МГЮА

приоритет2030^
право для лидерства

АНАЛИТИЧЕСКИЙ ДОКЛАД

«Правовое управление киберпространством в целях устойчивого развития»

Автор: д.ю.н. Терентьева Людмила Вячеславовна, доцент, профессор кафедры международного частного права Университета имени О.Е. Кутафина (МГЮА)

Оглавление

1. Киберпространство арена геополитического противостояния

Киберпространство с момента своего формирования постепенно становилось ареной геополитического противостояния государств, на которой страны пытаются отстаивать свое право как на контроль в отношении критически важных инфраструктур, так и на трансляцию ценностей, интересов, норм и идей. В частности, в Стратегии национальной кибербезопасности США 2018 г. еще до начала специально военной операции РФ говорилось о необходимости сохранения превосходства США в киберпространстве, появление и увеличение влияния которого на все сферы жизни современного мира, как было отмечено в Стратегии, совпали со становлением США в качестве единственной сверхдержавы во всем мире[1]. Опубликование данной Стратегии стало в России одним из побудительных мотивов принятия ФЗ от 1 мая 2019 г. N 90-ФЗ «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации» [2] (далее - Закон о суверенном Интернете), цель которого заключается в обеспечении безопасного и бесперебойного функционирования российского сегмента Интернета в случае его отключения от глобальной сети.

Противодействие угрозам устойчивого и бесперебойного функционирования национальной инфраструктуры киберпространства относится к числу важнейших национальных интересов государств. Фокусирование государственных интересов в данной сфере обусловило в свою очередь то, что киберпространство становится и как средство ведения информационной войны с применением информационных технологий в военно-политических целях, и объектом информационных атак.

---

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

[2] Федеральный закон от 1 мая 2019 г. N 90-ФЗ «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации»// СЗ РФ. 2019. № 18. Ст. 2214.

В связи с проведением спецоперации против Российской Федерации общее количество кибератак в 2022 г. увеличилось на 21% по сравнению с 2021 годом. Среди организаций жертвами атак чаще всего становились госучреждения (17%), медицинские учреждения (9%) и промышленность (9%). Как было отмечено спецпредставителем президента РФ по вопросам международного сотрудничества в области информационной безопасности, директором департамента международной безопасности МИД А. Крутских кибератаки осуществляются на Россию из разных стран, но их очаг в основном прослеживается из США, стран НАТО и Украины[3].

2. Угрозы бесперебойному функционированию киберпространству

Как было отмечено, в РФ имеются инструменты по обеспечению работы российского сегмента Интернета в случае его отключения от глобальной сети, позволяющие Роскомнадзору в соответствии с Законом о суверенном Интернете осуществлять полномочия по централизованному управлению сетями связи. Не пострадает в случае отключения и российская критическая инфраструктура, функционирование которой осуществляется вне связи с иностранными серверами и производителями. В целях обеспечения технологической независимости и безопасности критической информационной инфраструктуры РФ Указом Президента РФ от 30 марта 2022 г. было постановлено, что с 31 марта 2022 г. заказчики (за исключением организаций с муниципальным участием), осуществляющие закупки в соответствии с ФЗ от 18 июля 2011 г. N 223-ФЗ "О закупках товаров, работ, услуг отдельными видами юридических лиц", не могут осуществлять закупки иностранного программного обеспечения, в том числе в составе программно-аппаратных комплексов, в целях его использования на принадлежащих им значимых объектах критической информационной инфраструктуры РФ. В соответствии с Указом с 1 января 2025 г. органам государственной власти,

[3] Число кибератак в России и в мире (tadviser.ru).

заказчикам запрещается использовать иностранное программное обеспечение на принадлежащих им значимых объектах критической информационной инфраструктуры.

В то же время отключение России от глобального киберпространства не окажется без последствий. В результате отключения произойдут замедление его работы, а также блокировки соцсетей и ряд веб-сайтов. Так, за 2022 г. были исчислены потери в $21,5 млрд только от блокировок соцсетей в России, при том, что отключения доступа к глобальному киберпространству и замедления его работы не происходило[4]. При этом, предполагаемые потери от блокировки веб-сайтов исследователи не подсчитывали, в силу сложности их расчета.

По мнению ряда экспертов, Западу не выгодно отключать Россию от глобального интернета, поскольку Россия подключена к мировому интернету с помощью менее десятка узлов связи и через страну проводят трафик и другие государства, включая Японию[5]. Аналогичной позиции придерживаются и члены правления некоммерческой организации по управлению доменными именами и IP-адресами (ICANN), которая играет ключевую роль по распределению имен и адресов в сети Интернет. По мнению членов правления ICANN, создание ситуации нестабильности функционирования сети Интернет невозможно[6]. Тем не менее, 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.

---

[4] Эксперты оценили в $21,5 млрд потери России из-за блокировок в Интернете //https://trends.rbc.ru/trends/social/63dd144b9a79475517b0aedf.

[5] Раскрыты последствия отключения России от интернета.Lenta.ru. 26 февраля 2022//https://news.rambler.ru/tech/48208816/?utm_content=news_media&utm_medium=read_more&utm_source=copylinkhttps://news.rambler.ru/tech/48208816/?utm_content=news_media&utm_medium=read_more&utm_source=copylink.

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

Такие меры явно противоречат выработанной позицией стран в заключительном докладе Рабочей группы открытого состава 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[7]. 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 Cogent США заявил об отключении нескольких российских операторов, наиболее известными среди которых являлись VK, Ростелеком, Яндекс, Мегафон[8]. И в марте того же года украинский вице-премьер и министр цифровой трансформации М. Федоров обратился с письмом к корпорации ICANN генеральному директору ICANN Йорану Марби с просьбой отключить корневые серверы DNS в России и отозвать российские домены, такие как .ru, .рф и .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[9]. В то же время говорилось, что Исполнительный совет также выражает солидарность с теми операторами, на

---

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

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

[9] Htps://www.ripe.net/ripe/mail/archives/ripe-list/2022-March/002462.html.

которых лежит трудная задача поддержания доступа в Интернет для оказания помощи людям, страдающим от ужасных последствий вооруженных конфликтов и войн[10]. 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»[11]. В то же время следует отметить, что отрицательный ответ украинскому вице-премьеру и министру цифровой трансформации М. Федорову вызвал критику со стороны ряда официальных лиц Украины и стран северо-атлантического альянса[12]. И сам факт того, что данный вопрос стал предметом обсуждения, не может гарантировать устойчивость политики ICANN в предоставлении равного доступа к ресурсам сети.

Серьезные опасения бесперебойного функционирования Сети вызывает размещение критически важной для безопасности российского сегмента сети Интернет инфраструктуры в виде корневых серверов Интернета вне зоны российской юрисдикции. Десять из тринадцати основных корневых серверов системы доменных имен, обеспечивающих функционирование доменов верхнего уровня, расположены в США, три в Амстердаме, Стокгольме и Токио, и ни один из них в России. Кроме того, некоммерческая организация по управлению доменными именами и IP-адресами (ICANN), играющая ключевую роль по распределению имен и адресов в сети Интернет, зарегистрирована в Калифорнии (США), что позволило сделать вывод о подконтрольности сети Интернет США[13].

---

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

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

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

[13] Сандип Джоши (Sandeep Joshi) «Индия должна вывести Интернет из-под контроля США» Hindu 7 декабря 2013 г. URL: http://goo.gl/zGPofR.

Несправедливость существующего между странами распределения управления ресурсами, необходимых для обеспечения безопасного и устойчивого функционирования сети Интернет, была отмечена в п. 19 Указа Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности РФ» (далее — Доктрина информационной безопасности)[14].

Значимость постановки вопросов относительно форм и методов управления киберпространством проявляется не только в выработке принципов устойчивого функционирования глобальной Сети, но и в том, что такого рода вопросы являются основой концептуального осмысления юрисдикции и суверенитета государств в киберпространстве.

3. Международные документы о принципах управления киберпространства

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. 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. В Декларации напрямую не названы порицаемые государства, очевидно, что под ними подразумеваются Россия, КНДР, Китай, Иран.

[14] Указ Президента от 5 декабря 2016 г. № 646 «Доктрина информационной безопасности» // СЗ РФ. 2016. № 50. Ст. 7074.

Более радикальные формулировки были включены в Стратегию национальной кибербезопасности США 2018 г. [15] . 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[16].

В Стратегии 2018 г. в отличие от совместной Декларации о будущем Интернета 2022 г. были четко стигматизируются страны, обозначаемые в Декларации в качестве непоименованных конкурентов и противников, а именно: Россия, Иран, Северная Корея и Китай. Данные 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[17].

Следует отметить, что Россия и Китай также сформулировали общее концептуальное видение принципов функционирования информационно-

---

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

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

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

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 готовности углубления сотрудничества в сфере международной информационной безопасности и построения открытой, безопасной, устойчивой доступной ИКТ-среды, в заявлении также говорится о применении к информационному пространству 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. Курс на многостороннее, равноправное и прозрачное управление Интернетом был также подтвержден и на состоявшейся 21 марта 2023 года встрече Владимира Путина и Си Цзиньпина.

Провозглашенный в Заявлении суверенитет в отношении национальных сегментов сети «Интернет» требует пояснения, поскольку сфера проявления суверенитета в киберпространстве ни в одном нормативно-правовом акте не определена в силу неясности границ киберпространства. В этой связи внетерриториальный характер киберпространства обнаруживает ряд негативных явлений в виде возникновения потенциальной угрозы государственному суверенитету, построенному на таких традиционных признаках, как власть и территория.

Отсутствие механизмов, позволяющих устанавливать суверенные полномочия государства в киберпространстве, влечет сложности реализации государственной юрисдикции в данной области. Установление суверенитета и юрисдикции государства в отношении технического компонента киберпространства, физически находящегося на территории соответствующего государства, не вызывает сомнений, учитывая

территориальную природу суверенитета и юрисдикции государства. Между тем, киберпространство невозможно представить себе исключительно в виде физических объектов (компьютеры, серверы, маршрутизаторы, оптоволоконные кабели и т.п.), равно как и компьютерной сети, состоящей из множества компьютерных подсетей по всему миру. Помимо технологической составляющей киберпространство включает в себя множество нематериальных активов, таких как информация и программное обеспечение [18]. Основная функция киберпространства заключается в его виртуальной составляющей, которая представляет собой интерактивную среду взаимодействия широкого круга участников. Ввиду этого более целесообразным представляется определение суверенитета в киберпространстве, контуры которого должны быть установлены не только в отношении технического компонента сетевой инфраструктуры, поддерживающей бесперебойное функционирование сети, но и в отношении виртуальной составляющей киберпространства. А в этих целях необходимо сформулировать определение киберпространства, содержательное наполнение которого должно осуществляться путем конвергенции технологических и социальных подходов.

4. Понятие киберпространства

Зачастую в национальных и международных документах Интернет 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 являться и не являться

[18] 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. (дата обращения 12.01.2022).

частью Интернета[19]. Так кибернетическое пространство создают и обычные компьютерные сети внутри предприятия («экстранет»), а также виртуальные сети, которые предназначены для соединения частных сетей различных компаний между собой («интранет»). Кроме того, киберпространство охватывает не только Интернет, но и важнейшую инфраструктуру, поддерживающую современное общество, такую как электрические сети, системы водоснабжения, банковские операции, транспортные системы и т.п.

Сеть Интернет, создаваемая путем соединения небольших сетей компьютеров и серверов, представляет собой один из доступов к киберпространству, транспорт к нему.

В силу того, что киберпространство включает в себя широкий контур сетей связи, понятие «киберпространство» шире понятия «сеть Интернет» и именно в отношении первого понятия исследуются вопросы управления, суверенитета и юрисдикции государства. В то же время принимая во внимание, что в нормативных актах и доктрине понятие Интернет используется зачастую синонимично понятию киберпространству, следует оговориться, что в данной работе понятию Интернет в контексте толкования соответствующих актов будет придаваться широкий смысл в значении киберпространства.

На международном уровне без уточняющего определения термин «киберпространство» фигурирует в Окинавской хартии 2000 г.[20], Конвенции о преступности в сфере компьютерной информации 2001 г.[21].

Понятие «киберпространство» отсутствует в российском законодательстве, но закреплено в Проекте Концепции стратегии кибербезопасности в РФ [22] . В соответствии с указанным Проектом,

---

[19] 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.

[20] Окинавская Хартия глобального информационного общества от 22 июля 2000 г.// Дипломатический вестник. 2000. № 8. С.52.

[21] Конвенция вступила в силу 1 июля 2004 г. Российская Федерация в Конвенции не участвует.

[22] Проект Концепции Стратегии кибербезопасности РФ //URL: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf.

киберпространство рассматривается как определенный, имеющий четкие границы, элемент информационного пространства, а также в качестве сферы деятельности в информационном пространстве, образованной совокупностью коммуникационных каналов Интернета и других телекоммуникационных сетей, технологической инфраструктуры, обеспечивающей их функционирование, и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства).

Содержательные технологические признаки киберпространства прослеживаются в определении информационной инфраструктуры в Доктрине информационной безопасности 2016 г. в виде физической инфраструктуры (сети связи, объекты информатизации, телекоммуникационные сети, серверы, маршрутизаторы, процессоры, спутники, коммутаторы, кабели и др.), так и в виде нефизических активов (информационные системы и сайты в информационно-телекоммуникационной сети Интернет).

В зарубежных национальных источниках при определении киберпространства также акцентируется внимание на технологической инфраструктуре, а именно операционной области и набору средств, с помощью которых осуществляется хранение, изменение и использование информации**.**

Так, в Директиве Президента США по национальной безопасности 2008 г. киберпространство определено в качестве независимой сети информационной технологической инфраструктуры, включающей в себя Интернет, телекоммуникационные сети, компьютерные системы, встроенные процессы и контроллеры в критических отраслях[23]. В национальной военной стратегии операций в киберпространстве Министерства обороны США 2006 г. киберпространство понимается в качестве области, характеризующейся

[23] National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23)2008//URL:https://fas.org/irp/offdocs/nspd/nspd-54.pdf.

использованием электроники и электромагнитного спектра для хранения, модификации и обмена данными через сетевые системы и связанные с ними физические инфраструктуры [24] . В Таллинском руководстве по международному праву, применимому к кибербезопасности 2013 г. киберпространство также определяется исключительно в технологическом ключе, а именно как «пространство, образованное физическими и нефизическими составляющими и характеризующееся использованием компьютеров и электро-магнитных излучений для хранения, преобразования и обмена информацией с использованием компьютерных сетей» [25] . Под Интернетом в указанном руководстве понимается глобальная компьютерная сеть, состоящая из множества компьютерных сетей, в которой данные передаются с помощью единого набора протоколов[26].

Американская доктрина содержит определения, в которых киберпространство представлено в качестве электронной среды в виде компьютеров и других электронных устройств для хранения, изменения и обмена данными через сетевые системы и связанные с ними физические инфраструктуры [27] . Также киберпространство понимается в качестве операционной области, отличительный и уникальный характер которой обусловлен использованием электроники и электромагнитного спектра в целях создания, хранения, изменения, обмена и использования информации посредством взаимосвязанных систем на базе информационно-коммуникационных технологий и связанных с ним инфраструктур[28].

---

[24] US Department of Defense, The National Military Strategy for Cyberspace Operations. 2006. P. 3//URL:https:hsdl.org.

[25] Shmitt M.N. Tallinn Manual of the International Law Applicable to Cyber Warfare. Cambridge University Press, 2013. P. 25.

[26] Ibid.

[27] Schaap A. J. Cyber Warfare Operations: Development and Use under International Law// Air Force Law Review. 2009. Vol. 64. P.126.

[28] Kuehl D.T. «From Cyberspace to Cyberpower: Defining the Problem» in Cyberpower and National Security 48. Franklin D. Kramer, Stuart H. Starr & Larry K. Wentz, eds. 2009)//URL: https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-02.pdf?ver=2017-06-16-115052-210.

Л. Лессиг рассматривает киберпространство как технологическую среду, которая регулируется совокупностью норм и правил, составляющих некий «кодекс», или «код», который представляет собой программное обеспечение, технологические принципы проектирования архитектуры Интернета, протоколы и стандарты киберпространства[29].

В рамках социального подхода киберпространство определяется как социокультурный фактор, влияющий на становление сетевого общества[30]. Также киберпространство обозначено в качестве метафорической абстракции, которая применяется для описания объектов, широко распространенных в компьютерной сети, например, веб-сайт как «находящийся в киберпространстве», а сетевое общение как «коммуникация в киберпространстве»[31].

В характеристиках, которыми учеными наделяют киберпространство, как правило, отмечается его неделимость, несводимость к границам физического пространства[32], отсутствие однозначной географической определенности, многоуровневая структурированность, трансграничность[33], многомерность и отсутствие протяженности, физических параметров[34]. Также в доктрине говорится и о постоянной подвижности и изменчивости структуры киберпространства ввиду появления и прекращения информационных

---

[29] Lessig L. Code and other Laws of Cyberspace// URL: http://www.archiv.orgcyber.law.harvard.edu/lessigbio (дата обращения 20.10.2023).

[30] Хуторной С.Н. Киберпространство и становление сетевого общества: дисс. … канд. философ. наук. Воронеж. 2003.С.9-10.

[31] Барышев Р.А. Киберпространство и проблема отчуждения: дисс. … канд. философ. наук. М. 2009. С.9-10; Волов А.Г. Философский анализ понятия «киберпространство» //Философские проблемы информационных технологий и киберпространства. 2011. № 2. С. 49-54.

[32] Войниканис Е.А. Право интеллектуальной собственности в цифровую эпоху: парадигма баланса и гибкости. М.: ИД "Юриспруденция", 2013//СПС Гарант.

[33] Касенова М.Б. Правовое регулирование трансграничного функционирования и использования интернета дисс. …докт. юрид. наук. М., 2016. С. 18; Федотов М.А. Конституционные ответы на вызовы киберпространства //Lex Russica. 2016. № 3. С. 164-182.

[34] Ансельмо Э. Л. Киберпространство в международном законодательстве: опровергает ли развитие Интернета принцип территориальности в международном праве?// Экономические стратегии. 2006. №2. С. 24-31.

ресурсов, изменения направления информационных потоков, а также создания новых технологий обработки и передачи информации[35].

Уникальность и феномен киберпространства составляют его глобальный характер, который выражен в универсальности доступа к сети и трансграничной специфики, позволяющей неограниченному количеству пользователей осуществлять взаимодействие, пересекающее государственные границы.

Социальные характеристики киберпространства проявляются прежде всего в том, что данное пространство, будучи одним из элементов информационного пространства, представляет собой социальную среду, функционирование которой поддерживается определенной технологической инфраструктурой. При этом социальные взаимосвязи между различными субъектами права возможны без связи с определенной географической территорией государства.

С позиций определения киберпространства как социального явления выступает М.С. Дашян, который, говоря об Интернете как о социальной структуре, выделяет ряд ее сущностных принципов, а именно конвергенция (смешение традиционных явлений и процессов в рамках одной открытой системы – Интернета); иерархичность, децентрализация, экстерриториальность; демократичность[36]. Интернет, по мнению ученого, образует новое информационное пространство - киберпространство, которое формируется вне пределов реального мира и, соответственно, не может оцениваться посредством физико-химических характеристик[37].

Рассмотрение киберпространства с позиций технических и социальных наук обусловило появление двухчастных и трехчастных определений

---

[35]Бондаренко С.В. Социальная общность киберпространства// Информационное общество. 2002. № 4. С. 61-64; Добринская Д.Е. Киберпространство: территория современной жизни// Вестник Московского Университета. Сер. 18. Социология и политология. 2018. Т. 24. № 1. С. 52-70.

[36] Дашян М.С. Право информационных магистралей (Law of information highways): вопросы правового регулирования в сфере Интернет. М.:Волтерс Клувер, 2007//СПС-Гарант.

[37] Там же.

киберпространства. Так, в определениях зарубежных ученых киберпространство представлено как в физическом, так и виртуальном аспекте [38] . Физическая часть представляет собой миллионы сетевых информационных и коммуникационных технологий, которые создают и активируют киберпространство (компьютеры, серверы, маршрутизаторы, процессоры, спутники, коммутаторы и кабели). Виртуальная часть состоит из электронных соединений и данных, передаваемых между частями его физической инфраструктуры и хранящимися в них [39] . В связи с чем изменение и развитие нового оборудования и программного обеспечения обусловливают изменение киберпространства.

В работе Д. Клементе киберпространство разделено уже на три уровня: физический уровень (оборудование, подводные кабели, маршрутизаторы и коммутационные устройства); логический уровень (программное обеспечение или строки кода, которые позволяет оборудованию функционировать и взаимодействовать); а также социальный уровень (или уровень киберперсонажа, т.е. взаимодействие между онлайн-персонажами, которые представляют людей или, все чаще, машины)[40].

Безусловно, к основной функции киберпространства следует отнести его виртуальную основу, а именно интерактивную среду взаимодействия пользователей по всему миру. При этом указанная основа мобилизована как физическими (телекоммуникационные сети, компьютерные системы, серверы, маршрутизаторы, процессоры, спутники, коммутаторы и кабели),

---

[38] 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.

[39] Ibid.

[40] Clemente D. Cyber Security and Global Interdependence: What Is Critical? The Royal Institute of International Affairs. 2013. P.5//URL: https://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/0213pr_cyber.pdf.

так и нефизическими элементами киберпространства (аппаратные приложения, программное обеспечение и др.).

Коммуникативные и технологические качества киберпространства отражены в международном стандарте *ISO/IEC* 27032: 2012 «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по обеспечению кибербезопасности» (*ISO/IEC* 27032: 2012 *Information technology Security techniques. Guidelines-for cybersecurity*) Международной организации по стандартизации (далее – международный стандарт *ISO/IEC* 27032: 2012). В п. 4.21 международного стандарта под киберпространством понимается комплексная среда, не существующая в физической форме, которая возникает в результате взаимодействия людей, программного обеспечения и удаленных сервисов с использованием информационных и телекоммуникационных технологий[41].

Таким образом, киберпространство можно отнести как к виртуальной коммуникативной среде, так и к определенным электронным носителям, обусловливающим доступ к данной среде.

При определении киберпространства необходимо принимать во внимание и субъектный подход, который обусловлен этимологией термина «киберпространство» (англ. *cyberspace*), который представлен сочетанием двух частей «*cyber*» (префикс «*cyber»* происходит от греческого слова *kybernao/kybernan*, используемого в значении «управлять», «контролировать») [42] и «*space*» («пространство»). Управление киберпространством заключается в координирующих функциях по распределению адресного пространства, эксплуатации корневых серверов, созданию и администрированию системы доменных имен и адресов Интернета и т.п.

---

[41] ISO/IEC 27032: 2012 Information technology Security techniques. Guidelines-for cybersecurity//URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en.

[42] Kuehl D.T. Op.cit.//URL: https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-02.pdf?ver=2017-06-16-115052-210.

В процесс управления киберпространством интегрированы негосударственные организации: Общество Интернета (*Internet Society (ISOC)*), Некоммерческая организация по управлению доменными именами и IP-адресами (*ICANN*) и т. п.; структуры, не являющиеся юридическими лицами: Рабочая группа по проектированию интернета (*Internet Engineering Task Force (IETF);* государства; межправительственные организаци*и*. Широкий круг субъектов, привлеченных в процесс управления Интернетом, обозначен и в рамках заседаний рабочей группы по управлению Интернетом (*the Working Group of Internet Governance, WGIG*) в 2004–2005 гг., в него были включены правительства, частный сектор, гражданское общество, межправительственные и неправительственные международные организации, а также иные форумы[43].

Именно такого рода управление широким кругом заинтересованных сторон (негосударственными организациями, частными лицами, государствами и т.п.) задает определенную специфику киберпространству, которое в отличие от наземного, воздушного, космического и морского пространства, традиционно регулируемого международным правом, не имеет «естественного» (природного) происхождения и является продуктом человеческого творчества. Киберпространство представляет собой искусственную среду для создания, передачи и использования информации. При этом 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

[43] Background Report. The Working Group on Internet Governance. June 2005. World Summit on the Information Society. URL: http://www.itu.int/wsis/wgig/docs/wgig-background-report.pdf..

Таким образом, в целях конвергенции социального, технологического и субъектного подходов киберпространство следует понимать как управляемую широким кругом разноуровневых субъектов (негосударственные организации, частные лица, государства, межправительственные организации и др.) искусственную телекоммуникационную среду реализации общественных отношений, функционирование и поддержание которой осуществляется посредством программно-технической инфраструктуры в виде ее физической части (телекоммуникационные сети, компьютеры, серверы, маршрутизаторы, процессоры, спутники и др.) и нефизической (виртуальной) части (операционные системы, стандарты передачи данных, аппаратные приложения, программное обеспечение и др.).

5. Модель мультистейкхолдеризма

Основа глобального управления киберпространством была заложена на Всемирных встречах по вопросам Интернета в 2003 г. и 2005 г., где были сформулированы принципы глобального управления Интернетом, заключающиеся в участии в процессе управления различных субъектов, в том числе государств, общественных организаций, научного и технического сообщества, и также был создан координационный и консультативный орган - Форум по управлению Интернетом (IGF), ставший координационным и консультативным.

Понятие «управление Интернетом» (Internet governance) был предложен в ходе заседаний рабочей группы по управлению Интернетом (the Working Group of Internet Governance, WGIG) в 2004–2005 гг. [44], под ним понимается процесс, посредством которого принимаются необходимые для управления, координации, администрирования и развития Интернета решения, связанные с принципами, нормами, правилами. При этом

[44] Background Report. The Working Group on Internet Governance. June 2005. World Summit on the Information Society. URL: http://www.itu.int/wsis/wgig/docs/wgig-background-report.pdf..

понимание «управление Интернетом» должно осуществляться в широком контексте, не ограничиваясь только техническим функционированием киберпространством, выработкой технических протоколов и стандартов, но и включать в себя вопросы связанные с правовым, экономическим и социокультурным развитием общества. Так, еще в 2005 г. на втором заседании Оргкомитета Тунисского раунда Саммита в предварительном отчете Рабочей группы было обозначено, что управление Интернет подразумевает более широкий спектр вопросов, чем распределение адресного пространства и администрирование системы доменных имен[45].

В Декларации принципов управления Интернетом, принятой Советом Европы в 2011 г., выделены десять принципов, к которым относятся: права человека, демократия и верховенство права; многосторонняя модель управления; ответственность государств; привлечение интернет-пользователей к процессу принятия решений; универсальность Интернета; целостность Интернета; децентрализованное управление; соблюдение сетевой архитектуры; сетевая открытость; культурное и языковое разнообразие[46].

В исследованиях, посвященных вопросам Интернета, отмечено, что регулирование использования Интернета в каждой стране также является частью процесса управления им[47]. Следует отметить, что понятие «управление киберпространством», принимая во внимание трансграничную природу киберпространства, является, несомненно, более широким по отношению к реализации юрисдикции государств в киберпространстве. Данный факт детерминирован тем, что в процесс управления киберпространством

---

[45] Завершилось второе заседание Рабочей группы ООН по управлению Интернет//https://ifap.ru/pr/2005/050221a.htm. Tunis Agenda for the Information Society. WSIS-05/TUNIS/DOC/6(Rev. 1)-E. (18 November 2005). World Summit on the Information society, 2005.

[46] Geneva Declaration of Principles. Building the Information Society: a Global Challenge in the New Millennium, WSIS, 2003. URL: http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-E.pdf.

[47] Стратегия национального развития и задачи юридической науки: колл. монография по результатам IX Международной научно-практической конференции / В.С. Акимов, М.А. Аливердиева, Р.В. Амелин и др.; под общ. ред. Ю.Л. Васильченко, И.М. Рассолова, С.Г. Чубуковой. Москва, 2016.

интегрированы по большей части негосударственные организации: Общество Интернета (Internet Society (ISOC)), Некоммерческая организация по управлению доменными именами и IP-адресами (ICANN) и т. п.; структуры, не являющиеся юридическими лицами: Рабочая группа по проектированию интернета (Internet Engineering Task Force (IETF)), а также государства и межправительственные организации. Широкий круг субъектов, привлеченных в процесс управления Интернетом, обозначен и в рамках заседаний рабочей группы по управлению Интернетом (the Working Group of Internet Governance, WGIG) в 2004–2005 гг., в него были включены правительства, частный сектор, гражданское общество, межправительственные и неправительственные международные организации, а также иные форумы[48].

Как отмечено М.Б. Касеновой, ориентирование технологической поддержки работы Сети под международный охват предопределяет логику ее управления, а именно существование внешнего, интернационализированного механизма управления[49]. Между тем международный характер не позволяет определить степень участия в данном процессе каждого отдельного государства, а также распределение зон реализации интересов государств и частного сектора в киберпространстве. Участие всех заинтересованных субъектов в международном управлении киберпространством исключительно на условиях равноправия вряд ли вообще может быть реализовано, принимая во внимание, что защита национальных интересов государств в информационной сфере, в том числе киберпространстве, не может быть переложена на частный сектор. Кроме того, несмотря на обозначенный широкий круг субъектов, осуществляющих управление Сетью, следует отметить, что международное управление реализуется исключительно де-факто, а не де-юре, хотя угрозы информационной безопасности детерминирует необходимость принятия решений по предотвращению

[48] Background Report. The Working Group on Internet Governance. June 2005. World Summit on the Information Society. URL: http://www.itu.int/wsis/wgig/docs/wgig-background-report.pdf.
[49] Касенова М. Глобальное управление Интернетом в контексте современного международного права // ИНДЕКС БЕЗОПАСНОСТИ № 1 (104). Т. 19. 2012. С. 45.

ущерба национальным интересам государств в информационной сфере на международном правовом уровне. О необходимости международно-правового регулирования данного процесса заявлено и в Доктрине информационной безопасности, в п. 19 которой отмечены трудности формирования системы международной информационной безопасности, направленной на достижение стратегической стабильности и равноправного стратегического партнерства, ввиду отсутствия международно-правовых норм, регулирующих межгосударственные отношения в информационном пространстве.

В настоящее время проблема влияния государств на глобальное управление Сетью в большей степени сосредоточена на функционировании организации ICANN, имеющей особое значение в сфере управления сетью Интернет.

На протяжении долгого времени на открытых площадках рядом государств неоднократно высказывалась озабоченность о ключевой роли США в управлении сетью Интернет и выдвигались предложения по пересмотру 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. Рабочая группа по проектированию интернета (Internet Engineering Task Force (IETF)) представляет собой структурное подразделение корпорации системы Общества интернета (ISOC) — юридического лица Федерального округа Колумбия США. Штаб-квартира компании Verisign находится в штате Виргиния (США).

Таким образом, 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.

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 между некоммерческой компанией по управлению доменными именами и IP-адресами (*ICANN*) и Национальным управлением информации и связи (*NTIA*), являющимся подразделением Министерства торговли США в 2000 г. [50], управление *ICANN* адресным пространством Интернета (доменными зонами и IP-адресами) осуществлялось через подконтрольную Министерству торговли США структуру *IANA* (Администрация адресного пространства Интернет).

Функционируя в рамках ICANN в качестве его структурного подразделения, IANA отвечала за безотказную трансграничную работу Интернета, координировала присвоение технических параметров протоколов, администрировала файл корневых серверов DNS, управляла доменами верхнего уровня, занималась распределением адресных ресурсов Интернета[51].

Несмотря на то, что инфраструктурой Интернета управляла ICANN, соглашение между ICANN с Министерством торговли США и NTIA было справедливо оценено в доктрине в качестве инструмента, который позволял правительству США легитимизовать свой «надзор» за деятельностью ICANN [52]. Возможность осуществления надзора со стороны США за распределением доменных имен и IP-адресов и, как следствие, фактическое отсутствие многостороннего сотрудничества государств в данной сфере не свидетельствовали о самостоятельности ICANN. В этой связи превалирующая роль США в сфере управления Интернетом и вопрос о

---

[50] URL: http://www.iana.org/assignments/iana-ipv6-specialregistry/iana-ipv6-special-registry.xhtml; 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.

[51] ICANN/U.S. Government Contract for the IANA Functions (effective 1 October 2012) / ICANN, 01.10.2012. URL: http://www.icann.org/en/about/agreements/iana/contract-01oct12-en.pdf.

[52] Касенова М. Трансформация IANA и правовой статус-кво Корпорации Интернета. URL: http://pircenter.org/media/content/files/13/14737440390.pdf.

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) [53] . На проводимых по инициативе ООН Всемирных встречах по вопросам информационного сообщества в Женеве в 2003 г. и в Тунисе в 2005 г. Китай призывал к созданию новой международной организации, Франция выступала за создание межправительственного контроля, осуществляемого группой избранных демократических стран [54] . Руководство Европейского Союза предлагало создание международной организации для регулирования Интернета [55]. Бразилия в ходе совещаний на 48-й конференции ICANN в Буэнос-Айресе высказывала предложение о необходимости отведения главной роли в управлении Интернетом ООН[56].

Сторонники изменения концепции управления сетью Интернет обосновывали несправедливость контроля международного инструмента коммуникации только одним государством тем, что в ряде стран (Россия,

---

[53] Итоговый отчет по стратегии ICANN от 23.05.2014. URL: https://www.icann.org/ru/system/files/files/ig-ecosystem-report-23may14-ru.pdf. 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.

[54] Кукьер К.Н. Кто будет контролировать Интернет // Россия в глобальной политике. 2006. Т. 4. № 1. С. 39–48.

[55] Зиновьева Е.С. Международное управление Интернетом: проблемы, подходы, перспективы // Вестник МГИМО Университета. 2010. № 6 (15). С. 167–174.

[56] Итоговый отчет по стратегии ICANN от 23.05.2014. URL: https://www.icann.org/ru/system/files/files/ig-ecosystem-report-23may14-ru.pdf. 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.

Китай, Индия) пользователей Интернета намного больше, чем в США[57]. В этой связи на 49-ой конференции 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 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[58].

Тем не менее, замена структуры IANA публичной некоммерческой корпорацией PTI не обеспечила принцип децентрализованного управления сетью Интернет. Возможность влияния США на управление сетью Интернет сохраняется и по сей день, поскольку США остается страной регистрации компаний, имеющих ключевые координирующие функции по распределению адресного пространства, эксплуатации корневых серверов, созданию и администрированию системы доменных имен и адресов интернета (Domain Name System).

Еще до изменений 2016 г. попытки глобализации сети Интернет оценивались в научной литературе весьма критически. Отмечалось, что официальная позиция Правительства США не оставляет ни малейшего повода усомниться, что Правительство США продолжит оказывать управляющее административное и регламентирующее воздействие на деятельность ICANN,

---

[57] Mark Grabowski, Obama's Risky Internet Giveaway, Wash. Exam'r (Sept. 26, 2016, 12:03 AM). URL: http://www.washingtonexaminer.com/obamas-risky-internet-giveaway/article/2602802.

[58] Продолжение функций IANA на период 2018 года. URL: https://www.icann.org/news/blog/iana-2018-ru.

прежде всего, в сфере технического обеспечения функционирования системы доменных имен (DNS) [59] , был сделан вывод о недостижимости интернационализации управления Интернетом и передаче контроля в отношении критических элементов инфраструктуры Сети международному сообществу, поскольку предлагаемая институциональная архитектура не отвечает принципу управления Интернетом с участием всех заинтересованных сторон так, как его понимают на Западе[60].

Делегирование ряда функций по управлению сложной сетевой инфраструктурой тем или иным организациям является вполне логичным[61]. Так, например, сетевой провайдер — компания Verisign на основании договора с Национальным управлением информации и связи США (NTIA) выполняет функции Технического менеджера корневой зоны DNS[62]. Следует отметить, что тревогу вызывает не сам принцип распределения функций по управлению сетью Интернет между различными компаниями и корпорациями, а нахождение данных компаний в зоне американской юрисдикции. Доминирующее положение юридических лиц США в трансграничном управлении Интернетом, находящихся под юрисдикцией США либо связанных с юрисдикцией США на договорно-правовом уровне, была отмечена многими авторами (О. Демидов, М.Б. Касенова, А. Стрельцов)[63].

Централизованная координация технического компонента в рамках определенных юрисдикций (разработка и внедрение стандартов

---

[59] Даниленков А.В. Интернет-право. М.: Юстицинформ, 2014 // СПС «Гарант».

[60] Демидов О. Игра про правила. URL: http://www.globalaffairs.ru/number/Igra-pro-pravila-17640.

[61] Ващекина И.В., Ващекин А.Н. Информационный обмен между уровнями иерархий в банковских, промышленных и торговых системах // Научное обозрение. Экономические науки. 2017. № 3. С. 51–59.

[62] VERISIGN. URL: https://www.verisign.com/en_US/company-information/index.xhtml.

[63] Касенова М.Б. «Глобальное сообщество заинтересованных сторон» и перспективы трансграничного управления Интернетом // Право и государство: теория и практика. 2014. № 10 (118). С. 138–143; Стрельцов А. Суверенитет и юрисдикция государства в среде информационно-коммуникационных технологий в контексте международной безопасности // Международная жизнь. 2017. № 2. С. 88–106; Демидов О. Игра про правила. URL: http://www.globalaffairs.ru/number/Igra-pro-pravila-17640.

функционирования Сети, создание новых сервисов, производство сетевого оборудования) не может не вызвать вопросов. Инфраструктура поддержки уникальных идентификаторов Интернета физически сосредоточена в семи странах (США, Австралия, Маврикий, Нидерланды, Уругвай, Швеция и Япония). Именно в юрисдикциях этих стран находятся региональные регистратуры Интернета и операторы корневых серверов сети Интернет[64]. Хотя в самой корпорации отмечено, что ICANN занимается координацией одного технического компонента экосистемы Интернета — имен, номеров и параметров протокола Интернета — и не занимается цензурой в Интернете[65], возможность влияния США на управление сетью Интернет сохраняется и по сей день. 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, содержательной составляющей, принимая во внимание нахождение многочисленных информационно-коммуникационных платформ и сервисов, оказывающих серьезное влияние на информационную политику других стран. Телекоммуникационные корпорации Google, Apple, Facebook, Amazon, Microsoft (GAFAM) занимают лидирующие позиции в мире в качестве поисковых сервисов, социальных сетей, сервисов электронной коммерции и производства операционных систем и образуют экосистему приложений, которая используется как на общественном, так и на государственном уровнях[66].

В п. 53 Стратегии национальной безопасности РФ 2021 г. отмечены негативные тенденции в виде стремления транснациональных корпораций закрепить свое монопольное положение в сети Интернет и контролировать все

---

[64] Медриш М. Высокая передача: кому достался контроль над IANA. URL: http://pircenter.org/articles/2057-vysokaya-peredacha-komu-dostalsya-kontrol-nad-iana.

[65] Шехади Ф. Разъяснение неточностей и заблуждений в отношении объявления США и функций IANA. URL: https://www.icann.org/news/blog/iana-ru-2014-03-20-07-22-02-0700.

[66] Дегтерев Д.А., Рамич М.С., Пискунов Д.А. Подходы США и КНР к глобальному управлению киберпространством: «новая биполярность» в «сетевом обществе»// Вестник международных организаций. 2021. Т.16. №3. С.7-33.

информационные ресурсы путем введения такими корпорациями (при отсутствии законных оснований и вопреки нормам международного права) цензуры и блокировки альтернативных интернет-платформ[67].

Представляет интерес, что в Указе Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности РФ» несмотря на уже принятую концепцию мультистейкхолдеризма в отношении киберпространства распределение между странами ресурсов, необходимых для обеспечения безопасного и устойчивого функционирования сети Интернет, было оценено как не позволяющее реализовать управление данными ресурсами на принципах доверия и справедливости. Кроме того, в 2017 г., когда задача интернационализации сети Интернет посредством установления концепции мультистейкхолдеризма уже была реализована, Президент РФ Владимир Путин поручил профильным Минкомсвязи и МИДу договориться со странами БРИКС о создании независимого от существующего Интернета посредством создания независимой от контроля международных организаций системы корневых серверов доменных имен (DNS) [68] . Необходимость проведения подобных мер обосновывалась тем, что работоспособность Интернета зависит главным образом от международной некоммерческой корпорации по распределению имен и адресов ICANN, а сама организация находится в юрисдикции США.

В этой связи следует заключить, что процесс интернационализации управления Интернетом можно признать несостоятельным. Сохранение ICANN, ключевых координирующих функций по распределению адресного пространства, эксплуатации корневых серверов, созданию и администрированию системы доменных имен и адресов интернета (Domain Name System) позволяет сделать вывод, что управление сетью Интернет

---

[67] Указ Президента РФ от 2.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации»//СЗ РФ. 2021. №27(ч.II). Ст. 5351.

[68] Советник Путина пообещал россиянам незаметное отключение от мирового интернета. URL: https://www.finanz.ru/novosti/aktsii/Covetnik-putina-poobeshchal-rossiyanam-nezametnoe-otklyuchenie-ot-mirovogo-interneta-1018615540.

фактически сохраняется за США как страной регистрации соответствующей компании. Обладая доступом к управлению критическими ресурсами сети Интернет, США получают власть в создании и определении правил включения и других стандартов сети Интернет[69].

Таким образом, установленная концепция мультистейкхолдеризма не снимает проблемы контроля США за инфраструктурой сети Интернет. Факт регулирования отношений в киберсреде специализированными некоммерческими организациями, зарегистрированными на территории США, позволяет признавать процесс международного управления глобальной Сетью в большей степени де-факто, но не де-юре. Кроме того, международное управление сетью Интернет на условиях равноправного участия всех заинтересованных субъектов вообще вряд ли может быть реализовано, принимая во внимание, что Сеть является сферой реализации как частных, так и публично-правовых интересов, в число которых входят такие ключевые интересы государств, как предотвращение угроз информационной безопасности. Учитывая, что данные вопросы являются предметом обсуждения преимущественно субъектами международного публичного права, международное управление Сетью требует распределения зон реализации интересов и ответственности между субъектами публичного и частного права.

6. Модель многостороннего управления

Антагонистом модели мультистейкхолдеризма выступает модель многостороннего управления киберпространством, в рамках которой также предлагается управлять киберпространством с учетом интересов всех заинтересованных лиц, включая бизнес и представителей интернет-

[69] Дегтерев Д.А., Рамич М.С., Пискунов Д.А. Подходы США и КНР к глобальному управлению киберпространством: «новая
биполярность» в «сетевом обществе»// Вестник международных организаций. 2021. Т.16. №3. С.

сообщества. Но существенным отличием последней модели является то, что ключевую роль в многостороннем управлении играют государства. В рамках данной модели особую значимость приобретают вопросы установления государственного суверенитета в киберпространстве и защиты национальной критической инфраструктуры. 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 процессе 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 Шанхайской организации сотрудничества, 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 [70]. Государства ШОС выступили за выработку универсальных правил, принципов и норм ответственного поведения [71] государств в информационном пространстве и

[70] Бишкекская декларация Совета глав государств – членов Шанхайской организации сотрудничества 14 июня 2019 года// http://www.kremlin.ru/supplement/5421.

[71] Bitros G.C., Kyriazis N.C. Democracy and an Open-Economy World Order. Springer International Publishing AG 2017. P.29.

обязались активно сотрудничать в данной области в целях обеспечения информационной безопасности 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. Было отмечено, что тенденция суверенизации Интернета может привести к его фрагментации или балканизации. Также были высказаны опасения непринятия норм, регулирующих отношения в киберпространстве, интернет-сообществом, если представители указанного сообщества не принимали участие в их разработке[72].

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.

На сайте корпорации ICANN отмечено, что ключевым фактором успешных усилий по управлению Интернетом в долгосрочной перспективе обеспечивается сложным равновесием различных сил и поддержанием эффективной экосистемы сотрудничества[73]. При этом, отмечается на сайте, в этой экосистеме сама корпорация ICANN играет «небольшую, но крайне важную роль», касающуюся системы уникальных идентификаторов Интернета.

Несмотря на внешнюю привлекательность идеи равного участия, достижение устойчивого равновесия между разнородного состава стейкхолдеров, степень вовлеченность которых в процесс управления различен, предоставляется практически невозможным. Функционирование организации на принципе исключительно горизонтальных связей

---

[72] Bitros G.C., Kyriazis N.C. Democracy and an Open-Economy World Order. Springer International Publishing AG 2017. P.29.

[73] Управление Интернетом// https://www.icann.org/resources/pages/internet-governance-2013-06-14-ru.

заинтересованных участников вне вертикального построения управления, для которого характерно принятие решений, практически неосуществимо.

На сегодняшний день возможность участия государств в управлении сетью по модели мультистейкхолдеризма является фактически номинальной. Весьма вероятно, что именно этим объясняется противоречивая характеристика роли ICANN, представленная на сайте данной организации, выраженная антономичным оксюмороном в виде прилагательных «небольшой» и «крайне важной».

Кроме того, закономерен вопрос, даже без учета текущей напряженной политической обстановки насколько вообще возможно равноправное участие всех вовлеченных в процесс управления субъектов, принимая во внимание 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 и т.п. Справедливости ради следует здесь 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 сети Интернет с целью накопления и использования опыта частного сектора при формировании государственной информационной политики. Но формальную, ключевую роль в данном процессе, безусловно должны играть государства. Как было отмечено заместителем постоянного представителя РФ 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 годах, «…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»[74].

Что касается аргумента о неспособности государств успешно заниматься управлением сети Интернет без участия бизнеса и общественного сектора, то в рамках международных организаций создаются открытые инклюзивные площадки, где проводятся обсуждения по вопросам управления киберпространства. 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 ООН обсуждение строится на открытой площадке широким кругом субъектов, включая и представителей заинтересованных неправительственных организаций, частного сектора.

В докладе Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности ООН (РГОС) 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[75].

В настоящий момент возможность участия государств в управлении сетью по модели мультистейкхолдеризма обусловлена тем, что в Правлении ICANN участвует также представитель GAC – правительственного

---

[74] Полянский указал на право государств отвечать за кибербезопасность//Известия. 25 июля 2022// https://iz.ru/1370207/2022-07-25/polianskii-ukazal-na-pravo-gosudarstv-otvechat-za-kiberbezopasnost.

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

консультативного совета, который представляет интересы правительств и межправительственных организаций.

Наличие правительственного консультативного совета 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 В. Макарова - члена экспертного совета при Министерстве цифрового развития о доминировании США при управлении сетью Интернет в ходе дискуссии 28 апреля 2021 г.[76].

В отчете ICANN 2022 г. было указано, что Интернет, не является исключительно американским, поскольку Устав ICANN запрещает более пяти директоров одного и того же географического региона, также ICANN уже несет ответственность перед всем мировым сообществом ICANN, включая 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 4 февраля 2022 г.

Тезис об ответственности ICANN правительственному консультативному комитету вступает в противоречие с Уставом ICANN, в соответствии с которым GAC дает только рекомендации и в случае расхождения с действиями Правления, от Правления требуется обосновать

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

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.

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

По мнению авторов отчета ICANN, место нахождение 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 четырех[77]. Данный тезис спорен. Функции корневых серверов являются ключевыми, поскольку для бесперебойного функционирования Интернета необходим так называемый пиринг – обмен данными провайдерами первого уровня, 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 адреса того или иного сайта. В РФ не находится ни одного корневого сервера, 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

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

создание резервных серверов 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.

Такие меры явно противоречат выработанной позицией стран в заключительном докладе Рабочей группы открытого состава 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 [78]. 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.

В этой связи хотя США и принадлежит к кругу стран, поддерживающих концепцию мультистейкхолдеризма, реальное положение вещей свидетельствует, что в рамках данной модели США имеют преимущественное положение, которое позволяет реализовывать свои правила в киберпространстве, что, в свою очередь, явно не отражает принципа равного участия в управлении. Отказ от принципа равного участия в управлении киберпространством прослеживается и в приведенной выше Стратегии

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

национальной кибербезопасности США 2018 г., в которой постулируется необходимость сохранения превосходства США в киберпространстве[79].

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 чем монопольное сосредоточение ресурсов для бесперебойного функционирования сети в пределах одного государства или небольшой группы государств 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 влияния[80]. В связи с указанным 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

[79] National Cyber Strategy of the United States of America 2018// https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.
[80] https://www.cfr.org/report/confronting-reality-in-cyberspace

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. [81].

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 не допущении заведомого использования территории государств для совершения международно-противоправных деяний с использованием ИКТ; об ответственном представлении информации о факторах уязвимости в сфере ИКТ и т.п.

Следует отметить, что впервые «нет международной информационной войне» сформулировала Россия в 1998 г., когда в Генеральную Ассамблею 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 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 [82] . Также в

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

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

Резолюции была отмечена 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[83]. 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 ООН (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 ООН и Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (РГОС). В рамках ГПЭ на основе консенсуса были приняты четыре доклада (от 2010, 2013, 2015 и 2021 годов), в которых были рекомендованы правила ответственного поведения государств в киберпространстве в контексте международной безопасности.

В резолюции 70/237 Генеральная Ассамблея призвала государства-члены при использовании ИКТ руководствоваться докладом Группы правительственных экспертов 2015 года, в котором содержится 11 добровольных, не имеющих обязательной силы норм ответственного поведения государств[84]. В число норм входили обязательства государств сотрудничать в разработке и осуществлении мер по укреплению стабильности и безопасности в использовании ИКТ и предупреждению совершения

---

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

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

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 Интернете (прав на неприкосновенность личной жизни в эпоху цифровых технологий, право свободно выражать свое мнение); не поддерживать деятельность в сфере ИКТ, если такая деятельность противоречит его 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 т.д.

В докладах ГПЭ говорилось 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.

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 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)[85].

Как было отмечено, в отличие от ГПЭ ООН в рамках РГОС ООН обсуждение строится на открытой площадке широким кругом субъектов, включая и представителей заинтересованных неправительственных организаций, 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.

3 ноября 2021 г. на заседании Первого комитета Генеральной Ассамблеи была принята резолюция A/C.1/76/L.13, совместный проект которой внесли Россия и США [86]. В Резолюции были отмечены принятие заключительного доклада РГОС по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности[87], а также были отмечены усилия ГПЭ ООН по подготовке заключительного доклада по поощрению ответственного поведения государств в контексте международной безопасности[88].

Принятие данной Резолюции и сам доклад РГОС 2021 г. был оценен 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, предотвращения конфликтов в информационной сфере, недопущение его милитаризации, и

---

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

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

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

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

использование ИКТ исключительно в мирных целях[89]. Следующим шагом прогнозировалось подготовка Конвенции о противодействии использования ИКТ в преступных целях для придания данным правилам обязательного характера.

В июле 2022 г. в штаб-квартире ООН в Нью-Йорке открылась новая сессия Рабочей группы открытого состава (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. Постулирование 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 или БРИКС, где,

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

координируя свою деятельность с ООН, можно было бы предложить более конкретные механизмы и инструменты по достижению тех задач, которые были сформулированы РГОС и ГПЭ.

При этом понимание управление Интернетом должно осуществляться в широком контексте, не ограничиваясь только техническим функционированием киберпространством, выработкой технических протоколов и стандартов, но и включать в себя вопросы связанные с правовым, экономическим и социокультурным развитием общества. Так еще в 2005 г. на втором заседании Оргкомитета Тунисского раунда Саммита в предварительном отчете Рабочей группы было обозначено, что управление Интернет подразумевает более широкий спектр вопросов, чем распределение адресного пространства и администрирование системы доменных имен[90].

Если нормативное понимание суверенитета имеет презумптивный характер и может не совпадать с текущими возможностями государства по реализации государственной политики, то иначе обстоит дело с концепцией управления киберпространством, которая имеет реальное содержание. На сегодняшний день управление фактически сосредоточено в руках корпораций, находящихся в зоне юрисдикции США. Взаимозависимость концепций суверенитета и управления проявляется в том, что установление суверенитета в отношении киберпространства возможно только в отношении контролируемого государством пространства. Именно поэтому зачастую вопросы управления и суверенитета поднимаются специалистами синхронно.

Интересная полемика относительно суверенитета и концепций управления киберпространством сложилась между старшим советником Китайского международного института стратегического развития Хао Ели (Hao Yeli), автора многочисленных работ по вопросам регулирования

---

[90] Завершилось второе заседание Рабочей группы ООН по управлению Интернет//https://ifap.ru/pr/2005/050221a.htm. Tunis Agenda for the Information Society. WSIS-05/TUNIS/DOC/6(Rev. 1)-E. (18 November 2005). World Summit on the Information society, 2005.

отношений в киберпространстве и обеспечению национальной кибербезопасности, и американскими специалистами по кибербезопасности. В открытом письме Хао Ели была предложена теория трех перспектив, в соответствии с которой успешность правового регулирования отношений в киберпространстве, которое автор разделяет на три уровня: инфраструктуру, приложение и ядро, достигается при равном учете интересов государства, гражданина и международного сообщества[91].

Согласованность интересов международного сообщества и государства автор видит в передаче государством некоторой части своего национального суверенитета, что способствует культурному обмену, экономическому сотрудничеству и кибербезопасности. Так, в отношении нижнего уровня киберпространства - физическая и техническая инфраструктура - по мнению автора, суверенитет может быть передан международному сообществу в целях установления единого международного стандарта взаимодействия; средний уровень - приложения, интернет-платформы должен управляться на основе многостороннего совместного управления с участием многих заинтересованных сторон, а также баланса между свободой и порядком; верхний уровень, составляющий ядро киберпространства, к которому автор относит законодательство, политическую безопасность и идеологию, отнесен к прерогативе национальных государств. Предложение дифференцированного управления Интернетом было озвучено еще в 2003 г. в п. 49 Декларации принципов Построения информационного общества, где полномочия по связанным с Интернет вопросам государственной политики (в т.ч. вопросы государственной политики международного уровня) были отнесены к суверенному праву государств и межправительственным организациям; частному сектору была отведена роль в развитии Интернет, как в технической, так и в экономической сфере; международные организации должны

[91] A Three-Perspective Theory of Cyber Sovereignty by Rtd. Major General Hao Yeli// https://www.belfercenter.org/publication/governing-cyberspace-state-control-vs-multistakeholder-model.

разрабатывать относящиеся к Интернет технические стандарты и соответствующие политики[92].

Сама передача суверенитета международному сообществу вызывает определенные вопросы. Как справедливо отмечено А.Я. Капустиным, международное сообщество не представляет собой суверенное объединение государств и сам факт суверенитета государств не дает ни малейших оснований предполагать, что качество суверенитета может появиться также у неформального их объединения [93] . Если имеется в виду передача определенных полномочий по управлению киберпространством на основе международного договора международной организации, то такого рода инициативы были сформулированы давно, начиная с момента создания механизма распределения адресного пространства в сети Интернет, в связи с обеспокоенностью превалирующей ролью США в сфере управления Интернетом. Таким же спорным выглядит тезис Хао Ели о выделении отдельного уровня, составляющего ядро киберпространства, к которому автор относит законодательство, политическую безопасность и идеологию. Отношения в рамках функционирования киберпространства на любом уровне не может быть освобождено от законодательства соответствующего государства, в связи с чем выделение области национальной безопасности, политики и законодательства в отдельный самостоятельный уровень практически невозможно.

Справедливо отмечено в работе Н.А. Истомина, который, цитируя п. 49 Декларации принципов Построения информационного общества [94] , где разграничиваются вопросы государственной политики, касающейся

---

[92] Декларация принципов Построение информационного общества – глобальная задача в новом тысячелетии. Документ WSIS-03/GENEVA/DOC/4-R 12 декабря 2003 года. https://www.un.org/ru/events/pastevents/pdf/dec_wsis.pdf.

[93] Капустин А.И. Суверенитет государства в киберпространстве: международно-правовое измерение // Журнал зарубежного законодательства и сравнительного правоведения. 2022. № 6. С.99-108.

[94] Декларация принципов Построение информационного общества – глобальная задача в новом тысячелетии. Документ WSIS-03/GENEVA/DOC/4-R 12 декабря 2003 года. https://www.un.org/ru/events/pastevents/pdf/dec_wsis.pdf.

Интернета, и вопросы «повседневной деятельности технического и эксплуатационного характера», ставит под сомнение возможность разграничения между вопросами государственной политики и сугубо техническими аспектами [95] . Автором отмечается, что в управлении Интернетом нет таких вопросов, которые нельзя было бы отнести прямо или косвенно к публичной политике и которые не могли бы стать объектом государственного регулирования, а значит государства всегда в той или иной степени будут участвовать во всех аспектах управления Интернетом [96].

Именно поэтому в целях эффективного и устойчивого управления киберпространством должны быть разработаны и приняты дополнительные меры по усилению государственного контроля в отношении информационного пространства. Провозглашаемая рядом стран, преимущественно входящих в ШОС, концепция установления суверенитета в киберпространстве может быть выстроена только в отношении контролируемого государством пространства на основе модели многостороннего управления, в рамках которой решающая роль в управлении отводится государством. При этом управление киберпространством не может быть лимитировано ограниченным кругом вопросов будь то вопросы государственной политики или разработки технических стандартов, политик, протоколов, принимая во внимание условность подобного разделения и имманентную взаимосвязь указанных вопросов.

[95] Истомин Н.А. Модель участия заинтересованных сторон в управлении Интернетом на международном уровне // Право и политика. 2020. № 5. С. 90 - 109.
[96] Там же. С. 90 - 109.