanism, digitalization.*