# УПРАВЛЕНИЕ КИБЕРПРОСТРАНСТВОМ В УСЛОВИЯХ ПРОТИВОСТОЯНИЯ РОССИИ И СТРАН СЕВЕРОАТЛАНТИЧЕСКОГО АЛЬЯНСА[1]

***Терентьева Л. В.***[2]

***Ключевые слова:*** *информационная безопасность, информационно-коммуникационное пространство, сеть, суверенитет, мультистейкхолдеризм, модель многостороннего управления, эффективность.*

***Аннотация***

*Цель работы: установление текущего способа управления киберпространством и обоснование наиболее эффективной модели многостороннего управления государствами.*

*Метод: сравнительно-правовой анализ подходов мультистейкхолдеризма и концептуально-логическое моделирование многостороннего управления киберпространством в условиях противостояния России и стран Североатлантического альянса.*

*Результаты: выявлено, что доктринальные и нормативные характеристики киберпространства, такие как демократичность, децентрализованность, неделимость, несводимость к границам физического пространства, утрачивают свое значение в силу сложившейся фрагментации киберпространства в условиях военно-политического противостояния государств; установлена невозможность мультистейкхолдерного управления киберпространством на основе равноправного участия всех вовлеченных в процесс управления субъектов, принимая во внимание, как их неоднородность по своему составу, так и неодинаковый уровень целей и задач, поставленных перед данными субъектами; обоснована эффективность многосторонней модели управления киберпространством государствами, допускающей неформальное участие заинтересованных представителей неправительственных организаций и частного сектора.*

**DOI: 10.21681/1994-1404-2022-3-51-60**

Информационно-коммуникационное пространство с момента своего формирования постепенно становилось ареной геополитического противостояния государств. В условиях военно-политических конфликтов данное пространство фактически трансформируется в площадку силового воздействия на противника. Основным фронтом на поле «информационного боя» является *киберпространство*, реальное понимание которого в настоящий момент стало весьма далеким от его прекраснодушного восприятия в Декларации независимости 1996 г. Джона Барлоу: «*цивилизация сознания… человечная и честная*», «*пространство…независимо[е] от тираний*», «*мир одновременно везде и нигде, но не там, где живут наши тела*», «*мир, в который могут войти все без привилегий и дискриминации, независимо от цвета кожи, экономической или военной мощи и места рождения*» и др. Помимо указанных идеалистических конструкций киберпространства, в основу указанной Декларации был также положен ряд практически не осуществимых, хотя и весьма привлекательных идей, как, например, идеи построения общественного строя с общественными средствами производства и социальным равенством. Так, были манифестированы *способ правления на основе этики, просвещенного эгоизма и общего блага; мир, где кто угодно и где угодно может высказывать свои мнения; развитие киберпространства посредством совокупных действий* и др.

Спустя 26 лет в апреле 2022 г. США, Австралия, Канада, Европейский Союз и Великобритания подписали Декларацию о будущем Интернета, в которой были обозначены принципы открытого, бесплатного, глобального, надежного и безопасного функционирования Интернета, принципы уважения прав человека в Интернете. Содержательно указанные принципы перекликаются с постулатами Барлоу, но, сформулированные в 2022 г., они оказались еще более далекими от действительности, чем установки Декларации Барлоу на 1996 г., когда Интернет находился на самой ранней стадии своей эволюции и объединял всего лишь около миллиона пользователей.

Доктринальные характеристики киберпространства, такие как демократичность [3, 13], децентрализованность, неделимость, несводимость к границам фи-

[1] Статья подготовлена по проекту «Приоритет 2030».

[2] ***Терентьева Людмила Вячеславовна,*** *доктор юридических наук, доцент, профессор кафедры международного частного права Московского государственного университета имени О.Е. Кутафина, г. Москва, Российская Федерация.*

*E-mail: terentevamila@mail.ru*

зического пространства [2], в настоящее время также не отражают реального положения вещей.

Здесь следует заметить, что в национальных и международных документах Интернет часто синонимизируется с киберпространством. Такой подход не вполне верен, поскольку сеть Интернет представляет собой только один из видов компьютерных сетей, который создается путем соединения небольших сетей компьютеров и серверов, для доступа к киберпространству. Киберпространственная инфраструктура является более широкой, поскольку включает в себя компьютеры, которые могут быть как подключены, так и не подключены к Интернету, а также сети, которые могут и являться, и не являться частью Интернета[3]. Киберпространство охватывает не только Интернет, но и важнейшую инфраструктуру, поддерживающую современное общество, такую как электрические сети, системы водоснабжения, банковские операции, транспортные системы и др.

В определениях зарубежных ученых киберпространство представлено как в физическом, так и виртуальном аспекте [6, 14]. *Физическая* часть представляет собой миллионы сетевых информационных и коммуникационных технологий [6—10], которые создают и активируют киберпространство (компьютеры, серверы, маршрутизаторы, процессоры, спутники, коммутаторы и кабели) [11]. *Виртуальная* часть состоит из электронных соединений и данных, передаваемых между частями его физической инфраструктуры и хранящимися в них[4]. В этой связи представленная выше характеристика киберпространства в виде несводимости к государственным границам представляется спорной, поскольку именно физическая часть активирует киберпространство. Интерактивная среда, безусловно, не может существовать сама по себе, поскольку она мобилизована физическими элементами киберпространства, находящимися в пределах юрисдикции определенного государства.

Иные характеристики в виде глобальности, демократичности, децентрализованности и неделимости также вызывают вопросы.

На сегодняшний день глобальный характер сети Интернет сменился его фрагментарным характером. Показательно, что хотя Декларация о будущем Интернета 2022 г., с *одной* стороны, формулирует принцип глобального Интернета, с *другой* стороны — сама же и провоцирует его раскол, апеллируя к неким авторитарным правительствам, которые ограничивают открытый Интернет и используют его для злонамеренных действий, спонсируемых государством или поощряемых им, включая распространение дезинформации и киберпреступлений.

Более радикальные формулировки были включены в Стратегию национальной кибербезопасности США 2018 г.[5] Опубликование данной Стратегии стало в России побудительным мотивом принятия Федерального закона от 1 мая 2019 г. № 90-ФЗ «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации»[6] (Закон о суверенном Интернете), цель которого заключается в обеспечении безопасного и бесперебойного функционирования сети Интернет на территории России.

Так, в Стратегии национальной кибербезопасности США 2018 г., наряду с целями обеспечения безопасности США путем защиты сетей, систем, программных функций и данных, построения безопасной, успешной цифровой экономики и стимулирования развития инноваций на национальном уровне, были поставлены также весьма экспансивные задачи. В числе таких задач — обеспечение мира и безопасности путем увеличения возможностей США совместно с их союзниками и партнерами по сдерживанию, а, при необходимости, и по наказанию лиц и государств, использующих цифровые инструменты в злонамеренных целях, а также расширение американского влияния за рубежом с целью более широкого внедрения основных принципов открытого, функционально совместимого, надежного и безопасного Интернета[7].

В Стратегии 2018 г., в отличие от совместной Декларации о будущем Интернета 2022 г., уже четко стигматизируются страны, обозначаемые в Декларации в качестве непоименованных конкурентов и противников, а именно: Россия, Иран, Северная Корея и Китай. Эти страны позиционируются в Стратегии как страны, которые подрывают принципы свободного Интернета на международных форумах, нарушают законодательство других государств, осуществляя акты экономического шпионажа и хакерские атаки, и рассматривают киберпространство в качестве площадки, которая позволяет нейтрализовать превосходящую военную, экономическую и политическую мощь США[8].

Россия и Китай также сформулировали общее концептуальное видение принципов функционирования информационно-коммуникационной среды, сделав 4 февраля 2022 г. совместное Заявление о международных отношениях, вступающих в новую эпоху, и глобальном устойчивом развитии (далее — Заявление 2022 г.). Помимо отмеченной в Заявлении 2022 г. готовности углубления сотрудничества в сфере *международной информаци-*

[3] At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues. May 13, 2014. P. 8–9. URL: https://www.nap.edu/read/18749/chapter/3

[4] Там же.

[5] National Cyber Strategy of the United States of America 2018. URL: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

[6] Федеральный закон от 1 мая 2019 г. № 90-ФЗ «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации. 2019. № 18. Ст. 2214.

[7] National Cyber Strategy of the United States of America 2018. URL: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

[8] Там же.

*онной безопасности* и построения открытой, безопасной, устойчивой доступной ИКТ-среды («информационно-коммуникационно-технологической»), в Заявлении также говорится о применении к *информационному пространству* [1, 6—9] утвержденных Уставом ООН принципов неприменения силы, уважения государственного суверенитета и основных прав и свобод человека, невмешательства во внутренние дела других государств.

В Заявлении 2022 г. страны также выступили за равные права на управление сетью Интернет и суверенное право на регулирование и обеспечение безопасности национальных сегментов сети Интернет при активном подключении Международного союза электросвязи к решению этих задач.

Заметим, что на протяжении долгого времени на открытых площадках рядом государств неоднократно высказывалась озабоченность о ключевой роли США в управлении сетью Интернет и необходимости пересмотра существующей модели управления. Так, некоммерческая частная корпорация по распределению имен и адресов в сети Интернет (ICANN), осуществляющая важнейшие функции по управлению доменными именами и IP-адресами, зарегистрирована в Калифорнии (США) и действует в соответствии с калифорнийским правом.

В процесс управления киберпространством интегрированы также: Общество Интернета (Internet Society — ISOC), сетевой провайдер — компания Verisign, которая на основании договора с Национальным управлением информации и связи США (NTIA) выполняет функции технического менеджера корневой зоны системы доменных имен (Domain Name System — DNS), а также структура, не являющаяся юридическим лицом, — Рабочая группа по проектированию Интернета (Internet Engineering Task Force — IETF). При этом рабочая группа IETF представляет собой структурное подразделение корпорации системы ISOC — юридического лица Федерального округа Колумбия США. Штаб-квартира компании Verisign находится в штате Виргиния (США).

Отсюда следует, что компании, осуществляющие функции, имеющие глобальные последствия (поскольку от действия данных компаний зависит бесперебойная работа киберпространства по всему миру), являются юридическими лицами США и, соответственно, находятся под юрисдикцией США [5].

При этом до 2016 г. Правительство США могло напрямую влиять на политику ICANN. В соответствии с «Соглашением между Правительством США и Корпорацией ICANN на осуществление функций IANA», заключенным в 2000 г.[9] между некоммерческой компанией по управлению доменными именами и IP-адресами (ICANN) и Национальным управлением информации и связи (NTIA), являющимся подразделением Министерства торговли США, управление ICANN адресным пространством Интернета (доменными зонами и IP-адресами) осуществлялось через подконтрольную Министерству торговли США структуру IANA (Администрация адресного пространства Интернет).

Превалирующая роль США в сфере управления Интернетом и вопрос о выводе сетевой инфраструктуры из-под контроля США становились предметом широкого обсуждения на международном уровне, начиная с момента создания механизма распределения адресного пространства в сети Интернет. Так, МИД России неоднократно предлагал пересмотр существующей модели и передачу отдельных либо всех функций IANA Международному союзу электросвязи (МСЭ)[10].

В связи с этим на 49-й конференции Некоммерческой организации по управлению доменными именами и IP-адресами (ICANN) в Сингапуре 28 марта 2014 г. обсуждалось заявление Национальной администрации по телекоммуникациям и информации Министерства торговли США о своем намерении передать ответственное руководство функциями IANA[11] глобальному сообществу заинтересованных сторон (стейкхолдеров) по модели мультистейкхолдеризма, а именно управления Интернетом с учетом интересов всех участников Интернет-сообщества, бизнеса и государств.

С 1 октября 2016 г. технические функции по ведению баз данных (реестра) доменов верхнего уровня структуры IANA перешли под контроль внутренней структуры ICANN «Публичные технические идентификаторы» (Public Technical Identifiers — PTI), являющейся публичной некоммерческой корпорацией, дочерней организацией Корпорации ICANN[12]. Между тем, несмотря на декларацию осуществления политики мультистейкхолдеризма, данная модель не обеспечила принцип децентрализованного управления сетью Интернет.

Возможность влияния США на управление сетью Интернет сохраняется и по сей день, поскольку США остается страной регистрации компании, имеющей ключевые координирующие функции по распределению адресного пространства, эксплуатации корневых серверов, созданию и администрированию системы доменных имен и адресов Интернета (DNS). При этом США является держателем контрольного пакета акций в данной сфере не только в связи с тем, что технологическая составляющая сети Интернет находится в зоне юрисдикции США, но и в отношении интерактивной,

[9] URL: http://www.iana.org/assignments/iana-ipv6-specialregistry/iana-ipv6-special-registry.xhtml (дата обращения: 01.11.2020); Memorandum of Understanding Between the U.S. Department of Commerce and the Internet Corporation for Assigned Names and Numbers. ICANN. 1999. 31 December. URL: http://www.icann.org/general/icann-mou-25nov98.htm

[10] Итоговый отчет по стратегии ICANN от 23.05.2014. URL: https://www.icann.org/ru/system/files/files/ig-ecosystem-report-23may14-ru.pdf (дата обращения: 21.01.2019). В Основах государственной политики РФ в области международной информационной безопасности до 2020 г. сформулирована цель интернационализации управления информационно-телекоммуникационной сетью Интернет и увеличение в этом контексте роли Международного союза электросвязи.

[11] Администрация адресного пространства Интернет, не являющаяся юридическим лицом группа технических экспертов, подконтрольных Министерству торговли США и входящих в подразделение ICANN.

[12] Продолжение функций IANA на период 2018 г. URL: https://www.icann.org/news/blog/iana-2018-ru (дата обращения: 21.01.2019).

содержательной составляющей, принимая во внимание нахождение многочисленных информационно-коммуникационных платформ и сервисов, оказывающих серьезное влияние на информационную политику других стран.

Привлекательность модели мультистейкхолдеризма и доверие к ней существенно снизились после разоблачений Эдварда Сноудена в 2013 г. о слежке правительственных организаций США за пользователями в Интернете, мониторинге компьютеров и перехвате телефонных звонков иностранных политиков и чиновников спецслужбами Великобритании и США. В связи с этим особую значимость приобрели вопросы установления государственного суверенитета в киберпространстве и защиты национальной критической инфраструктуры.

То есть наряду с моделью мультистейкходеризма, предполагающей равное участие всех заинтересованных субъектов, получила свое обоснование и *модель многостороннего управления* сетью государствами. В соответствии с данной моделью управления основную ответственность в данной сфере несут государства. Обсуждение релевантных вопросов происходит в рамках международных и региональных организаций, но при этом не исключается участие иных заинтересованных лиц. Если *первая* модель мультистейкхолдеризма преимущественно поддерживается западными странами — США, Великобританией, Канадой и Австралией, то *вторая* модель широкого вовлечения государств в процесс управления включает в себя страны Шанхайской организации сотрудничества (ШОС). Так, в фокусе внимания ШОС находится формирование мирного, безопасного и открытого информационного пространства, взаимодействие в котором строится на равных правах для всех стран и при обеспечении суверенных прав государств на управление Интернетом в своем национальном сегменте. По итогам заседания Совета глав государств — членов ШОС в 2019 г. была подписана Бишкекская декларация Совета глав государств — членов ШОС, в которой указана необходимость противодействовать использованию информационно-коммуникационных технологий в целях подрыва политической, экономической и общественной безопасности в странах ШОС, пресекать пропаганду идей терроризма, сепаратизма и экстремизма с использованием сети Интернет[13]. Государства ШОС выступили за выработку универсальных правил, принципов и норм ответственного поведения государств в информационном пространстве и обязались активно сотрудничать в данной области в целях обеспечения *информационной безопасности* [7, 10] на пространстве ШОС.

В западной литературе модель многостороннего управления Интернетом вызвала серьезную критику. Апологетами концепции мультистейкхолдеризма было указано, что государства не могут успешно заниматься управлением сети Интернет без участия бизнеса и общественного сектора [12]. Было отмечено, что тенденция суверенизации Интернета может привести к его фрагментации или «балканизации». Были также высказаны опасения непринятия норм, регулирующих отношения в киберпространстве, Интернет-сообществом, если представители указанного сообщества не принимали участие в их разработке [12].

С указанными аргументами можно поспорить, но прежде всего следует оценить саму возможность управления киберпространством на основе модели мультистейкхолдеризма, в основе которой лежит *концепция равноправного участия* всех заинтересованных субъектов. Здесь закономерен вопрос, даже без учета текущей напряженной политической обстановки, насколько вообще возможно равноправное участие всех вовлеченных в процесс управления субъектов, принимая во внимание как их неоднородность по своему составу, так и неодинаковый уровень целей и задач, поставленных перед данными субъектами. Сеть является площадкой реализации как частных интересов, когда она используется в качестве канала трансляции коммерческих инициатив, так и публичных интересов.

В число последних входят ключевые интересы по обеспечению безопасности государства и общества в виде предотвращения киберугроз, кибератак, поддержание устойчивого и бесперебойного функционирования *информационной инфраструктуры* [6—9] и др. Справедливости ради здесь следует сказать, что в обеспечении безопасного и открытого киберпространства, безусловно, заинтересованы частные коммерческие и некоммерческие компании, которые в равной степени испытывают на себе последствия кибератак и киберугроз, что, в свою очередь, говорит о целесообразности политики вовлечения всех заинтересованных структур в процесс управления сетью Интернет с целью накопления и использования опыта частного сектора при формировании государственной информационной политики. Но формальную, ключевую роль в данном процессе в настоящее время все-таки должны играть государства. Как было отмечено заместителем постоянного представителя Российской Федерации при ООН Д. Полянским в ходе сессии Рабочей группы открытого состава (РГОС) ООН по вопросам безопасности в сфере использования информационно-коммуникационных технологий (ИКТ) и самих ИКТ в 2021—2025 гг.: «*…частные нормы и практики Запада станут основой для международного права в сфере информационной безопасности…. однако амбиции «обладателей капиталов» несравнимы с уровнем ответственности в этой сфере, которую должны нести государства*»[14].

Что касается аргумента о неспособности государств успешно заниматься управлением сетью Интернет без участия бизнеса и общественного сектора, то в рам-

[13] Бишкекская декларация Совета глав государств — членов Шанхайской организации сотрудничества от 14 июня 2019 г. URL: http://www.kremlin.ru/supplement/5421

[14] Полянский указал на право государств отвечать за кибербезопасность // Известия. 2022. 25 июля.

ках международных организаций создаются открытые инклюзивные площадки, где проводятся обсуждения по вопросам управления киберпространством. Так, в 2018 г. начала свою работу новая площадка — РГОС, где обсуждались вопросы развития норм, правил и принципов ответственного поведения государств, прорабатывались вопросы, каким образом международное право применяется к использованию ИКТ государствами. В рамках РГОС обсуждение строится на открытой площадке широким кругом субъектов, включая и представителей заинтересованных неправительственных организаций, частного сектора.

В докладе РГОС по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности ООН от 18 марта 2021 г. был сделан акцент на то, что все заинтересованные стороны должны использовать ИКТ таким образом, чтобы не создавать угрозу миру и безопасности, но основную ответственность за поддержание международного мира и безопасности несут государства[15].

В настоящий момент возможность участия государств в управлении сетью по модели мультистейкхолдеризма обусловлена тем, что в Правлении ICANN участвует также представитель GAC — Правительственного консультативного комитета, который представляет интересы правительств и межправительственных организаций.

Наличие Правительственного консультативного комитета в «Обновленном отчете ICANN, ориентированном на государство: Законы Российской Федерации, касающиеся Интернета, и обсуждения в ООН» 6 июня 2022 г. (Country Focus Report Update: Russian Federation Internet-Related Laws and UN Deliberations) (далее — отчет ICANN 2022 г.) стало одним из аргументов, опровергающих тезис члена экспертного совета при Министерстве цифрового развития В. Макарова о доминировании США при управлении сетью Интернет в ходе дискуссии 28 апреля 2021 г.[16]

В отчете ICANN 2022 г. указано, что Интернет не является исключительно американским, поскольку Устав ICANN запрещает более пяти директоров одного и того же географического региона, ICANN также уже несет ответственность перед всем мировым сообществом; ICANN включает Правительственный консультативный комитет ICANN (GAC), где Россия является членом, а Международный союз электросвязи (МСЭ) является организацией-наблюдателем.

Указанные аргументы представляются спорными, принимая во внимание, что инициативой государств при обсуждении повестки управления сетью Интернет было не сохранение за Международным союзом электросвязи совещательных и наблюдательных функций, а передача ему ключевых функций по управлению сети Интернет, о чем также сказано в совместном заявлении Китая и России от 4 февраля 2022 г.

Тезис об ответственности ICANN перед Правительственным консультативным комитетом вступает в противоречие с Уставом ICANN, в соответствии с которым GAC дает только рекомендации, а в случае расхождения с действиями Правления от Правления требуется обосновать свои действия и попытаться выработать взаимоприемлемое решение. То есть можно зафиксировать, что именно за Правлением остается право выработки финальных решений. При этом, хотя в Правлении и есть представитель GAC, но правом голоса он не обладает. Как представляется, активный формат работы Правительственного консультативного комитета вряд ли обусловил бы инициативу государств БРИКС о размещении корневых серверов на территории данных государств.

Рекомендательный характер решений Правительственного консультационного комитета (GAC) был практически подтвержден в 2011 г., когда правление ICANN вопреки позиции GAC санкционировало доменную зону верхнего уровня для легального порнографического контента «.xxx» [4].

Нахождение 13 корневых серверов лишь в США, Японии, Голландии и Швеции (из них 10 — в США) также не свидетельствуют о глобальном принципе управления сетью. На корневых серверах США находятся файлы зоны .ru.

По мнению авторов отчета ICANN, местонахождение корневых серверов не ведет к угрозе бесперебойному функционированию сети Интернет, поскольку корневые серверы представляют собой сеть из сотен серверов во многих странах мира, а не только в перечисленных четырех[17]. Данный тезис спорен. Функции корневых серверов являются ключевыми, поскольку для бесперебойного функционирования Интернета необходим так называемый *пиринг* — обмен данными провайдерами первого уровня, к которым принадлежат корневые сервера. Как правило, браузер сначала обращается к корневому DNS-серверу, содержащему информацию о подчиненных серверах, и затем идет запрос к соответствующему подчиненному серверу, где, в свою очередь, содержится информация об IP-адресах того или иного сайта. В России не находится ни один корневой сервер, но в то же время имеется так называемая *замещающая инфраструктура* в виде копий корневых серверов, позволяющих выполнять функцию корневого сервера при наличии сбоев. Об этом также упомянуто в отчете ICANN в пользу вывода о невозможности создания ситуации нестабильности функционирования сети Интернет. Но создание резервных серве-

[15] A/75/816, 18 March 2021. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/068/74/PDF/N2106874.pdf?OpenElement. P. 25.

[16] Country Focus Report Update: Russian Federation Internet-Related Laws and UN Deliberations. 6 June 2022. ICANN. URL: https://itp.cdn.icann.org/en/files/government-engagement-ge/ge-011-06-06-2022-en.pdf

[17] Country Focus Report Update: Russian Federation Internet-Related Laws and UN Deliberations. 6 June 2022. ICANN. URL: https://itp.cdn.icann.org/en/files/government-engagement-ge/ge-011-06-06-2022-en.pdf

ров для обеспечения стабильности работы Интернета является инициативой исключительно самой России.

Кроме того, несмотря на заявления членов правления ICANN о невозможности «отключения Интернета», такие инициативы, судя по всему, имели место в 2003 г., когда национальный домен Ирака .iq по решению ICANN был изъят у национального иракского администратора — компании InfoCom, а также в 2012 г. в Сирии, когда на два дня Интернет был отключен.

Такие меры явно противоречат выработанной позиции стран в заключительном докладе РГОС по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности ООН, где говорится, что государства не должны использовать посредников для совершения международно-противоправных деяний с применением ИКТ и должны стремиться обеспечить, чтобы их территория не использовалась для совершения таких деяний негосударственными субъектами, действующими по указанию государства или под его контролем, а также отмечена ответственность государств в отношении субъектов, принадлежащих государству или находящихся под его контролем[18]. Но данные положения не являются обязательными международными нормами и носят всего лишь рекомендательный характер. В этой связи реальная практика деятельности компаний вступает в противоречие с сформулированными в Отчете правилами.

Так, в марте 2022 г. крупный интернет-провайдер США Cogent заявил об отключении нескольких российских операторов, наиболее известными среди которых являлись VK, Ростелеком, Яндекс, Мегафон[19]. И в марте того же года украинский вице-премьер и министр цифровой трансформации М. Федоров обратился с письмом к генеральному директору ICANN Йорану Марби с просьбой отключить корневые серверы DNS в России и отозвать российские домены, такие как .ru, .рф, .su. Ответное письмо было подготовлено исполнительным советом RIPE NCC – одним из пяти региональных регистраторов, в котором было гарантировано бесперебойное предоставление услуг вне зависимости от внутриполитических споров, международных конфликтов, войн[20]. В то же время говорилось, что Исполнительный совет также выражает солидарность с теми операторами, на которых лежит трудная задача поддержания доступа в Интернет для оказания помощи людям, страдающим от ужасных последствий вооруженных конфликтов и войн[21]. Мотивом отрицательного ответа, как представляется, была не приверженность принципу нейтральности, а те прагматичные аргументы, которые были высказаны, в частности, бывшим президентом ICANN Полом Туми: «*Сохранение уровня протокола в России – лучший способ обеспечить эффективность сайтов, предлагающих различные взгляды российской аудитории*»[22]. В то же время следует заметить, что отрицательный ответ украинскому вице-премьеру и министру цифровой трансформации М. Федорову вызвал критику со стороны ряда официальных лиц Украины и стран Североатлантического альянса[23]. И сам факт того, что данный вопрос стал предметом обсуждения, не может гарантировать устойчивость политики ICANN в предоставлении равного доступа к ресурсам сети.

В этой связи, хотя США и принадлежит к кругу стран, поддерживающих концепцию мультистейкхолдеризма, реальное положение вещей свидетельствует, что в рамках данной модели США обладают контрольным пакетом акций, позволяющим реализовывать *свои правила* в киберпространстве, что явно не отражает принципа равного участия в управлении. Отказ от принципа равного участия в управлении киберпространством прослеживается и в Стратегии национальной кибербезопасности США 2018 г., в которой постулируется необходимость сохранения превосходства США в киберпространстве, появление и увеличение влияния которого на все сферы жизни современного мира, как отмечено в Стратегии, совпали со становлением США в качестве единственной сверхдержавы во всем мире[24].

Таким образом, на сегодняшний день вряд ли возможно говорить об интернациональном, открытом, демократичном управлении киберпространством в условиях разделения стран на различные противоборствующие группировки, в рамках которых информационные технологии в равной степени являются как средством кибератак, так и объектом для них. В связи с этим монопольное сосредоточение ресурсов для бесперебойного функционирования сети в пределах одного государства актуализирует альтернативную концепцию управления киберпространством, где ключевую роль в данном процессе играют государства.

Любопытно, что и в США фиксируется тенденция фрагментации киберпространства, но, как представляется, беспокойство по этому поводу питается опасениями утратить монопольный контроль над сетью. Так, в опубликованном независимой целевой группой, организованной Советом по международным отношениям США, в июле 2022 г. отчете о внешней политике США в киберпространстве утверждается невозможность дальнейшей реализации концепции глобального, безопасного, свободного и открытого Интернета в связи тем, что различные государства контролируют Интернет, локализуют данные, блокируют и модерируют контент, а также запускают кампании политического вли-

[18] A/75/816, 18 March 2021. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/068/74/PDF/N2106874.pdf?OpenElement. P. 24.

[19] URL: https://cisoclub.ru/amerikanskij-internet-provajder-cogent-otklyuchaet-rossijskih-operatorov-yandeks-rostelekom-vk-megafon-vympelkom-i-drugih

[20] URL: https://www.ripe.net/ripe/mail/archives/ripe-list/2022-March/002462.html

[21] Там же.

[22] URL: https://www.pcmag.com/news/icann-denies-ukrainian-request-to-shut-down-russian-internet-domains

[23] URL: https://arstechnica.com/tech-policy/2022/03/ukraine-wants-russia-cut-off-from-core-internet-systems-experts-say-its-a-bad-idea

[24] National Cyber Strategy of the United States of America 2018. URL: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

яния[25]. В связи со сказанным целевая группа пришла к *выводу* о необходимости формирования *новой внешней политики* в сфере киберпространства, которая должна быть выражена: в консолидации коалиции союзников по видению Интернета в качестве международной коммуникационной платформы; в дипломатическом и экономическом давлении на противников; согласовании политики цифровой конкуренции с более широкой стратегией национальной безопасности; в заключении цифрового торгового соглашения с партнерами; в принятии общей политики цифровой конфиденциальности, которая совместима с европейским регламентом защиты данных (GDPR); создании международного центра киберпреступности; сохранении технологического превосходства, привлечение государств к ответственности за вредоносную деятельность, происходящую с их территорий, и т. п. [26]

Возможность следования указанной траектории создания блокового противостояния несколько тормозит реализацию решений, которые с 90-х годов принимались на различных площадках ООН: о создании международного порядка в сфере киберпространства (а именно, сотрудничества в деле предупреждения злонамеренного использования ИКТ); о недопущении заведомого использования территории государств для совершения международно-противоправных деяний с использованием ИКТ; об ответственном представлении информации о факторах уязвимости в сфере ИКТ и др.

Следует обратить внимание на то, что впервые «*нет международной информационной войне*» сформулировала Россия в 1998 г., когда Генеральной Ассамблее ООН был предложен проект резолюции по выработке согласованной позиции о военном применении информационно-коммуникационных технологий. Хотя в резолюцию Генеральной Ассамблеи не вошел ряд поднятых РФ вопросов, в числе которых были и угрозы военного применения ИКТ, необходимость запрещения таких вооружений и сопоставления воздействия оружия массового уничтожения и информационного оружия, в согласованном тексте резолюции Генеральной Ассамблеи была выражена озабоченность, что информационные технологии могут быть использованы в целях, несовместимых с задачами обеспечения международной стабильности и безопасности[27].

В Резолюции была также обоснована необходимость предотвращения неправомерного использования информационных ресурсов или технологий в преступных или террористических целях, было предложено выработать общую оценку информационной безопасности, определить основные понятия, относящихся к информационной безопасности, и разработать международно-правовые принципы, которые были бы направлены на укрепление безопасности глобальных информационных и телекоммуникационных систем[28]. С этого года Генеральный секретарь ежегодно представлял Генеральной Ассамблее доклад, содержащий позиции государств — членов ООН по данной теме. В 2004 г., также по инициативе России, была сформирована Группа правительственных экспертов (ГПЭ) ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности.

С 2018 г. вопросы международной безопасности обсуждались на двух площадках ООН — ГПЭ и РГОС по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. В рамках ГПЭ на основе консенсуса были приняты четыре доклада (2010, 2013, 2015, 2021 гг.), в которых были рекомендованы *правила ответственного поведения* государств в киберпространстве в контексте международной безопасности. В докладах ГПЭ говорилось также о том, что суверенитет государств и международные нормы и принципы, проистекающие из суверенитета, применяются к осуществлению государствами деятельности, связанной с ИКТ, и к их юрисдикции над ИКТ-инфраструктурой, расположенной на их территориях.

В резолюции 70/237 Генеральная Ассамблея призвала государства-члены при использовании ИКТ руководствоваться докладом Группы правительственных экспертов 2015 г., в котором содержится 11 добровольных, не имеющих обязательной силы норм ответственного поведения государств[29]. В число норм входят обязательства государств сотрудничать в разработке и осуществлении мер по укреплению стабильности и безопасности в использовании ИКТ и предупреждению совершения действий в сфере ИКТ, способных создать угрозу международному миру и безопасности; не позволять использовать территорию государств для совершения международно-противоправных деяний с использованием ИКТ; сотрудничать в целях обмена информацией, оказания взаимопомощи, преследования лиц, виновных в террористическом и преступном использовании ИКТ; соблюдать права человека в Интернете (права на неприкосновенность личной жизни в эпоху цифровых технологий, право свободно выражать свое мнение); не поддерживать деятельность в сфере ИКТ, если такая деятельность противоречит обязательствам по международному праву, наносит преднамеренный ущерб критически важной инфраструктуре; принимать надлежащие меры для защиты своей критически важной инфраструктуры от угроз в сфере ИКТ и др.

Россия и Китай явились инициаторами создания в рамках ООН более инклюзивного формата обсуждения вопросов информационной безопасности, который бы позволил принимать участие в обсуждении всем заинтересованным участникам. Поэтому в 2018 г. начала

[25] URL: https://www.cfr.org/report/confronting-reality-in-cyberspace

[26] Там же.

[27] A/RES/53/70, 4 January 1999. URL: https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70&referer= /english/&Lang=R

[28] A/RES/53/70, 4 January 1999. URL: https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70&referer= /english/&Lang=R

[29] A/70/174, 22 July 2022. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/37/PDF/N1522837.pdf?OpenElement

свою работу новая площадка — РГОС, где обсуждались вопросы дальнейшего развития норм, правил и принципов ответственного поведения государств, прорабатывались вопросы, каким образом международное право применяется к использованию ИКТ государствами. В частности, открытым остался вопрос, может ли государство воспользоваться своим неотъемлемым правом на самооборону (статья 51 Устава) в связи с такими видами связанной с ИКТ деятельности, которые могут быть истолкованы другими государствами как угроза силой или ее применение (статья 2(4) Устава)[30].

Как было показано, в отличие от ГПЭ ООН, в рамках РГОС ООН обсуждение строится на открытой площадке широким кругом субъектов, включая и представителей заинтересованных неправительственных организаций, и частного сектора. Существование двух переговорных форматов ГПЭ и РГОС было обусловлено политическим соперничеством России и США, но компромисс был найден, в результате которого стороны обратились к единой переговорной арене — РГОС.

На заседании Первого комитета Генеральной Ассамблеи 3 ноября 2021 г. была принята резолюция A/C.1/76/L.13, совместный проект которой внесли Россия и США[31]. В Резолюции были отмечены принятие заключительного доклада РГОС по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности[32], а также усилия ГПЭ ООН по подготовке заключительного доклада по поощрению ответственного поведения государств в контексте международной безопасности[33].

Принятие данной Резолюции и сам доклад РГОС 2021 г. были оценены спецпредставителем президента России по вопросам международного сотрудничества в сфере информационной безопасности Андреем Крутских как триумфальный успех российской дипломатии, поскольку были закреплены базовые подходы, выдвигаемые Россией, по предотвращению конфликтов в *информационной сфере* [6, 7, 9], недопущению её милитаризации, и использованию ИКТ исключительно в мирных целях[34]. Следующим шагом прогнозировалась подготовка Конвенции о противодействии использованию ИКТ в преступных целях для придания данным правилам обязательного характера.

В июле 2022 г. в штаб-квартире ООН в Нью-Йорке открылась новая сессия РГОС по кибербезопасности. Но работа новой сессии проходила в тяжелых условиях, принимая во внимание скандальный флер, сопровождавший ее открытие. Российской Федерацией было заблокировано участие в сессиях связанных с Западом IT-компаний и неправительственных организаций (Microsoft, Cybersecurity Tech Accord, Global Forum on Cyber Expertise), Украина заветировала организации, связанные с Россией (Центр международной информационной безопасности и научно-технической политики МГИМО, Российский совет по международным делам, Институт государства и права РАН, Российский Федеральный центр судебной экспертизы при Министерстве юстиции), США отказали в визе главе российской делегации на РГОС.

Работа на данной площадке продолжается, хотя и с большими сложностями в условиях текущей международной обстановки. Постулат РГОС о том, что международное право и, в частности, Устав ООН применимо и имеет ключевое значение для поддержания мира и стабильности и содействия обеспечению открытой, безопасной, стабильной, доступной и мирной ИКТ-среды, представляет собой безусловную значимость, равно как и пока открытый вопрос, каким образом международное право применяется к использованию ИКТ государствами, а также вопрос о придании юридической обязательности нормам, которые были сформулированы на всех предыдущих сессиях РГОС и ГПЭ. Проработка таких вопросов необходима и на региональном уровне, а именно в рамках ШОС, которая, координируя свою деятельность с ООН, могла бы предложить более конкретные механизмы и инструменты по достижению тех задач, которые были сформулированы РГОС и ГПЭ.

[30] A/75/816, 18 March 2021. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/068/74/PDF/N2106874.pdf?OpenElement. P. 25.

[31] A/C.1/76/L.13, 8 October 2021. URL: https://namib.online/wp-content/uploads/2021/10/N2128104.pdf

[32] A/75/816, 18 March 2021. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/068/74/PDF/N2106874.pdf?OpenElement.

[33] A/76/135, 14 July 2021. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/075/88/PDF/N2107588.pdf?OpenElement.

[34] В РФ заявили, что рабочая группа ООН по информационной проблематике начнет работу в июне. URL: https://namib.online/2021/03/v-rf-zajavili-chto-rabochaja-gruppa-oon-po-informacionnoj-problematike-nachnet-rabotu-v-ijune

*Рецензент:* ***Запольский Сергей Васильевич,*** *доктор юридических наук, профессор, заслуженный юрист Российской Федерации, главный научный сотрудник Института государства и права Российской академии наук, г. Москва, Российская Федерация.*
*E-mail: zpmoscow@mail.ru*

**Литература**

1. Бурый А.С., Ловцов Д.А. Перспективы стандартизации информационного пространства умного города // Информационно-экономические аспекты стандартизации и технического регулирования. 2022. № 2(66). С. 4—11.
2. Войниканис Е.А. Право интеллектуальной собственности в цифровую эпоху: парадигма баланса и гибкости. М. : Юриспруденция, 2014. 552 с. ISBN 978-5-9516-0680-8.

3. Дашян М.С. Право информационных магистралей (Law of information highways): вопросы правового регулирования в сфере Интернет. М. : Волтерс Клувер, 2007. 275 с. ISBN 978-5-466-00307-9.
4. Демидов О.В. Сдадут ли США ключи от Интернета? // Индекс безопасности. 2014. Т. 20. № 2 (109). С. 119—122.
5. Касенова М.Б. «Глобальное сообщество заинтересованных сторон» и перспективы трансграничного управления Интернетом // Право и государство: теория и практика. 2014. № 10 (118). С. 138—143.
6. Ловцов Д.А. Системология правового регулирования информационных отношений в инфосфере : монография. М. : РГУП, 2016. 316 с. ISBN 978-5-93916-505-1.
7. Ловцов Д.А. Теория защищенности информации в эргасистемах : монография. М. : РГУП, 2021. 276 с. ISBN 978-5-93916-896-0.
8. Ловцов Д.А. Информационная теория эргасистем : монография. М. : РГУП, 2020. 314 с. ISBN: 978-5-93916-887-8.
9. Ловцов Д.А. Системология информационного права // Правосудие / Justice. 2022. Т. 4. № 1. С. 41—70. DOI: 10.37399/2686- 9241.2022.1.41-70 .
10. Ловцов Д.А. Обеспечение информационной безопасности в российских телематических сетях // Информационное право. 2012. № 4. С. 3—7.
11. Терентьева Л.В. Понятие киберпространства и очерчивание его территориальных контуров // Правовая информатика. 2018. № 4. С. 66—71. DOI: 10.21681/1994-1404-2018-4-66-71 .
12. Bitros G.C., Kyriazis N.C. Democracy and an Open-Economy World Order. Springer International Publishing AG, 2017, p. 29.
13. Manuel R. Torres Soriano. Internet as a driver of political change: cyber-pessimists and cyber-optimists. Revista del Instituto Español de Estudios Estratégicos, No. 1, 2013, p. 335.
14. Spade C.J.M. Information as Power: China's Cyber Power and America's National Security. Edited by Jeffrey L. Caton. May 2012, p. 6. URL: https://itlaw.wikia.org/wiki/Information_as_Power:_China%27s_Cyber_Power_and_America%27s_National_Security

# GOVERNING CYBERSPACE UNDER THE CONDITIONS OF CONFRONTATION BETWEEN RUSSIA AND THE COUNTRIES OF THE NORTH ATLANTIC ALLIANCE

*Liudmila Terent'eva*[35]

***Keywords:*** *information security, information and communication space, network, sovereignty, multistakeholderism, multilateral governance model, efficiency.*

***Abstract***

*Purpose of the work: establishing the current way of governing cyberspace and justifying the most efficient model of multilateral governance of countries.*

*Methods used: comparative legal analysis of multistakeholderism approaches and conceptual logical modelling of multilateral governance of cyberspace under the conditions of confrontation between Russia and the countries of the North Atlantic Alliance.*

*Findings: it is shown that such doctrinal and normative characteristics of cyberspace such as democracy, decentralisedness, indivisibility, irreducibility to the boundaries of physical space lose their significance due to the current fragmentation of cyberspace under the conditions of military and political confrontation of countries. The impossibility of a multi-stakeholder governance of cyberspace based on equitable participation of all subjects involved in the management process is established considering the heterogeneity of composition of these subjects as well as the different level of goals and tasks set before these subjects. A justification is given for the efficiency of a model of multilateral governance of cyberspace by countries allowing informal participation of interested representatives of non-governmental organisations and the private sector.*

**References**

1. Buryi A.S., Lovtsov D.A. Perspektivy standartizatsii informatsionnogo prostranstva umnogo goroda. Informatsionno-ekonomicheskie aspekty standartizatsii i tekhnicheskogo regulirovaniia, 2022, No. 2(66), pp. 4–11.

[35] ***Liudmila Terent'eva,*** *Dr.Sc. (Law), Professor at the Department of International Private Law of the Kutafin Moscow State Law University, Moscow, Russian Federation.*
*E-mail: terentevamila@mail.ru*

2. Voinikanis E.A. Pravo intellektual'noi sobstvennosti v tsifrovuiu epokhu: paradigma balansa i gibkosti. M. : Iurisprudentsiia, 2014. 552 pp. ISBN 978-5-9516-0680-8.
3. Dashian M.S. Pravo informatsionnykh magistralei (Law of information highways): voprosy pravovogo regulirovaniia v sfere Internet. M. : Volters Kluver, 2007. 275 pp. ISBN 978-5-466-00307-9.
4. Demidov O.V. Sdadut li SShA kliuchi ot Interneta? Indeks bezopasnosti, 2014, t. 20, No. 2 (109), pp. 119–122.
5. Kasenova M.B. "Global'noe soobshchestvo zainteresovannykh storon" i perspektivy transgranichnogo upravleniia Internetom. Pravo i gosudarstvo: teoriia i praktika, 2014, No. 10 (118), pp. 138–143.
6. Lovtsov D.A. Sistemologiia pravovogo regulirovaniia informatsionnykh otnoshenii v infosfere : monografiia. M. : RGUP, 2016. 316 pp. ISBN 978-5-93916-505-1.
7. Lovtsov D.A. Teoriia zashchishchennosti informatsii v ergasistemakh : monografiia. M. : RGUP, 2021. 276 pp. ISBN 978-5-93916-896-0.
8. Lovtsov D.A. Informatsionnaia teoriia ergasistem : monografiia. M. : RGUP, 2020. 314 pp. ISBN: 978-5-93916-887-8.
9. Lovtsov D.A. Sistemologiia informatsionnogo prava. Pravosudie / Justice, 2022, t. 4, No. 1, pp. 41–70. DOI: 10.37399/2686-9241.2022.1.41-70 .
10. Lovtsov D.A. Obespechenie informatsionnoi bezopasnosti v rossiiskikh telematicheskikh setiakh. Informatsionnoe pravo, 2012, No. 4, pp. 3–7.
11. Terent'eva L.V. Poniatie kiberprostranstva i ocherchivanie ego territorial'nykh konturov. Pravovaia informatika, 2018, No. 4, pp. 66–71. DOI: 10.21681/1994-1404-2018-4-66-71 .
12. Bitros G.C., Kyriazis N.C. Democracy and an Open-Economy World Order. Springer International Publishing AG, 2017, r. 29.
13. Manuel R. Torres Soriano. Internet as a driver of political change: cyber-pessimists and cyber-optimists. Revista del Instituto Español de Estudios Estratégicos, No. 1, 2013, p. 335.
14. Spade S.J.M. Information as Power: China's Cyber Power and America's National Security. Edited by Jeffrey L. Caton. May 2012, r. 6. URL: https://itlaw.wikia.org/wiki/Information_as_Power:_China%27s_Cyber_Power_and_America%27s_National_Security