

УДК 32

DOI: 10.34670/AR.2020.14.41.015

**Проблемы кибербезопасности в условиях регулирования
межгосударственных отношений в информационном
пространстве: позиция России**

Увижева Алена Владимировна

Аспирант,
Северо-Осетинский государственный университет им. К.Л. Хетагурова,
362025, Российская Федерация, Владикавказ, ул. Ватутина, 44-46;
e-mail: maritab19@yandex.ru

Койбаев Борис Георгиевич

Доктор политических наук, кандидат исторических наук, профессор,
завкафедрой всеобщей истории и исторической политологии,
Северо-Осетинский государственный университет им. К.Л. Хетагурова,
362025, Российская Федерация, Владикавказ, ул. Ватутина, 44-46;
e-mail: koibaevbg@mail.ru

Пех Артур Александрович

Старший преподаватель кафедры землеустройства и экологии,
Горский государственный аграрный университет,
362040, Российская Федерация, Владикавказ, ул. Кирова, 37;
e-mail: artur.gejmer@mail.ru

Аннотация

Предметом исследования в статье выступают вопросы информационной безопасности России и мира в условиях непрекращающейся глобализации. Рассмотрены основные инициативы Российской Федерации в части обеспечения кибербезопасности в информационном пространстве, взаимодействия дипломатов нашей страны в рамках организаций СНГ, ШОС и ЕАЭС в области стабильного и защищенного информационного сотрудничества на базе резолюций ООН. Проанализированы базовые подходы России в отношении правил поведения в сфере обеспечения международной информационной защищенности. Изучены правовые аспекты разработки международных конвенций по установлению стабильного и безопасного цифрового пространства. Дипломаты Российской Федерации не раз предпринимали попытки внести на рассмотрение в ООН проект правил взаимодействия между странами в информационном пространстве. Обеспокоенность нашей страны и многих партнеров за ее пределами обусловлена уязвимостью пользовательских данных в эпоху информационных технологий и высокого уровня компьютеризации населения. Данная обеспокоенность выражена в желании нашей страны защитить национальное информационное пространство от вмешательства извне. Интерпретация результатов исследования показывает, что на сегодняшний день, несмотря

на инициативу России по созданию международной правовой базы, регламентирующей информационное пространство, и ввиду расхождений между концепциями и видением западных и российских дипломатов, достоверно не существует прочной международной правовой основы, способной обеспечить защиту интересов стран в глобальной информационной среде.

Для цитирования в научных исследованиях

Увижева А.В., Койбаев Б.Г., Пех А.А. Проблемы кибербезопасности в условиях регулирования межгосударственных отношений в информационном пространстве: позиция России // Теории и проблемы политических исследований. 2020. Том 9. № 5А. С. 136-145. DOI: 10.34670/AR.2020.14.41.015

Ключевые слова

Информационная политика, информационная безопасность, Россия, мировое сообщество, информационные войны, кибертерроризм, кибербезопасность.

Введение

На современном этапе развития информационных технологий, когда новые информационно-коммуникационные технологии воздействуют на ряд аспектов политической жизни [Койбаев, 2012, 50], для многих стран мира такие явления, как хакерские атаки, информационные войны и кибертерроризм, представляют собой проблему, препятствующую эффективному взаимодействию между объектами бизнеса, военными и гражданскими структурами, промышленными предприятиями, населением.

В середине XX в. многие страны уже пытались принять решение в сфере обеспечения информационной безопасности. Однако принятие 10 декабря 1948 г. Всеобщей декларации о правах человека, где в ст. 12, 19 и 26 были установлены законные права людей на получение и распространение информации любыми средствами вне зависимости от нахождения в том или ином государстве, и последующие попытки Генеральной ассамблеи ООН урегулировать возникающие со все большей частотой случаи информационных атак и информационных конфликтов (локальных информационных войн) не смогли повлиять на то, что многие страны мира и прежде продолжают игнорировать данные ключевые положения международного регламента.

Попытки развития международного законодательства в области обеспечения информационной безопасности были предприняты и в Конвенции Совета Европы «О защите прав человек и основных свобод» от 1950 г., и в Международном пакте «О политических и гражданских правах» от 1966 г. Обе конвенции выделяют право на свободу информации в том виде, в котором оно было изначально закреплено в 1948 г.

Российская Федерация, для которой задача создания положительного образа страны стала важнейшей направленностью государственной информационной стратегии [Койбаев, 2013, 45] и которая заинтересована в снижении угрозы в информационной среде, представила свой проект резолюции на Генеральной Ассамблее ООН в 1998 г. Содержание проекта резолюции отражало призыв России к объединению усилий стран участников ООН в целях противодействия использованию информационных технологий в политических, военных, террористических и

иных противоправных целях. Призыв подвергся критике со стороны ряда ведущих западных государств. Только спустя 12 лет в 2010 г. угрозы, о которых наша страна упоминала в конце XX в., были зафиксированы в докладе о достижениях мирового сообщества в области информатизации и цифровизации группы представительных экспертов ООН.

В декабре 2014 г. была принята Резолюция Генеральной Ассамблеи ООН A/RES/69/28 «Достижения в сфере информатизации и коммуникаций в контексте международной безопасности». Основные положения данного документа закрепляли идеи и стремления государств в необходимости обеспечения безопасности в цифровом пространстве. Страны, чьи интересы могут быть затронуты посягательствами на их информационный суверенитет, сошлись в едином мнении о комплексном содействии в противодействии существующим и потенциальным угрозам, разработке стратегий по их предупреждению, ликвидации, сохранению свободного потока пользовательской информации.

По мнению многих исследователей данной проблемы, среди которых можно выделить Пан Ги Муна (бывшего Генерального секретаря ООН), международное пространство все еще находится на раннем этапе развития норм и правил в области обеспечения информационной безопасности на глобальном и локальном уровнях. Несмотря на этот факт, обеспечение международной безопасности в киберсреде является перспективным направлением, требующим к себе особого внимания со стороны развивающихся и развитых стран мира.

Основная часть

Российская Федерация, как уже было сказано ранее, начиная с 1998 г. начала проявлять активность в области рассмотрения вопросов информационной безопасности на постсоветском пространстве и на глобальном уровне. Наша страна как один из главных членов ООН принимала активное участие в утверждении множества резолюций данной организации, в том числе регламентов, цель создания которых состояла в обеспечении безопасного киберпространства.

Принятый уже после 1998 г. в результате обсуждения проект резолюции, затрагивающий вопросы достижения в сфере информационных технологий безопасности в киберпространстве, сформировал обязательную процедуру ежегодного предоставления странами – членами ООН отчетов, содержащих различные мнения по вопросам создания условий для обеспечения информационной безопасности.

Кроме того, Российская Федерация также принимала активное участие в обеспечении международной безопасности в информационной среде. Дипломаты нашей страны взаимодействовали с членами ООН, ШОС, ЕАЭС. В октябре 2011 г. Россия, совместно с государствами членами ШОС (Китай, Узбекистан, Таджикистан, Российская Федерация), направила письмо с проектом так называемых Правил поведения в области обеспечения безопасности в международном пространстве. Однако данный проект был отклонен ввиду неоднозначной оценки и шквала критики со стороны зарубежных партнеров, ориентирующихся на подходы западных стран в вопросах регулирования отношений в информационном пространстве.

Обеспечение информационной безопасности в цифровом пространстве страны Запада представляли иначе, чем страны ШОС и Российская Федерация. Главное отличие российской концепции от западной заключалось в том, что страны Запада предполагали меньший объем

контроля над информационными процессами обмена пользовательской информацией со стороны государства, тогда как российская концепция строилась на необходимости госрегулирования потока информации в федеральных границах и в трансграничном поле.

Несмотря на разногласия между странами в вопросах регулирования информационного потока и безопасности пользовательских данных, активное сотрудничество Российской Федерации и западных партнеров привело к тому, что в декабре 2011 г. в столице Великобритании прошла конференция, посвященная вопросам безопасности в киберпространстве. Ее плодами стали разграничение друг от друга понятий «международная информационная безопасность» и «кибербезопасность» и укрепление понятия «кибербезопасность» в области нормативно-правового регулирования информационного пространства (киберпространства).

В настоящее время Российская Федерация и дальше продолжает совершенствовать концепции стратегии кибербезопасности. Представители федеральных органов законодательной и исполнительной власти принимают в этом активное участие. В перечень понятий, рассматриваемых в том числе в Совете Федерации и на уровне министерств и ведомств, входят «киберпространство», «кибербезопасность», «информационное пространство», «информационная безопасность», «цифровая среда», т. е. понятия, присутствующие и в международном регламенте.

Минусы государственной стратегии кибербезопасности России состоят в том, что применима данная стратегия исключительно на федеральном уровне в силу отсутствия трансграничности (сопоставления с международным регламентом). Соответствия же между международным и российским нормативными регламентами прослеживаются в допущении к нормотворческой работе в сфере информационной безопасности на национальном уровне при условии обозначения в правовых актах трансграничного термина «кибербезопасность».

В январе 2015 г. в рамках инициатив государств – членов ШОС в ООН был внесен документ, затрагивающий нормы поведения в области обеспечения международной безопасности. Основные идеи настоящего документа формировались вокруг принятого Соглашения о сотрудничестве государств – участников СНГ в сфере обеспечения информационной безопасности от 20 ноября 2013 г.

Содержание данных норм (позже названных Правилами), внесенных в ООН, регламентирует мирный характер предотвращения конфликтов и войн в глобальном информационном пространстве. Главный посыл Правил заключается в недопущении установления порядков и стратегий ведения «киберконфликтов» и «кибервойн».

Российская Федерация, на базе предложенных государствами – участниками ШОС Правил, приняла Основы государственной политики в области международной информационной безопасности на период до 2020 г. – документ стратегического планирования, утвержденный Приказом Президента РФ от 24 июля 2013 г. № Пр-1753, в котором определяются основные угрозы в области глобальной безопасности в информационной среде, базовые цели, задачи государственной политики страны в области кибербезопасности.

Инициатива России в области обеспечения информационной безопасности проявляется и в заключении двухсторонних соглашений о сотрудничестве в сфере кибербезопасности и защиты информационного пространства страны от кибератак. Двухсторонние соглашения были заключены Российской Федерацией с такими странами, как Индия, США, Китай, ЮАР, а

предварительные контакты уже налажены с Францией, Израилем, Германией, Японией и Южной Кореей. Многие государства, прознав об инициативах России и разработанных нашей страной концепциях безопасного пользования цифровой средой, начали проявлять интерес к заключению двухсторонних конвенций. Уже к 2014 г. Российской Федерацией были заключены соглашения с Республикой Куба и Республикой Белоруссия.

Соглашения с Республикой Куба от 11 июня 2014 г. и с Республикой Белоруссия от 25 декабря 2013 г. предусматривают взаимодействие правительств стран, заключивших договор, в области решения задач, связанных с обеспечением безопасности информации на международной арене, и преследуют такую цель, как разграничение эффективных и безопасных информационных площадок от тех, которые уязвимы к вмешательству извне [Права..., 1995].

Двухсторонние соглашения направлены на достижение перспектив в осуществлении сотрудничества на международной информационной площадке, способствующего социально-экономическому развитию стран, поддержанию стабильности в регионах и обеспечению мирного урегулирования споров без вмешательства во внутренние дела стран (см. Указ Президента РФ от 31 декабря 2015 г. № 683).

До 2020 г. основу федеральной политики России в области обеспечения кибербезопасности составляет Указ Президента РФ от 24 июля 2013 г. № Пр-1753. Данный указ определяет международную информационную безопасность как состояние глобального киберпространства и цифрового поля, способное обеспечить как полное, так и частичное отсутствие нарушений законных прав человека при осуществлении сбора, хранения, систематизации и распространения информации, законных прав всех государств в рамках взаимодействия в информационной среде, защиту от деструктивного вмешательства в элементы государственной информационной инфраструктуры и т. д. (см. Указ Президента РФ от 31 декабря 2015 г. № 683). На базе данных Правил нашей страной заключаются в том числе и соглашения об обеспечении международной информационной безопасности.

Концепции соглашений Российской Федерации рассматривают международную кибербезопасность как состояние международных отношений, способных обеспечить стабильность и безопасность государств в киберпространстве на глобальном уровне.

Инициатива Российской Федерации была заблокирована и в 2018 г. Предложенный нашей страной проект разработки доклада в рамках группы правительственных экспертов ООН должен был быть основан на Правилах ответственного поведения государств в информационном пространстве, а сам доклад мог бы послужить толчком к принятию новой резолюции. Однако страны запада отклонили инициативу России в угоду своим стратегическим интересам.

На всем протяжении первых двух десятилетий XXI в. наша страна неоднократно предлагала организованным группам экспертов правительств стран мира, объединенным под эгидой ООН, разработать и принять универсальный регламент, так называемые Правила ответственного поведения стран в цифровом пространстве. Хотя концепция, предложенная Российской Федерацией, носила исключительно миротворческий характер, она встретила противоречивый отклик со стороны западных стран. Позиция западных партнеров не вызывала одобрения предложенных нашей страной решений, что, на наш взгляд, только укрепляло понимание того факта, что западные страны стремятся навязать миру свои взгляды на обеспечение безопасности в киберпространстве и свои правила пользования цифровой средой при взаимодействии между

государством, населением и объектами предпринимательской деятельности – корпорациями, компаниями, фабриками и фирмами.

Одной из стран, имеющих схожие с Российской Федерацией взгляды на концепции обеспечения информационной безопасности на глобальной арене, является КНР. 8 сентября 2020 г. в рамках выступления министра иностранных дел КНР Ван И Китаем была проявлена инициатива по принятию международных правил игры в сфере информационной безопасности, строящихся на принципах справедливости и нейтралитета. В заявлении министр иностранных дел Ван И описывал восемь принципов ведения бизнеса компаниями технологического сектора, работающими с персональными данными пользователей сразу в нескольких странах одновременно [Разин, www].

Согласно одному из принципов, компании, занятые в сфере предоставления услуг, связанных с информационными технологиями, должны брать на себя обязательства не вмешиваться в работу инфраструктуры зарубежных стран и не использовать личные данные клиентов в корыстных целях.

Общая картина представленных министром Ван И принципов складывается вокруг противодействия использованию информационных и цифровых технологий в целях нанесения критического ущерба инфраструктуре стран и препятствования незаконного сбора информации о пользователях, собственниках, потребителях. Также инициатива китайской стороны формируется вокруг создания особых каналов юридической помощи в рамках правоприменения для решения вопросов, связанных с получением сведений от государств, в границах которых такие сведения находятся в ограниченном или закрытом доступе.

Немаловажным в выступлении министра Ван И было и упоминание о недавних случаях обнаружения американскими спецслужбами лазеек в программах китайского производства, функционировавших на смартфонах совместно с популярными приложениями и производящих, по мнению спецслужб, сбор данных и потребителей. Китай предлагает требовать от поставщиков цифровых услуг не злоупотреблять доверием стран и их населением и не создавать лазейки в программных продуктах для незаконного получения данных о пользователях.

Инициатива КНР строится на тех же основах и подходах, что и соглашения, заключаемые Российской Федерацией со странами-партнерами: на уважении местных законов, на невмешательстве в дела страны, на предотвращении попыток властей получить доступ к данным без разрешения их владельцев.

Базовые подходы Российской Федерации в сфере обеспечения информационной безопасности основываются на принципах, приведенных на рис. 1.

Комплексное следование Российской Федерацией всем принципам информационной безопасности уже позволяет активно осуществлять взаимодействие между странами-партнерами, заключившими соглашение об информационной безопасности, в рамках правового поля. На практике, исходя из ситуации на мировой арене, можно судить о том, что наша страна делает огромные шаги на пути к созданию прочной правовой основы для регулирования деятельности в информационном пространстве.

Для нашей страны, как и для большинства членов ООН, важно закрепить в информационной сфере принципы неприменения силы, невмешательства во внутренние дела других государств, уважения государственного суверенитета, соблюдения прав и свобод человека. Деятельность Российской Федерации на международной арене в рамках правового поля только доказывает

целеустремленность нашей страны в вопросах обеспечения кибербезопасности, соблюдения прав и свобод человека, безопасного использования цифрового поля.



Рисунок 1 - Принципы информационной безопасности Российской Федерации

В своих инициативах в части решения проблем информационной безопасности на глобальном уровне Российская Федерация не является «игроком-одиночкой». Множество стран Востока и Запада уже приходят к тем же заключениям, о которых твердили дипломаты России в конце XX в. На это могут уйти годы, а то и десятилетия, однако вклад Российской Федерации в становление правовой основы, которой будет в силах регламентировать деятельность государств в цифровой среде, невозможно переоценить.

Заключение

Несмотря на попытки Российской Федерации и иных государств, заинтересованных в обеспечении информационной безопасности на глобальном уровне, на сегодняшний день достоверно не существует прочной политико-правовой основы, способной регламентировать деятельность всех участников международных отношений на политической арене мира.

Библиография

1. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности: резолюция Генеральной Ассамблеи ООН A/RES/69/28 от 02.12.2014. URL: <https://undocs.org/ru/A/RES/69/28>
2. Койбаев Б.Г. Политический имидж государства в современном глобальном информационном пространстве // Вестник Северо-Осетинского государственного университета им. К.Л. Хетагурова. 2013. № 1. С. 45-48.
3. Койбаев Б.Г. Формирование новой системы международных отношений в условиях становления глобального информационного общества // Вестник Северо-Осетинского государственного университета им. К.Л. Хетагурова. 2012. № 1. С. 50-54.
4. Концепция внешней политики Российской Федерации: утв. Президентом РФ 12.02.2013. URL: http://www.consultant.ru/document/cons_doc_LAW_142236/
5. О Стратегии национальной безопасности Российской Федерации: указ Президента РФ от 31.12.2015 № 683. URL: http://www.consultant.ru/document/cons_doc_LAW_191669/
6. Права и свободы личности. М., 1995. 224 с.
7. Разин А. Китайские власти выступили с глобальной инициативой в сфере информационной безопасности. URL: <https://3dnews.ru/1020079>
8. Соглашение между Правительством Российской Федерации и Правительством Республики Куба о сотрудничестве в области обеспечения международной информационной безопасности. URL: <http://docs.cntd.ru/document/420213806>
9. Соглашение о сотрудничестве государств – участников СНГ в области обеспечения информационной безопасности. URL: <http://docs.cntd.ru/document/420278452>

The problems of cybersecurity in the context of the regulation of interstate relations in the information space: Russia's position

Alena V. Uvizheva

Postgraduate,
Khetagurov North Ossetian State University,
362025, 44-46 Vatutina st., Vladikavkaz, Russian Federation;
e-mail: maritab19@yandex.ru

Boris G. Koibaev

Doctor of Political Science, PhD in History, Professor,
Head of the Department of universal history and historical political science,
Khetagurov North Ossetian State University,
362025, 44-46 Vatutina st., Vladikavkaz, Russian Federation;
e-mail: koibaevbg@mail.ru

Artur A. Pekh

Senior Lecturer at the Department of land management and ecology,
Gorsky State Agrarian University,
362040, 37 Kirova st., Vladikavkaz, Russian Federation;
e-mail: artur.gejmer@mail.ru

Abstract

The article studies the information security of Russia and the world in the context of incessant

globalisation. It deals with the main initiatives of the Russian Federation in terms of ensuring cybersecurity in the information space, interaction of the diplomats of our country within the framework of the Commonwealth of Independent States, the Shanghai Cooperation Organisation and the Eurasian Economic Union in the field of stable and secure information cooperation on the basis of the United Nations resolutions. The authors of the article study the legal aspects of the development of international conventions with a view to ensuring a stable and safe digital space. Russian diplomats have made many attempts to submit for approval a draft with the rules for interaction among states in the global space. Our country and its representatives are concerned that users' information in the era of information technology is very vulnerable to external interference. This concern is reflected in the desire of our country to protect the national information space from outside interference. The research results show that today, despite Russia's initiative to create an international legal framework regulating the information space, there is no effective global legal framework capable of protecting the interests of countries in the international information environment.

For citation

Uvizheva A.V., Koibaev B.G., Pekh A.A. (2020) Problemy kiberbezopasnosti v usloviyakh regulirovaniya mezhgosudarstvennykh otnoshenii v informatsionnom prostranstve: pozitsiya Rossii [The problems of cybersecurity in the context of the regulation of interstate relations in the information space: Russia's position]. *Teorii i problemy politicheskikh issledovaniy* [Theories and Problems of Political Studies], 9 (5A), pp. 136-145. DOI: 10.34670/AR.2020.14.41.015

Keywords

Information policy, information security, Russia, global community, information wars, cyberterrorism, cybersecurity.

References

1. Dostizheniya v sfere informatizatsii i telekommunikatsii v kontekste mezhdunarodnoi bezopasnosti: rezolyutsiya General'noi Assamblei OON A/RES/69/28 ot 02.12.2014 [Developments in the field of information and telecommunications in the context of international security: UN General Assembly Resolution A/RES/69/28 of December 2, 2014]. Available at: <https://undocs.org/ru/A/RES/69/28> [Accessed 03/08.20].
2. Koibaev B.G. (2012) Formirovanie novoi sistemy mezhdunarodnykh otnoshenii v usloviyakh stanovleniya global'nogo informatsionnogo obshchestva [Building a new system of international relations in the context of the formation of a global information society]. *Vestnik Severo-Osetinskogo gosudarstvennogo universiteta im. K.L. Khetagurova* [Bulletin of the Khetagurov North Ossetian State University], 1, pp. 50-54.
3. Koibaev B.G. (2013) Politicheskii imidzh gosudarstva v sovremennom global'nom informatsionnom prostranstve [The political image of a state in the modern global information space]. *Vestnik Severo-Osetinskogo gosudarstvennogo universiteta im. K.L. Khetagurova* [Bulletin of the Khetagurov North Ossetian State University], 1, pp. 45-48.
4. Kontseptsiya vneshnei politiki Rossiiskoi Federatsii: utv. Prezidentom RF 12.02.2013 [The conception of the foreign policy of the Russian Federation: approved by the President of the Russian Federation on February 12, 2013]. Available at: http://www.consultant.ru/document/cons_doc_LAW_142236/ [Accessed 03/08.20].
5. O Strategii natsional'noi bezopasnosti Rossiiskoi Federatsii: ukaz Prezidenta RF ot 31.12.2015 № 683 [On the National security strategy of the Russian Federation: Decree of the President of the Russian Federation No. 683 of December 31, 2015]. Available at: http://www.consultant.ru/document/cons_doc_LAW_191669/ [Accessed 03/08.20].
6. Prava i svobody lichnosti [The rights and freedoms of an individual] (1995). Moscow.
7. Razin A. Kitaiskie vlasti vystupili s global'noi initsiativoi v sfere informatsionnoi bezopasnosti [The Chinese authorities launched a global initiative in the field of information security]. Available at: <https://3dnews.ru/1020079> [Accessed 03/08.20].
8. Soglasenie mezhdru Pravitel'stvom Rossiiskoi Federatsii i Pravitel'stvom Respubliki Kuba o sotrudnichestve v oblasti obespecheniya mezhdunarodnoi informatsionnoi bezopasnosti [The agreement between the Russian Government and

-
- the Government of the Republic of Cuba on cooperation in the field of international information security]. Available at: <http://docs.cntd.ru/document/420213806> [Accessed 03/08.20].
9. Soglashenie o sotrudnichestve gosudarstv – uchastnikov SNG v oblasti obespecheniya informatsionnoi bezopasnosti [The agreement on cooperation among CIS countries in the field of information security]. Available at: <http://docs.cntd.ru/document/420278452> [Accessed 03/08.20].