# Управление Интернетом: системные диспропорции и пути их разрешения[1, 2]

*С.А. Васильковский, А.А. Игнатов*

**Васильковский Сергей Алексеевич** – н.с. Центра исследований международных институтов Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации (ЦИМИ РАНХиГС); Российская Федерация, 119034, Москва, Пречистенская наб., 11, оф. 403; E-mail: vasilkovskiy-sa@ranepa.ru

**Игнатов Александр Александрович** – аспирант МГИМО, м.н.с. Центра исследований международных институтов Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации (ЦИМИ РАНХиГС); Российская Федерация, 119034, Москва, Пречистенская наб., 11, оф. 403; E-mail: ignatov-aa@ranepa.ru

*Распространение цифровых технологий приводит к массовой цифровизации всех видов общественных отношений. Формирующаяся в ходе данного процесса цифровая экономика становится ведущим фактором мирового экономического роста и критерием развитости государства. Основой цифровой экономики является Интернет, обеспечивающий функционирование новых моделей бизнеса, форм социального взаимодействия, инновационного производства, общественной дипломатии. Система управления Интернетом отличается от иных современных международных систем общественно-политических отношений тем, что ведущую роль в ней играют негосударственные организации, в частности, Корпорация по присвоению доменных имен (ICANN) и Общество Интернета (ISOC), а деятельность государств существенно ограничена базовыми свойствами системы, что затрудняет реализацию цифрового суверенитета государства. Цель настоящей статьи заключается в определении способов сглаживания данного несоответствия.*

*Анализируя современное состояние системы управления Интернетом, авторы статьи определяют ее ключевые характеристики, обуславливающие конфликтогенность системы. К ним относятся децентрализованность, недостаточный оценочный уровень подотчетности и легитимности. Авторы анализируют инструментарий ICANN и ISOC и выделяют среди них ключевые инструменты, которые фактически закрепляют за организациями статус центральных в системе управления Интернетом. В заключительной части представлены рекомендации авторов статьи относительно действий международного сообщества для смягчения выявленных диспропорций.*

**Ключевые слова:** цифровые технологии; цифровая экономика; цифровой суверенитет; Интернет; управление Интернетом; кибервласть; ICANN; ISOC

**Для цитирования:** Васильковский С.А., Игнатов А.А. (2020) Управление Интернетом: системные диспропорции и пути их разрешения // Вестник международных организаций. Т. 15. № 4. С. 7–29 (на русском и английском языках). DOI: 10.17323/1996-7845-2020-04-01

[1] Статья поступила в редакцию в августе 2020 г.

[2] Статья подготовлена в рамках выполнения научно-исследовательской работы государственного задания РАНХиГС.

## Введение

Стремительное развитие *цифровой экономики* и Интернета как ее основного компонента [Бухт, Хикс, 2018, p. 148–151] в последние десятилетия привело к трансформации всех сфер общественной жизни. Недавние успехи в развитии экономической деятельности на базе Интернета существенно повысили его значимость в качестве фактора производства в различных отраслях (см., например, [Джан, Чен, 2019; Kaila, Tarp, 2019; Shiroma et al., 2019; Korchagin et al., 2019; Pozdnyakova et al., 2019]). Многократное увеличение пропускной способности *цифровой инфраструктуры*[3] позволило существенно нарастить объемы цифровой торговли: по итогам 2017 г. совокупный объем проданных при помощи инструментов электронной торговли товаров и услуг достиг 29 трлн долл. США [UNCTAD, 2019, p. 15]. В итоге *цифровая экономика*, или, как ее справедливо называют в некоторых источниках, *интернет-экономика*, в настоящее время составляет порядка 22% мировой экономики, и этот показатель продолжает расти [Бухт, Хикс, 2018, p. 158].

В то же время Интернет является потенциальным источником угроз, связанных с обеспечением безопасности. Согласно тексту Директивы Европейского союза (ЕС) по сетевой и информационной безопасности, безопасность информационных сетей, основной из которых является Интернет, играет определяющую роль в обеспечении трансграничных перемещений товаров, услуг и граждан и, следовательно, является основополагающим элементом обеспечения бесперебойной работы внутреннего рынка [Европейский союз, 2016, para 3].

Таким образом, современный Интернет представляет собой арену столкновения разнородных интересов и акторов. При этом возможности влияния государств, которые остаются важнейшими субъектами международных отношений и мировой политики, на процесс принятия решений в сфере управления Интернетом существенно ограничены [Liaropoulos, 2013; Nye, 2014; Haugen, 2020]. В то же время для системы управления Интернетом характерен недостаточный оценочный уровень подотчетности ключевых негосударственных акторов, занимающих доминирующее положение в данной области глобального управления, что снижает *легитимность* системы в целом и подрывает доверие к принимаемым решениям [Keohane, 2011; Haugen, 2020]. Отдельные работы указывают на необходимость более предметного участия государств в управлении Интернетом, например, в вопросах, касающихся защиты прав человека и гражданина [Zalnieriute, Milan, 2019].

В среде, базовые характеристики которой создают предпосылки для возникновения различных угроз, государства стремятся максимизировать свое влияние на принятие решений по вопросам управления Интернетом. Данная задача является актуальной и для России: действующая Доктрина информационной безопасности Российской Федерации направлена, в частности, на *«продвижение в рамках деятельности международных организаций позиции Российской Федерации, предусматривающей обеспечение равноправного и взаимовыгодного сотрудничества всех заинтересованных сторон в информационной сфере»* [Правительство РФ, 2016].

Указанные диспропорции являются неотъемлемой характеристикой системы управления Интернетом на современном этапе. Цель настоящей статьи заключается в поиске путей разрешения данных противоречий.

---

[3] Наиболее распространенное определение данного понятия было предложено ОЭСР: «*<Цифровая инфраструктура – это> эффективные, надежные и широкодоступные сети широкополосной связи и услуги, программное обеспечение и комплектующие, на которых основывается цифровая экономика*» [OECD, 2017, p. 28]. Только за последнее десятилетие пропускная способность трансграничных сетей передачи данных выросла в 45 раз [Nye, 2017], а количество устройств, использующих технологию интернета вещей (Internet of Things), вскоре должно превысить 20 млрд [Naughton, 2016].

Статья состоит из трех частей. В первой части авторы рассматривают основные характеристики системы управления Интернетом, обуславливающие возникновение конфликта между ограниченностью государственного суверенитета и недостаточной легитимностью деятельности негосударственных акторов. Во второй части авторы анализируют особенности деятельности ICANN и ISOC как основных негосударственных организаций в системе управления Интернетом и характеризуют их деятельность с точки зрения наличия системных противоречий. В третьей части предложены рекомендации авторов статьи относительно возможных путей сглаживания выявленных противоречий.

## О базовых характеристиках и роли государств в управлении Интернетом

Управление Интернетом – исключительно сложный процесс, поскольку *«Интернет по определению является комплексной системой, которая не управляется некой отдельной организацией»* [Van Horenbeeck, 2018, p. 6]. Краткий обзор истории возникновения и развития Интернета позволяет уже на раннем этапе определить некоторые противоречия, характеризующие данную систему в настоящее время.

Прообразом современного Интернета принято считать созданную в США в конце 1960-х годов систему ARPANET (Advanced Research Project Agency Network). Системы, подобные ARPANET, развивались в то время и в других странах, но именно американский проект можно считать предтечей Интернета [Paloque-Berges, Schafer, 2019, p. 4].

Первым спонсором ARPANET стало Агентство по перспективным исследованиям Министерства обороны США. Данная система создавалась для обеспечения доступа к удаленным компьютерам по всей стране. Именно в рамках ARPANET были впервые апробированы технологии, которые впоследствии определили особенности работы современного Интернета, в частности, технология маршрутизации данных и первая версия протокола Интернета. В 1986 г. прежними участниками проекта ARPANET был создан Инженерный совет Интернета (IETF)[4] – первая открытая профессиональная организация, поставившая целью развитие сетевых технологий. Проект ARPANET был свернут в 1990 г. в связи с пересмотром бюджетной политики Министерства обороны США.

Начиная с 1990-х годов количество пользователей Интернета возрастало стремительными темпами и уже в 2006 г. превысило отметку 1 млрд по статистике Международного союза электросвязи (МСЭ). Определяющими факторами распространения Интернета стали удешевление персональных компьютеров и развитие соответствующей инфраструктуры связи по всему миру.

Рост значимости Интернета побудил мировое сообщество приступить в начале 2000-х годов к выработке консенсуса по базовым характеристикам развития и управления глобальной информационной сети. Основные принципы были закреплены в Декларации, принятой в ходе работы Всемирной встречи на высшем уровне по вопросам информационного общества в 2003–2005 гг. Декларация содержит указание на необходимость поддержания «сотрудничества и партнерских отношений между всеми заинтересованными сторонами» [ООН, 2003, para 20], под которыми подразумеваются органы государственного управления, частный сектор, гражданское общество, Организация Объединенных Наций и другие международные организации. Отмечая, что

[4] Не следует путать с Рабочей группой проектирования Интернета (IETF). Инженерный совет Интернета был реорганизован и в настоящее время носит название Совет по архитектуре Интернета (IAB) и входит в «семью» организаций Общества Интернета.

«управление использованием Интернета охватывает как технические вопросы, так и вопросы государственной политики» [ООН, 2003, para 49], Декларация возлагает на все вовлеченные стороны обязанности по развитию технических и экономических аспектов функционирования Интернета, а в отношении государств уточняет следующее:

*«Политические полномочия по связанным с Интернет вопросам государственной политики являются суверенным правом государств. Государства имеют права и обязанности в отношении связанных с Интернет вопросов государственной политики международного уровня»* [Ibid., para 49 (a)].

Многообразие акторов, принимающих участие в регулировании Интернета, обуславливает сложность взаимодействия между ними и невозможность выделения в этой системе единого центра. Джозеф Най (Joseph S. Nye) характеризует систему управления Интернетом как *комплексный режим*, охватывающий взаимодействие вовлеченных акторов на *физическом* и *информационном* уровне. Управление Интернетом также является компонентом более сложного режима управления *киберпространством*[5] [Nye, 2014]. Государства, «гнездящиеся среди других субъектов управления <Интернетом>» [Scholte, 2017, p. 166], ведут деятельность преимущественно на *физическом уровне*, тогда как частные компании и международные организации в основном действуют на *информационном уровне*. На этом же уровне возникают и главные *угрозы*, появляющиеся по мере развития Интернета, при этом действия злоумышленников в информационном пространстве могут наносить несоизмеримо высокий ущерб на физическом уровне, *«где ресурсы ограничены и имеют высокую цену»* [Nye, 2014, p. 5].

Управление киберпространством как некой *новой реальностью* предполагает наличие принципиально иных инструментов реализации влияния. На фоне активного внедрения цифровых технологий в общественно-политические реалии повышается роль *кибервласти*[6], круг полноценных обладателей которой теперь не ограничивается национальными государствами. Рождаемая данным явлением асимметрия приводит к перераспределению сил на международное арене [Nye, 2010].

Монополия государств на обладание и реализацию традиционной *власти* вовсе не предопределяет их лидерство в *киберпространстве*. Относительно низкие издержки входа на рынок, анонимность пользователей и асимметрия уязвимостей означают, что новые акторы имеют больше возможностей для применения «жесткой» и «мягкой» силы в киберпространстве, чем в иных областях международной политики. Основной проблемой здесь является несоразмерность мощи национальных государств, обусловленной их традиционной ролью в международных делах и весьма ограниченными возможностями контроля киберпространства.

Высокие издержки ведения государствами деятельности на *информационном уровне* обуславливают доминирование в нем негосударственных акторов. Наряду с прочими компонентами немаловажными элементами информационной компоненты системы управления Интернетом являются его *адресная система* и *технические стандарты*, единообразно применяемые на всем пространстве всемирной сети. Без них существование Интернета не представляется возможным. Первый аспект находится в ведении Корпорации по присвоению доменных имен (ICANN), а разработкой и утверждением *стандартов Интернета* занимаются организации под управлением Общества Интернета (Internet Society, ISOC) (рис. 1).

---

[5] «<Киберпространство – это> глобальная область мировой информационной среды, состоящая из взаимосвязанных сетей ИКТ-инфраструктур, включая Интернет, сетей телекоммуникации, компьютерных систем, а также вычислительных и регулирующих устройств» [Franzese, 2009, p. 9].

[6] «<Кибервласть – это> *способность использовать киберпространство для достижения преимущества и влияния в других средах при помощи инструментов власти*» [Nye, 2010, p. 4].

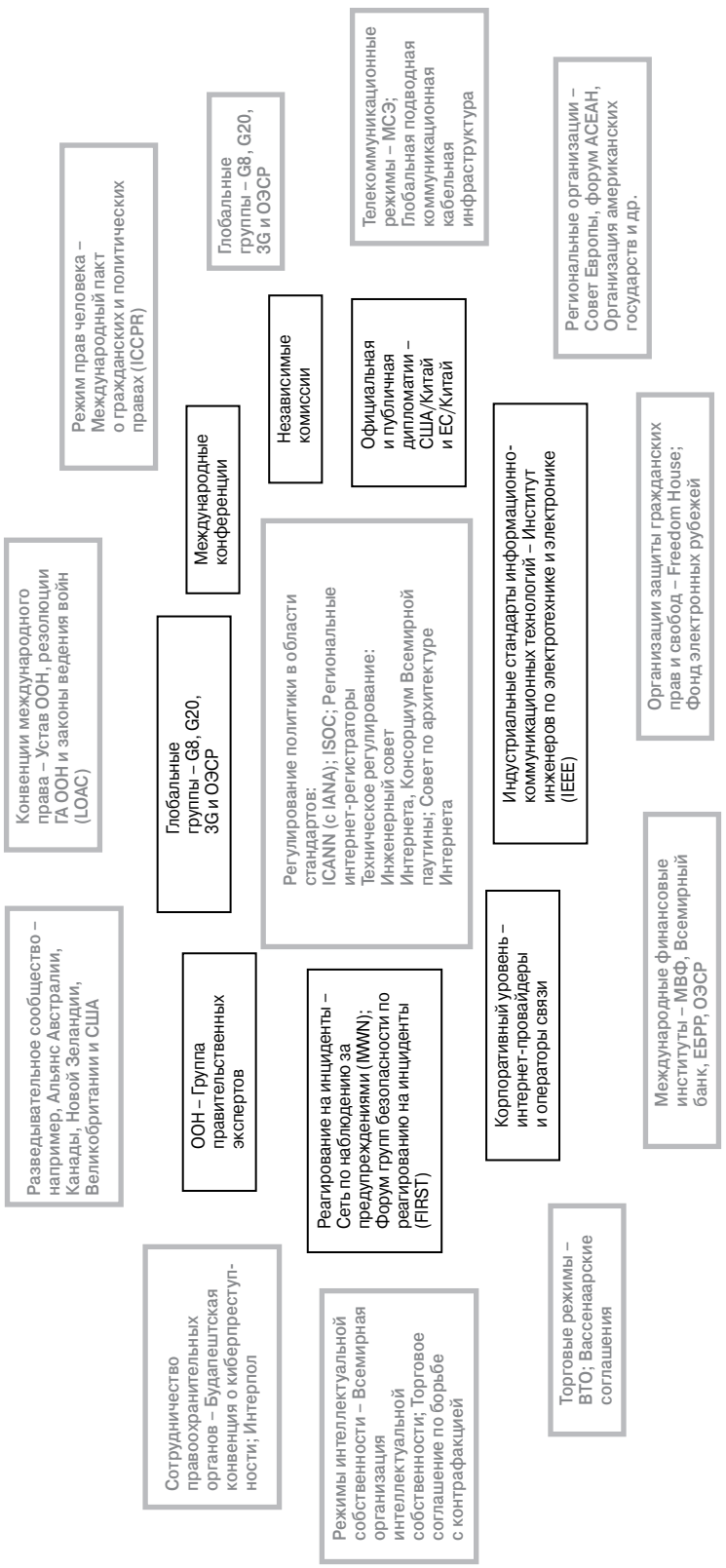


*Рис. 1.* Комплексный режим управления деятельностью в киберпространстве

*Источник:* [Nye, 2014, p. 8].

Деятельность государств на всех уровнях управления Интернетом продиктована логикой защиты собственного *суверенитета*, при этом в контексте управления Интернетом и *киберпространством* часто употребляется термин *цифровой суверенитет*. К настоящему моменту сложились два основных подхода к определению сущности данного понятия, которое имеет критическое значение для понимания *текущей* и *желаемой* роли государств в управлении Интернетом.

Представители *первого* направления придерживаются традиционного для *реализма* и *неореализма* подхода к определению роли государства и свойствах *государственного суверенитета* в условиях развития цифровых технологий. Среди авторов, которые могут быть условно включены в данную группу (см., например, [Wu, 1997; Franzese, 2009; Irion, 2012; Schmitt, 2013; Polatin-Reuben, Wright, 2014; Zheng et al., 2017; Qi et al., 2018; Ukolov, Cherkasov, 2019], преобладает убеждение в первенстве государства и национального права в цифровом (*кибер*)пространстве, что позволяет говорить о *тождественности* понятий «суверенитет» (подразумевается суверенитет государства) и «цифровой суверенитет». Контроль государства над элементами *цифровой инфраструктуры*, расположенными на подконтрольных ему территориях, создает основу для реализации государством своего суверенитета в киберпространстве. Отдельные авторы (см., например, [Kukkola, Ristolainen, 2018]) указывают, что подобное заключение не является достоянием исключительно академических кругов и находит прямое выражение в политике некоторых современных государств, в частности России [Ibid., p. 1]. Схожие утверждения встречаются в работах китайских исследователей [Zheng et al., 2017; Qi et al., 2018].

Представители *второго* направления (см., например, [Globerman, 1978; Grant, 1983; Bratton, 2015; Mueller, 2017; Couture, Toupin, 2019; Истомин, 2020]) в рассматриваемом вопросе придерживаются более *либерального* подхода. Государство рассматривается как *один из* носителей цифрового суверенитета наряду с частными компаниями [Grant, 1983; Истомин, 2020] и отдельными личностями [Couture, Toupin, 2019]. «Размытие» *государственного суверенитета* при попытке проецировать его в *киберпространстве* обусловлено несколькими факторами, среди которых основными являются создание новых технологических решений частными компаниями без участия со стороны государственных органов [Grant, 1983] и ограниченность присутствия государства в новых системах управления цифровым развитием [Bratton, 2015]. Инертность государства в киберпространстве приводит к тому, что в некоторых вопросах оно уступает роль нормоустанавливающего института, как, например, произошло в случае с деятельностью частных компаний по управлению адресным пространством Интернета – «правомерность деятельности» таких компаний признается «в национальном праве государств, в интеграционных образованиях..., в международном праве...» [Истомин, 2020].

Оба рассмотренных подхода сходятся в том, что на *физическом уровне* государства обладают значительно большими возможностями в деле реализации собственного *цифрового суверенитета*, чем на *информационном уровне*. Отдельное государство имеет возможность контролировать элементы цифровой инфраструктуры в пределах своей юрисдикции, что позволяет на физическом уровне рассматривать *цифровой суверенитет* в качестве тождественного классическому, «вестфальскому», *суверенитету* [Nye, 2014, p. 8]. Конфликты на этом уровне имеют *горизонтальную природу*, то есть государства конкурируют между акторами одной с ними природы с применением привычных средств, реализуя тем самым свою *кибервласть*.

На *информационном уровне* ситуация складывается иначе. Контролируя до определенного предела цифровую инфраструктуру, государство может применять положения собственного национального права для регулирования *отдельного сегмента* Интернета,

но не системы в целом. Конфликт в данном случае имеет не только горизонтальное, но и вертикальное выражение – государства конкурируют и между собой, и с акторами, имеющими принципиально отличную от них сущность, например, с негосударственными организациями, такими как ICANN и ISOC, которые «учитывают мнения, но не “голоса” государств» [Nye, 2014, p. 6]. При этом попытки выработать некий общий консенсус в отношении отдельных вопросов управления Интернетом привычными для государств средствами на базе международных организаций, например, специальных рабочих групп Организации Объединенных Наций[7] и Международного союза электросвязи[8], не имели значительного успеха в том смысле, что они не привели к выработке некоего универсального, применимого на практике решения в сфере управления Интернетом. Более значительные результаты были достигнуты на уровне региональных и межрегиональных договоренностей, примером чего является Будапештская конвенция о киберпреступности 2001 г., в отношении которой тем не менее справедливо следующее утверждение:

*«Наиболее значительное на сегодняшний день соглашение по вопросам киберпреступности было согласовано еще до появления Facebook и Twitter и примерно соответствует периоду зарождения цифрового гиганта Google. Маловероятно, что это соглашение способно охватить быстрые трансформации интернет-технологий, которые мы наблюдаем сегодня»* [Van Horenbeeck, 2018, p. 6].

Исходя из вышесказанного, мы приходим к выводу, что часть очень важных механизмов, обеспечивающих функционирование Интернета на современном этапе, формировались и функционируют без участия со стороны государств. Отчасти этим объясняется недостаточный оценочный уровень *подотчетности* подобных механизмов и, как следствие, недостаточный уровень *легитимности* системы управления Интернетом в целом.

В самом общем виде концепция *подотчетности* института глобального управления, к которой, безусловно, можно отнести и механизмы управления Интернетом, опирается на три компонента: *прозрачность* процесса принятия решений; предоставление *обоснования* для решений и действий; а также наличие у *адресатов подотчетности* возможности накладывать санкции в ответ на решения и действия, предпринимаемые институтом (цит. по: [Хилбрих, Шваб, 2018, p. 10]). Используя данную форму для анализа структуры и деятельности ICANN и ISOC, в следующем разделе статьи мы убедимся, что проистекающие из самой *«неподотчетной»* природы системы управления Интернетом свойства применимы и к указанным организациям.

---

[7] Специальная Группа правительственных экспертов ООН (ГПЭ ООН) занималась вопросами применимости норм международного права к регулированию киберпространства. В своих отчетах за 2013 и 2015 гг. ГПЭ ООН фактически допустила подобную возможность, что было поддержано ключевыми международными игроками. Однако уже в 2017 г. при обсуждении вопросов о применении норм гуманитарного права к ведению *кибервойны* и о праве государств на самооборону в случае нападения из киберпространства были выявлены существенные противоречия, которые привели к стагнации переговорного процесса (см. [Ваутерс, Велхерст, 2020]).

[8] В 2012 г. был принят действующий Регламент международной электросвязи (РМЭ). В ходе обсуждения Россией был предложен вариант РМЭ, значительно расширяющий полномочия МСЭ и предоставляющий больший контроль над информационными потоками национальным регуляторным органам. Позиция России была поддержана рядом государств, в том числе Китаем. Принятие данного проекта РМЭ лишило бы ICANN полномочий по регулированию адресного пространства Интернета. Из-за противодействия со стороны США, ЕС и ряда крупных компаний, в частности Google, проект не был принят, а РМЭ-2012 в итоговой редакции не охватывает вопросы, связанные с регулированием Интернета [ITU, 2012].

*Подотчетность* (*accountability*) рассматривается в качестве одного из важнейших компонентов *легитимности* институтов глобального управления (см., например, [Keohane, 2011, p. 102]). Даже при полном соответствии основным критериям *легитимности* института[9] несоответствие отдельных компонентов ожиданиям заинтересованных сторон в итоге неизбежно приводит к ее снижению. Неполная оценочная *легитимность* института тем не менее не отменяет возможности установления некоего временного *консенсуса* относительно его деятельности. Подобное положение может удовлетворять большинство участников процесса в течение некоторого периода, однако равновесие не может удерживаться вечно. Следствием недостатка *легитимности* института или включающей его *системы* являются попытки пересмотра статус-кво[10].

Таким образом, мы отмечаем следующие характеристики современной системы управления Интернетом.

Во-первых, данная система имеет комплексный, многоуровневый характер. *Управление Интернетом* подразумевает принятие решений на двух уровнях: *физическом* (цифровая инфраструктура) и *информационном* (различные связанные с системой международные режимы, технические стандарты и адреса). Государства принимают решения преимущественно на *физическом уровне*, устанавливая правила в отношении функционирования цифровой инфраструктуры на своей территории, тем самым частично реализуя свой *цифровой суверенитет*. Деятельность государств на *информационном уровне* на современном этапе ограничена сложившимся статус-кво, в условиях которого значительная часть решений принимается негосударственными акторами.

Во-вторых, текущая конфигурация системы управления Интернетом не допускает возникновения некоего единого центра, принимающего решения как на физическом, так и на информационном уровне. Попытки поручить функции принятия решений по отдельным вопросам управления Интернетом существующим международным институтам не увенчались успехом. Сложившаяся модель управления Интернетом допускает существование множества акторов, обладающих правом «решающего голоса», среди которых значительное количество представлено негосударственными организациями.

Наконец, логической производной от первых двух характеристик (многоуровневость и децентрализованность) является недостаточный оценочный уровень подотчетности ключевых институтов и, следовательно, *неполная легитимность* системы управления Интернетом. Данное утверждение будет более подробно раскрыто далее при анализе деятельности и структуры ключевых неправительственных организаций, занимающихся вопросами управления Интернетом – ICANN и ISOC.

---

[9] Роберт Кохейн выделяет шесть критериев легитимности: 1) *соответствие минимальным моральным стандартам* (соответствие общепринятым критериям, например, в вопросах обеспечения прав человека); 2) *инклюзивность* (возможность участия широкого круга заинтересованных сторон в принимаемых решениях); 3) *эпистемологическое равенство* (доступность информации о деятельности института для тех, кто испытывает воздействие от принимаемых решений); 4) *подотчетность* (возможность заинтересованных сторон оказывать влияние на принимаемые решения); 5) *демократические принципы управления* (наличие механизмов общественного контроля, защищенность прав меньшинства, обеспечение общего консенсуса при принятии решений на международном уровне); 6) *создание сравнительных преимуществ* (деятельность на международной основе должна приносить большую выгоду, чем альтернативные схемы взаимодействия, например, на двусторонней основе) [Keohane, 2011, p. 101–104]. Соответствие одним критериям и несоответствие другим, как, например, происходит в случае с деятельностью Совета Безопасности ООН в деле создания *сравнительных преимуществ* [Ibid., p. 105], в итоге выражается в недоверии к институту и принимаемым на его платформе решениям.

[10] См. сноски 5 и 6.

## ICANN и ISOC в управлении Интернетом: основные характеристики и диспропорции

Корпорация по присвоению доменных имен и Общество Интернета занимают особое положение в системе управления Интернетом и *киберпространством* в целом. В определенном смысле их задачей является выработка стандартов деятельности в киберпространстве. Рабочая инженерная группа Интернета (Internet Engineering Task Force, IETF) и Совет по архитектуре Интернета (Internet Architecture Board), которые занимают ключевую позицию в вопросах выработки и согласования технических аспектов функционирования Интернета, относятся к системе организаций, чья деятельность напрямую поддерживается силами Общества Интернета. Можно с уверенностью утверждать, что ISOC пользуется авторитетом не только в политических, но и в прикладных технологических вопросах (см. рис. 1).

В данном разделе статьи мы рассмотрим основные характеристики указанных организаций и определим инструменты, при помощи которых они участвуют в управлении Интернетом, а также возникающие в этой связи проблемы.

### *Корпорация по присвоению доменных имен и адресов (ICANN)*

ICANN – это «некоммерческая общественная корпорация, участники которой стремятся обеспечить безопасность, стабильность и функциональную совместимость Интернета. Она способствует конкуренции и разрабатывает политику в отношении уникальных идентификаторов Интернета. Благодаря своей координирующей роли ICANN оказывает *«существенное влияние на расширение и развитие Интернета»* [ICANN, 2020].

В техническом плане ICANN помогает координировать функции Администрации адресного пространства Интернета (IANA), которая предоставляет ключевые услуги для работы базовой адресной книги Интернета – Системы доменных имен (DNS). В свою очередь, основная сфера деятельности ICANN – это регулирование рынка доменных имен и унификация работы системы адресов сети Интернет. Кроме того, организация выполняет и другие функции: интернет-провайдинг, защита интеллектуальной собственности, защита интересов коммерческих и некоммерческих организаций, интернет-пользователей.

В своей деятельности ICANN опирается на два основных инструмента: рыночный и делиберативный. Этому есть две причины: во-первых, цель создания организации заключается в демонополизации рынка интернет-услуг; во-вторых, общественно-политическая повестка формируется «снизу вверх». Таким образом, политика ICANN основывается на поиске консенсуса с участием многих заинтересованных сторон.

Организации, входящие в структуру ICANN, и пользователи формируют запросы на нижнем уровне. Затем они рассматриваются в различных консультативных комитетах и рабочих группах. В итоге рекомендации предоставляются правлению для голосования. Согласно принятому уставу, ICANN организует международные съезды и конференции, тем самым предоставляя площадку, на которой все участники могут обсуждать вопросы политики по вопросам развития Интернета. Каждый может присоединиться к большинству рабочих групп ICANN, обеспечивая широкое представительство. Далее вопрос снова выносится на общественное обсуждение или отдается на доработку в комитеты. Процесс перезапускается необходимое число раз до тех пор, пока все звенья ICANN не выработают консенсусное решение или правление не примет все поправки и предложения.


*Рис. 2.* Организационная структура ICANN

*Источник:* Составлено авторами.

Схожим образом Корпорация выстраивает свои отношения с организациями – представителями национальных государств, налаживает аутрич-взаимодействие с другими международными фирмами, союзами и группами. Такое взаимодействие прежде всего опирается на рыночные механизмы и на международное право, а также на гражданское законодательство США и других национальных государств.

Главной проблемой, однако, остается калифорнийская юрисдикция ICANN. Организация имеет долгую историю сотрудничества с правительством США и долгое время была подотчетна ему. Движение к независимости началось 25 ноября 1998 г., когда ICANN и Министерство торговли США заключили Меморандум о взаимопонимании (Memorandum of Understanding) [NTIA, 1998], по которому к ICANN отходило управление некоторыми техническими функциями DNS, нумерацией интернет-адресов, координацией назначений портов и оказанием помощи в поддержании стабильности уникальных идентификаторов Интернета. При этом документ все еще требовал регулярной отчетности перед Министерством торговли США. Однако 10 марта 2016 г. ICANN выступила с предложением о передаче функций управления IANA от Национального управления по телекоммуникациям и информации (NTIA) Министерства торговли США глобальному сообществу.

Данное соглашение завершило совместное частно-государственное партнерство. Общая юридическая значимость этих изменений не столь высока, как политическая: США сохранили уменьшенную, но все же реальную степень контроля. Вывод на мировую арену дополнительного независимого актора снизил международную напряженность. Переход от государственного контроля в общественный сектор позволил решить три насущные проблемы:

1. Легитимность Организации и глобального Интернета. Так, уход от влияния правительства США позволил улучшить репутацию Организации на международной арене и снизить напряженность со стороны мирового сообщества [Becker, 2019].

2. Снижение влияния государств в пользу международных организаций или союзов, в частности ЕС.

3. Основные функции специфической отрасли были переданы экспертному сообществу. Система принятия решений «снизу вверх» позволила демократизировать деятельность корпорации.

С другой стороны, независимость ICANN повысила значимость Правительственного консультативного комитета (GAC). Ни одно решение ICANN, которое касается стран-участниц, не может быть принято без консультации с GAC [BYLAWS ICANN, 2020]. В настоящее время GAC насчитывает 178 членов и 38 наблюдателей, в число последних входят такие организации, как Совет Европы, Международный союз электросвязи, Международный уголовный суд, ВОЗ, WHOIS, ВТО, ЮНЕСКО и др. Согласно уставу ICANN, решения комитета носят рекомендательный характер и «касаются деятельности Организации, затрагивающей интересы правительств, в частности по вопросам взаимодействия правил ICANN с различными национальными законами и международными соглашениями, или вопросы государственной политики» [ICANN Strategic Plan, 2020]. Рекомендации могут быть как частного характера, то есть по конкретным заявкам на присвоение доменов общего уровня, так и общего характера.

Таким образом, GAC оказывает большое политическое влияние на деятельность ICANN. В итоге решения, которыми недовольны правительства США и Европы и их наиболее влиятельные деловые лобби, могут быть заблокированы в Организации, поскольку правление Организации должно найти консенсус в своем решении с Комитетом. С одной стороны, каждая страна имеет всего один голос в Комитете, что зачастую не позволяет выработать консолидированное решение. С другой стороны, региональные объединения, такие, например, как ЕС, имеют в Комитете больший вес.

Кроме того, система доменных имен все больше подвержена влиянию правительственных правоохранительных органов. Часть этого влияния проходит через GAC, но бо́льшая часть направляется через другие органы, такие как Организация поддержки общих имен (GNSO) [Bygrave, 2015].

### *Общество Интернета (ISOC)*

Общество Интернета (Internet Society, ISOC) было создано в 1992 г. группой энтузиастов, входивших в состав членов Инженерного совета Интернета. Исходная задача ISOC была сформулирована как «обеспечение институциональной основы и финансовой поддержки процесса развития стандартов Интернета»[11] [Cerf, 1995]. Развитие экосистемы Интернета, потребность в организации региональных представительств для поддержания единообразия в разработке и внедрении новых технологических стандартов и регламентов потребовали расширения финансирования сверх возможностей государственных программ.

Общество Интернета финансирует деятельность Рабочей группы по проектированию Интернета, Совета по архитектуре Интернета, Исследовательской рабочей группы Интернета, Инженерной управляющей группы Интернета, Альянса за доверие в Интернете и Регистратуры интересов общества (рис. 3). Общество обеспечивает сбор членских взносов от индивидуальных членов специализированных рабочих групп и пожертвований со стороны компаний-спонсоров.

[11] "...to provide an institutional home for and financial support for the Internet Standard process".

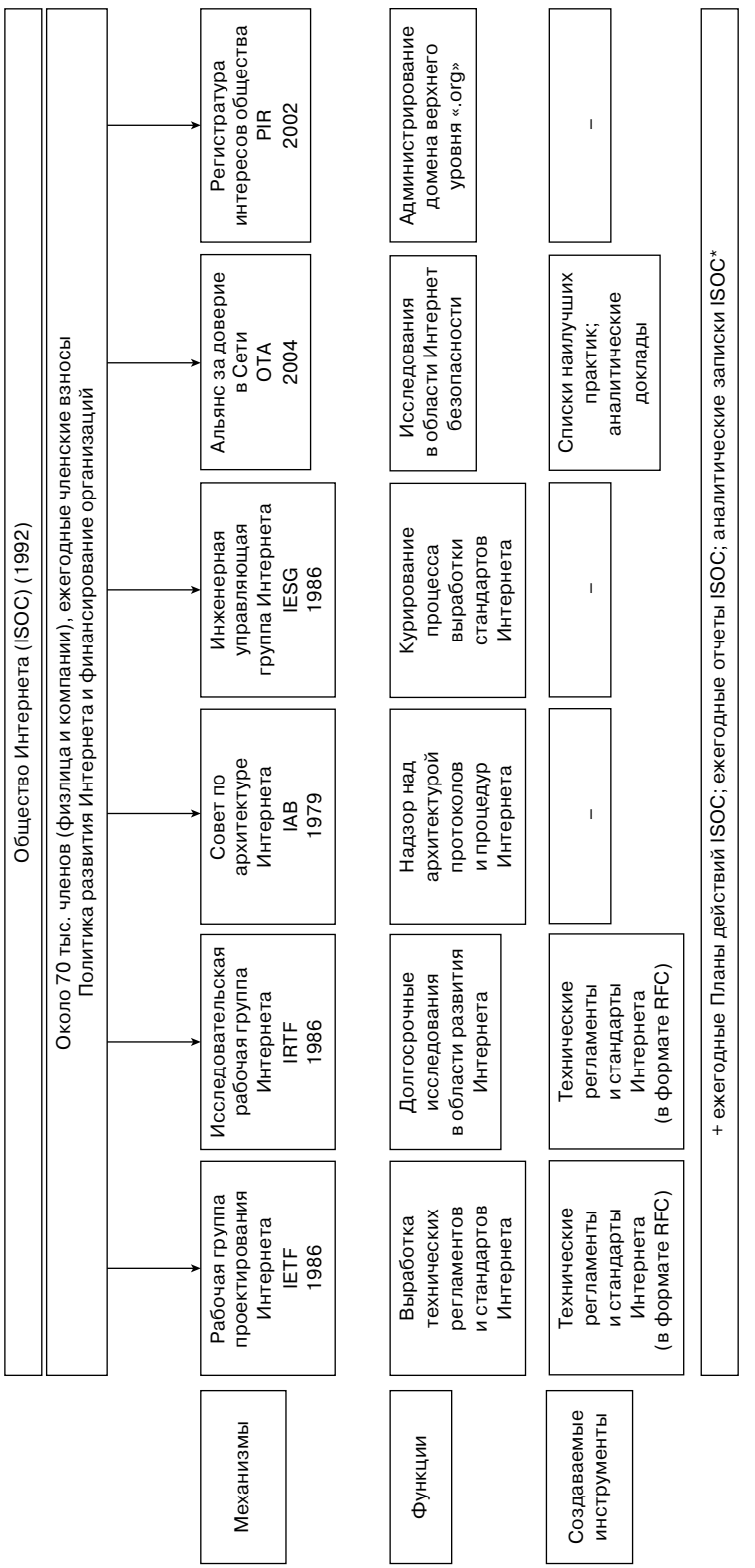


*Рис. 3.* Организации, функционирующие на базе Общества Интернета, их инструменты и функции

*Источник:* Составлено авторами.

Функции управляющего органа Общества Интернета выполняет Попечительский совет, состоящий из 13 членов. В отборе кандидатов принимают участие региональные представительства Общества, компании – спонсоры Общества и Рабочая группа проектирования Интернета. Помимо общих организационных функций Попечительский совет координирует, в том числе, работу Совета по архитектуре Интернета. За годы существования Общества членами Попечительского совета ни разу не становились граждане России или представители российских ИТ-компаний. Наибольшее количество назначений за время существования Общества получали граждане США[12].

Обществом Интернета предусмотрена система спонсорских преференций в зависимости от размера взноса[13]. Например, компании, получившие статус уровня «платиновый», могут спонсировать конкретные программы Общества наряду с наибольшим доступным количеством номинаций членов Попечительского совета Общества. Среди компаний, направляющих взносы на деятельность Общества Интернета, в настоящее время не представлены российские компании. Доминирующее положение в этой системе занимают крупные медиакорпорации США (табл. 1).

*Таблица 1.* Крупнейшие компании – спонсоры Общества Интернета (взносы более 100 тыс. долл. США)

| Страна происхождения | Название компании/организации | Характеристика деятельности |
|---|---|---|
| США | Comcast | Оператор кабельного телевидения и широкополосного доступа в Интернет |
| США | Juniper Networks | Производство телекоммуникационного оборудования |
| США | NBCUniversal | Оператор кабельного телевидения и широкополосного доступа в Интернет |
| США | Oracle Corporation | Производитель программного обеспечения |
| США | Private Internet Access | Оператор интернет-трафика |
| Нидерланды | Réseaux IP Européens Network Coordination Centre RIPE NCC | Региональный регистратор интернет-адресов |

*Источник:* <https://www.internetsociety.org/about-internet-society/organization-members/list/>.

ISOC на постоянной основе публикует множество документов, освещающих те или иные аспекты развития Интернета. Формирующиеся на их основе *инструменты* не обладают формальным статусом, а также не предполагают создания формализованных механизмов мониторинга и оценки. К публикуемым ISOC документам относятся так называемые *запросы на комментарии* (Request for comments, RFC), на базе которых

[12] ISOC Board of Trustees <https://www.internetsociety.org/board-of-trustees/>.

[13] Organization Membership Levels <https://www.internetsociety.org/about-internet-society/organization-members/membership-levels/>.

формируются стандарты Интернета, которые мы более подробно рассмотрим далее, Планы действий, Глобальные отчеты о развитии Интернета, аналитические материалы, а также списки наилучших практик в области сетевой безопасности, составляемые подотчетным Обществу Альянсом за доверие в Сети (ОТА).

ISOC как спонсор деятельности Рабочей группы проектирования Интернета и Исследовательской рабочей группы Интернета обладает авторскими правами на все опубликованные RFC и сформированные на их основе стандарты Интернета. Понятие *«стандарт Интернета»* подразумевает:

*...технически совершенный и обоснованный регламент, прошедший процесс множественной и независимой апробации в различных условиях, пользующийся поддержкой профессионального сообщества и признаваемый необходимым для функционирования всего Интернета или его сегмента*[14].

В свою очередь, понятие «технический регламент» подразумевает *«документ, описывающий любой протокол, инструмент, процедуру, соглашение по какому-либо вопросу или формату»*[15].

Каждый действующий стандарт Интернета посвящен конкретной проблеме, связанной с обеспечением бесперебойной работы сети Интернет на всем ее протяжении. В зависимости от сложности проблемы, а также длительности ее проработки, тот или иной стандарт Интернета может быть описан одним или несколькими RFC. Указанные RFC содержат описание проблемы, предложение по ее решению, а также определения вводимых или обновляемых понятий.

Предложения относительно разработки нового технического регламента вносят Рабочая группа проектирования Интернета и Инженерная рабочая группа Интернета. Решение о том, будет ли конкретный регламент дорабатываться до уровня стандарта Интернета, принимается Инженерной управляющей группой Интернета с одобрения Совета по архитектуре Интернета. При выполнении условий, заложенных в определении стандарта, техническому регламенту со временем присваивается статус стандарта Интернета.

Стандарты Интернета не относятся к юридически обязательным документам, однако высокая важность стандартов Интернета для поддержания его бесперебойной работы позволяет рассматривать их в качестве некой разновидности «мягкого права». Стандарты Интернета, утверждаемые органами Общества Интернета, признаются в качестве универсальных в каждом сегменте мирового Интернета. Учитывая, что роль Интернета в современном производстве, связи и государственном управлении является определяющей, формируемые Обществом Интернета стандарты Интернета фактически носят безальтернативный характер.

Таким образом, мы обнаруживаем важное несоответствие между функциями, которые выполняют ICANN и ISOC, и их структурой. Корпорация и Общество принимают решения по критически важным вопросам функционирования Интернета, однако они не в полной мере реализуют выявленные ранее компоненты подотчетности. Слабым компонентом подотчетности ICANN и ISOC является отсутствие формальных механизмов обеспечения обратной связи с отдельными *адресатами подотчетности*, которыми в случае с рассматриваемыми организациями являются все пользователи Интернета (государства, компании, индивидуальные пользователи и др.) (табл. 2).

[14] Bradner S. (1996) RFC 2026. The Internet Standard Process: Revision 3 <https://tools.ietf.org/html/rfc2026>.

[15] Ibid.

*Таблица 2.* Компоненты обеспечения подотчетности ICANN и ISOC

| **Компоненты обеспечения подотчетности** | **ICANN** | **ISOC** |
|---|---|---|
| Прозрачность | Финансовая отчетность налогового резидента США по форме 990s | Финансовая отчетность налогового резидента США по форме 990s. Ежегодные отчеты о деятельности Общества |
| Обоснованность принимаемых решений | Стратегический пятилетний план | Ежегодные отчеты о деятельности Общества |
| Механизмы обратной связи | Государственный консультативный комитет (GAC). *Решения комитета носят рекомендательный характер.* Комитеты ICANN постоянно взаимодействуют с контрагентами и конечными пользователями | *Не предусмотрено прямое взаимодействие с представителями государств*. Механизм премиального корпоративного членства. Региональные и международные тематические конференции *ad hoc*[16] |

*Источник*: Составлено авторами.

## Заключение. Перспективы развития Интернета и методы смягчения противоречий

Проведенный анализ показал, что децентрализованность, неподотчетность и неполноценная легитимность системы управления Интернетом являются прямым следствием инертности государств в деле согласования общих позиций по ключевым вопросам в рассматриваемой области. Интернет как концепция и совокупность единообразных технических стандартов развивался силами сообщества профессионалов, изначально преимущественно американского происхождения, а затем и при участии специалистов из других стран. Данная система изначально не предполагала вмешательства со стороны государств в процесс управления, в том числе и потому, что в момент своего зарождения и даже в процессе лавинообразного роста числа пользователей Интернета в 1990-е годы его потенциал в качестве фактора производства еще не был раскрыт.

Современная децентрализованная, неподотчетная и недостаточно легитимная система управления Интернетом представляет собой конфликтогенную среду. Данная характеристика рассматриваемой системы обусловлена ограниченностью возможностей государств в реализации собственного цифрового суверенитета, который рассматривается как продолжение государственного суверенитета в его классическом понимании. Государства стремятся к конкретизации «правил игры» в киберпространстве в интересах укрепления собственной безопасности. На практике это приводит к постепенной национализации отдельных сегментов Интернета.

Следствием текущего статус-кво становится дальнейшая интенсификация процесса национализации Интернета. Государства мира, в частности Россия [Kukkola, Ristolainen, 2018], стремятся в полной мере реализовать свой цифровой суверенитет. На практике это подразумевает усиление контроля над входящим, хранящимся и ис-

[16] Events calendar <https://www.internetsociety.org/events/>.

ходящим трафиком, что затрагивает как адресацию, так и технический аспект функционирования сети. Попытки утвердить некий единый стандарт политики в отношении информации и Интернета как средства ее передачи в таком случае рассматриваются отдельными государствами как нарушение цифрового суверенитета, что мешает выработке международного консенсуса (см. [Ваутерс, Велхерст, 2020]).

Негосударственные организации, такие как ICANN и ISOC, играют значительную роль в системе управления Интернетом. Данные организации обеспечивают некий международный консенсус в отношении адресации имен в системе Интернет и используемых технических стандартов, однако сложившийся консенсус не может считаться устойчивым. Специфика деятельности указанных организаций практически не оставляет государствам формальных рычагов воздействия на принимаемые решения. В отношении ISOC следует также отметить существующую расположенность к воздействию со стороны крупных, преимущественно американских, медиа- и ИТ-компаний. ICANN, в свою очередь, также подвергается критике за подотчетность юрисдикции США и невозможность государственного влияния, вследствие чего государства чувствует себя незащищенными в контексте контроля за доменными именами и адресами при фактическом доминировании одной общественной организации.

Развитие сетей и инфраструктуры согласовывается и контролируется на глобальном уровне посредством ежегодных конференций в рамках режима ICANN, на которых обсуждаются и излагаются протоколы и правила управления Интернетом. Китай, Россия и ряд стран Ближнего Востока все чаще оказывают давление на США, чтобы те отказались от исключительного контроля над магистральной сетью Интернета. Однако США пока явно не злоупотребляли своей протокольной властью, в то время как существуют опасения, что предоставление большего контроля другим акторам может нанести ущерб свободному потоку информации. Продолжающаяся борьба за последнее слово по протоколам, а также борьба между корпоративной властью и государственным регулированием окажутся фундаментальными для будущего Интернета. Итогом такого противостояния может стать либо его преобразование из относительно бесплатного общего достояния в пространство, контролируемое государством, либо дальнейшее противодействие этому тандема общества и организаций [Jensen, 2020].

Таким образом, мы приходим к следующим выводам относительно перспективных направлений деятельности международного сообщества в интересах сглаживания противоречий в сфере управления Интернетом.

Во-первых, на современном этапе проблема децентрализованности системы управления Интернетом не может быть эффективно решена на базе существующих механизмов согласования коллективных позиций. Примеры неудовлетворительных результатов переговоров на площадке ООН и МСЭ доказывают высокую политизированность вопросов управления Интернетом, в особенности его адресной компоненты. Данное обстоятельство препятствует выработке формального международного консенсуса, в связи с чем текущее «разделение труда» в сфере управления Интернетом представляется если не идеальным, то *лучшим из худших* вариантов развития событий.

Во-вторых, в отличие от децентрализованности, проблема *подотчетности* и недостаточной легитимности системы управления Интернетом может быть отчасти решена уже в настоящее время. Хотя ICANN и ISOC сейчас в той или иной степени обладают механизмами обеспечения подотчетности, они не могут считаться адекватными рассмотренным тенденциям, особенно в случае с ISOC.

В отличие от ICANN, ISOC не имеет в своей структуре органов, ответственных за прямое взаимодействие с органами государственной власти. В случае с Корпорацией эту функцию выполняет Комитет государственных представителей, который, однако,

не создает механизмов обратной связи с государствами как *адресатов подотчетности*, то есть не дает им возможности влиять на характер принимаемых решений. Таким образом, первым шагом на пути усиления подотчетности системы управления Интернетом в целом может стать создание структуры в рамках ISOC, аналогичной по функциям Комитету государственных представителей ICANN.

Тем не менее даже в случае, если ISOC обеспечит создание полноценного органа государственного представительства, данная мера не гарантирует полноценной подотчетности. Следующим шагом должно стать расширение полномочий государственных представителей в Комитете ICANN и гипотетической структуры ISOC, наделение их правом голоса в процессе назначения ключевых фигур в руководстве организаций и определения дальнейших стратегических шагов. Данная мера уравняет государства в правах с остальными участниками процесса, в частности с медийными корпорациями, что значительно продвинет систему управления Интернетом по пути реализации принципов Декларации 2003 г. [ООН, 2003].

## Источники


Бухт Р., Хикс Р. (2018) Определение, концепция и измерение цифровой экономики // Вестник международных организаций. Т. 13. № 2. С. 143–172. DOI: 10.17323/1996-7845-2018-02-07.

Ваутерс Я., Велхерст Э. (2020) Глобальное управление в сфере кибербезопасности: взгляд с позиции международного права и права ЕС // Вестник международных организаций. Т. 15. № 2.

Джан Л., Чен С. (2019) Цифровая экономика Китая: возможности и риски // Вестник международных организаций. Т. 14. № 2. С. 275–303. DOI: 10.17323/1996-7845-2019-02-11.

Европейский союз. (2016) Directive (EU) 2016/1148 of the European Parliament and of the council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union // Official Journal of the European Union, L 194/1.

Истомин Н.А. (2020) Признание государствами правомерности деятельности ICANN по управлению адресным пространством Интернета // Электронное сетевое издание «Международный правовой курьер». Режим доступа: http://inter-legal.ru/priznanie-gosudarstvami-pravomernosti-deyatelnosti-icann-po-upravleniyu-adresnym-prostranstvom-interneta (дата обращения: 08.06.2020).

ООН. (2003) Декларация принципов. Построение информационного общества – глобальная задача в новом тысячелетии / Всемирная встреча на высшем уровне по вопросам информационного общества. Женева, 2003 г. – Тунис, 2005 г. Режим доступа: https://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-R.pdf (дата обращения: 13.07.2020).

Правительство России. (2016) Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».

Хилбрих С., Шваб Д. (2018) «Группа двадцати»: на пути к большей подотчетности? Механизмы подотчетности «Группы двадцати» и новые вызовы в контексте Повестки для устойчивого развития на период до 2030 г. // Вестник международных организаций. Т. 13. № 4. С. 7–38.

Becker M. (2019) When public principals give up control over private agents: The new independence of ICANN in internet governance // Regulation & Governance.

Bradshow S., DeNardis L., Hampson F.O., Jardine E., Raymond M. (2016) The Emergence of Contention in Global Internet Governance // Who Runs the Internet? The Global Multi-stakeholder Model of Internet Governance. Center for International Governance Innovation. P. 45–66.

Bratton B.H. (2015) The Stack: On Software and Sovereignty. The MIT Press.

Bygrave L. (2015) Internet Governance by Contract. Oxford University Press.

BYLAWS. (2020a) Bylaws for Internet Corporation for Assigned Names and Numbers. Режим доступа: https://www.icann.org/resources/pages/governance/bylaws-en/#annexA2 (дата обращения: 06.07.2020).

Cerf V. (1995) IETF and the Internet Society. Режим доступа: https://www.internetsociety.org/internet/history-of-the-internet/ietf-internet-society/ (дата обращения: 08.07.2020).

Franzese W.P. (2009) Sovereignty in Cyberspace: Can It Exist? // Airforce Law Review. P. 1–42.

Froomkin M. (2011) Almost Free: An Analysis of ICANN's "Affirmation of Commitments" // Journal on Telecommunications and High Technology Law. Режим доступа: http://www.jthtl.org/content/articles/V9I1/JTHTLv9i1.pdf (дата обращения: 06.07.2020).

Haugen H.M. (2020) The crucial and contested global public good: principles and goals in internet governance // Internet Policy Review. Vol. 9. No. 1. P. 1–22.

ICANN Strategic Plan. (2020a) Режим доступа: https://www.icann.org/en/system/files/files/strategic-plan-2021-2025-24jun19-en.pdf (дата обращения: 06.07.2020).

ITU. (2012) Final Acts of the World Conference on International Communications (Dubai, 2012). Режим доступа: https://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12.pdf (дата обращения: 06.07.2020).

Jensen J.L. (2020) "Digital Feudalism", The Medieval Internet: Power, Politics and Participation in the Digital Age, Emerald Publishing Limited. P. 95–109.

Kaila H., Tarp F. (2019) Can the internet improve agricultural production? Evidence from Viet Nam // Agricultural Economics. Vol. 50. No. 6. P. 675–691.

Keohane R. (2011) Global governance and legitimacy // Review of International Political Economy. Vol. 18. No. 1. P. 99–109.

Korchagin A., Deniskina A., Fateeva I. (2019). Lean and energy efficient production based on internet of things (IOT) in aviation industry // E3S Web of Conferences. Vol. 110.

Kukkola R., Ristolainen M. (2018) Projected territoriality: A case study of the infrastructure of Russian "digital borders" // Conference: 17th European Conference on Cyberwarfare and Security ECCWS.

Liaropoulos A. (2013) Exercising State Sovereignty in Cyberspace: An International Cyber-Order under Construction? // Journal of Information Warfare. Vol. 12. No. 2. P. 19–26.

Liaropoulos A. (2016) Exploring the Complexity of Cyberspace Governance: State Sovereignty, Multistakeholderism, and Power Politics // Journal of Information Warfare. Vol. 15. No. 4. P. 14–26.

Mueller M. (2017) Will the Internet Fragment? Sovereignty, Globalization, and Cyberspace, Cambridge, UK: Polity.

Naughton J. (2016) The Evolution of the Internet: From Military Experiment to General Purpose Technology // Journal of Cyber Policy. Vol. 1. No. 1. P. 5–28.

NTIA. (1998) Memorandum of Understanding Between the U.S. Department of Commerce and Internet Corporation for Assigned Names and Numbers. Режим доступа: https://www.ntia.doc.gov/other-publication/1998/memorandum-understanding-between-us-department-commerce-and-internet-corporat (дата обращения: 06.07.2020).

Nye J.S. (2010) Cyber Power. Belfer Center for Science and International Affairs. Режим доступа: https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf (дата обращения: 06.07.2020).

Nye J.S. (2014) The Regime Complex for Managing Global Cyber Activities. Global Commission on Internet Governance.

Nye J.S. (2017) Deterrence and Dissuasion in Cyberspace // International Security. Vol. 41. No. 3. P. 44–47.

OECD. (2017) Digital Economy Outlook 2017. Режим доступа: https://www.oecd-ilibrary.org/docserver/9789264276284-en.pdf?expires=1592830757&id=id&accname=guest&checksum=BF5E12E9FB8C36FD7C2838DACBA57C2E (дата обращения: 22.06.2020).

OECD. (2019) Vectors of Digital Transformation. Режим доступа: https://www.sipotra.it/wp-content/uploads/2019/03/VECTORS-OF-DIGITAL-TRANSFORMATION.pdf (дата обращения: 04.06.2020).

Paloque-Berges C., Schafer V. (2019) ARPANET (1969–2019) // Internet Histories. P. 1–14. DOI: 10.1080/24701475.2018.1560921.

Polatin-Reuben D., Wright J. (2014) An Internet with BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet // Conference paper, 4th USENIX Workshop on Free and Open Communications on the Internet.

Pozdnyakova U., Mukhomorova I., Golikov V., Sazonov S., Pleshakov G. (2019) Internet of things as a new factor of production in the conditions of digital economy / E. Popkova (ed.) Ubiquitous Computing and the Internet of Things: Prerequisites for the Development of ICT. P. 1145–1154.

Qi A., Shao G., Zheng W. (2018) Assessing China's Cybersecurity Law // Computer Law & Security Review. DOI:10.1016/j.clsr.2018.08.007.

Ruggie J.G. (1982) International Regimes, Transactions, and Change: Embedded Liberalism in the Postwar Economic Order // International Organization. Vol. 36 (2).

Schmitt M.N. (2013) Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press.

Shiroma Y., Afuso H., Suwa R., Kinjo A., Tonooka Y., Kaga T., Nagayama I., Tamaki S., Maharjan G. (2019). Development of higher yield and high-quality mango production system based on Internet of Things // Electronics and Communications in Japan. Vol. 102. No. 6. P. 33–41.

Sholte J.A. (2017) Polycentrism and Democracy in Internet Governance // The Net and the Nation State. Cambridge University Press.

Ukolov V., Cherkasov V. (2019) Development of Digital Economy Regulatory Environment in Supply Chains Operations // International Journal of Supply Chain Management. Vol. 8. No. 6.

UNCTAD. (2019) Digital Economy Report 2019 Value creation and capture: implications for developing countries. Режим доступа: https://unctad.org/en/PublicationsLibrary/der2019_en.pdf (дата обращения: 03.07.2020).

Van Horenbeeck M. (2018) The future of Internet governance and cyber-security // Computer Fraud & Security. No. 5. P. 6–8.

Wu T.S. (1997) Cyberspace sovereignty? – The Internet and the International System // Harvard Journal of Law & Technology. Vol. 10. No. 311.

Zalnieriute M., Milan S. (2019) Internet Architecture and Human Rights: Beyond the Human Rights Gap // Policy & Internet. Vol. 11. No. 1. P. 6–15.

Zeng J., Stevens T., Chen Y. (2017) China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty" // Politics & Policy. Vol. 45 (3). P. 432–464. DOI:10.1111/polp.1220.

# Internet Governance: System Imbalances and Ways to Resolve Them[1, 2]

*S. Vasilkovsky, A. Ignatov*

**Sergei Vasilkovsky** – Researcher, Centre for International Institutions Research, Russian Presidential Academy of National Economy and Public Administration; 11 Prechistenskaya naberezhnaya, Moscow, 119034, Russian Federation; E-mail: vasilkovskiy-sa@ranepa.ru

**Alexander Ignatov** – PhD student at MGIMO University, Researcher, Centre for International Institutions Research, Russian Presidential Academy of National Economy and Public Administration; 11 Prechistenskaya naberezhnaya, Moscow, 119034, Russian Federation; E-mail: ignatov-aa@ranepa.ru

## Abstract

*The spread of digital technologies has led to the global digitalization of all types of public activities. The digital economy emerging during this process has become a leading factor in world economic growth and one of the criteria of national development. The digital economy is based on the Internet, which ensures the functioning of new business models, forms of social interaction and public diplomacy. The Internet governance system differs from other modern international systems of public and political relations in that the leading role in it is played by non-governmental organizations, in particular, the Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Society (ISOC). The activities of states are significantly limited by the basic properties of the system, which complicates the implementation of the state's digital sovereignty. The aim of this article is to determine ways to resolve this discrepancy.*

*Analyzing the current state of Internet governance, the authors outline the key characteristics that lead to potential conflict. These include decentralization, an insufficient evaluative level of accountability and lack of legitimacy. The authors analyze ICANN and ISOC toolkits and identify the key instruments that actually make organizations central to the Internet governance system. In conclusion, the authors provide recommendations for action by the international community to mitigate the identified imbalances.*

**Key words:** digital technologies; digital economy; digital sovereignty; Internet; Internet governance; cyber power; ICANN; ISOC

**For citation:** Vasilkovsky S., Ignatov A. (2020) Internet Governance: System Imbalances and Ways to Resolve Them. *International Organisations Research Journal*, vol. 15, no 4, pp. 7–29 (in English). DOI: 10.17323/1996-7845-2020-04-01

## References

Becker M. (2019) When Public Principals Give Up Control Over Private Agents: The New Independence of ICANN in Internet Governance. *Regulation & Governance*, vol. 13, no 4, pp. 561–76. Available at: https://doi.org/10.1111/rego.12250.

Bradner S. (1996) Best Current Practice: Internet Standards Process: Revision 3. Available at: https://tools.ietf.org/html/rfc2026 (accessed 3 November 2020).

Bradshaw S., DeNardis L., Hampson F.O., Jardine E., Raymond M. (2016) The Emergence of Contention in Global Internet Governance. *Who Runs the Internet? The Global Multi-Stakeholder Model of Internet Governance*. Global Commission on Internet Governance Research Volume Two. Center for International Governance Innovation/Chatham House. Available at: https://www.cigionline.org/sites/default/files/documents/GCIG%20Volume%202%20WEB.pdf (accessed 2 November 2020).

[1] The editorial board received the article in August 2020.

[2] The article was written on the basis of the RANEPA state assignment research programme.

Bratton B.H. (2015) *The Stack: On Software and Sovereignty*. The MIT Press.

Bukht R., Heeks R. (2018) Opredeleniye, kontseptsiya i izmereniye tsifrovoy ekonomiki [Defining, Conceptualising and Measuring the Digital Economy]. *Vestnik mezhdunarodnykh organizatsiy [International Organisations Research Journal]*, vol. 13, no 2, pp. 143–72. Available at: https://doi.org/10.17323/1996-7845-2018-02-07 (in Russian).

Bygrave L. (2015) *Internet Governance by Contract*. Oxford University Press.

Cerf V. (1995) IETF and the Internet Society. Internet Society, 18 July. Available at: https://www.internetsociety.org/internet/history-of-the-internet/ietf-internet-society/ (accessed 8 July 2020).

European Union (EU). (2016) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union. *Official Journal of the European Union*, L 194/1. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&rid=1 (accessed 3 November 2020).

Franzese P.W. (2009) Sovereignty in Cyberspace: Can It Exist? *Airforce Law Review*, vol. 64, pp. 1–42. Available at: https://www.afjag.af.mil/Portals/77/documents/AFD-091026-024.pdf (accessed 3 November 2020).

Froomkin M.A. (2011) Almost Free: An Analysis of ICANN's 'Affirmation of Commitments.' *Journal on Telecommunications & High Technology Law*, vol. 9, pp. 187–234. Available at: http://www.jthtl.org/content/articles/V9I1/JTHTLv9i1.pdf (accessed 6 July 2020).

Haugen H.M. (2020) The Crucial and Contested Global Public Good: Principles and Goals in Internet Governance. *Internet Policy Review*, vol. 9, no 1, pp. 1–22. Available at: https://doi.org/10.14763/2020.1.1447.

Hilbrich S., Schwab J. (2018) Towards a More Accountable G20? Accountability Mechanisms of the G20 and the New Challenges Posed to Them by the 2030 Agenda. *International Organisations Research Journal*, vol. 13, no 4, pp. 7–38. Available at: https://doi.org/10.17323/1996-7845-2018-04-01.

International Telecommunication Union (ITU). (2012) Final Acts of the World Conference on International Communications (Dubai, 2012). Available at: https://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12.pdf (accessed 6 July 2020).

Internet Corporation for Assigned Names and Number (ICANN). (2020a) Annex A-2: GNSO Guidance Process. Bylaws for Internet Corporation for Assigned Names and Numbers, as Amended 28 November 2019. Available at: https://www.icann.org/resources/pages/governance/bylaws-en/#annexA2 (accessed 6 July 2020).

Internet Corporation for Assigned Names and Number (ICANN). (2020b) ICANN Strategic Plan for Fiscal Years 2021–2025. Available at: https://www.icann.org/en/system/files/files/strategic-plan-2021-2025-24jun19-en.pdf (accessed 6 July 2020).

Internet Society (ISOC). (n. d., a) Board of Trustees. Available at: https://www.internetsociety.org/board-of-trustees/ (accessed 3 November 2020).

Internet Society (ISOC). (n. d., b) Organization Membership Levels. Available at: https://www.internetsociety.org/about-internet-society/organization-members/membership-levels/ (accessed 3 November 2020).

Internet Society (ISOC). (n. d., c) Our Organization Members. Available at: https://www.internetsociety.org/about-internet-society/organization-members/list/ (accessed 3 November 2020).

Internet Society (ISOC). (n. d., d) Attend an Event. Available at: https://www.internetsociety.org/events/ (accessed 3 November 2020).

Istomin N.A. (2020) Priznaniye gosudarstvami pravomernosti deyatel'nosti ICANN po upravleniyu adresnym prostranstvom Interneta [State Recognition of ICANN's Internet Address Space Management Activities]. *Mezhdunarodnyy pravovoy kur'yer* [International Legal Courier]. Available at: http://inter-legal.ru/priznanie-gosudarstvami-pravomernosti-deyatelnosti-icann-po-upravleniyu-adresnym-prostranstvom-interneta (accessed 8 June 2020). (in Russian)

Jensen J.L. (2020) *The Medieval Internet: Power, Politics and Participation in the Digital Age*. Emerald Publishing Limited.

Kaila H., Tarp F. (2019) Can the Internet Improve Agricultural Production? Evidence From Viet Nam. *Agricultural Economics*, vol. 50, no 6, pp. 675–91. Available at: https://doi.org/10.1111/agec.12517.

Keohane R. (2011) Global Governance and Legitimacy. *Review of International Political Economy*, vol. 18, no 1, pp. 99–109. Available at: https://doi.org/10.1080/09692290.2011.545222.

Korchagin A., Deniskina A., Fateeva I. (2019) Lean and Energy Efficient Production Based on Internet of Things (IOT) in Aviation Industry. *E3S Web of Conferences*, vol. 110. Available at: https://doi.org/10.1051/e3sconf/201911002124.

Kukkola R., Ristolainen M. (2018) Projected Territoriality: A Case Study of the Infrastructure of Russian 'Digital Borders.' Paper presented at the 17th European Conference on Cyber Warfare and Security ECCWS, Oslo. Available at: https://www.researchgate.net/publication/326292919_Projected_territoriality_A_case_study_of_the_infrastructure_of_Russian_%27digital_borders%27 (accessed 3 November 2020).

Liaropoulos A. (2013) Exercising State Sovereignty in Cyberspace: An International Cyber-Order Under Construction? *Journal of Information Warfare*, vol. 12, no 2, pp. 19–26. Available at: https://www.jstor.org/stable/26486852.

Liaropoulos A. (2016) Exploring the Complexity of Cyberspace Governance: State Sovereignty, Multistakeholderism, and Power Politics. *Journal of Information Warfare*, vol. 15, no 4, pp. 14–26.

Mueller M. (2017) *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace*. Cambridge: Polity.

National Telecommunications and Information Administration (NTIA). (1998) Memorandum of Understanding Between the U.S. Department of Commerce and Internet Corporation for Assigned Names and Numbers. 25 November. Available at: https://www.ntia.doc.gov/other-publication/1998/memorandum-understanding-between-us-department-commerce-and-internet-corporat (accessed 6 July 2020).

Naughton J. (2016) The Evolution of the Internet: From Military Experiment to General Purpose Technology. *Journal of Cyber Policy*, vol. 1, no 1, pp. 5–28. Available at: https://doi.org/10.1080/23738871.2016.1157619.

Nye J.S. (2010) Cyber Power. Belfer Center for Science and International Affairs, Harvard Kennedy School. Available at: https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf (accessed 6 July 2020).

Nye J.S. (2014) The Regime Complex for Managing Global Cyber Activities. Global Commission on Internet Governance Paper Series No 1, Centre for International Governance Innovation. Available at: https://www.cigionline.org/publications/regime-complex-managing-global-cyber-activities (accessed 3 November 2020).

Nye J.S. (2017) Deterrence and Dissuasion in Cyberspace. *International Security*, vol. 41, no 3, pp. 44–7. Available at: https://doi.org/10.1162/ISEC_a_00266.

Organisation for Economic Co-operation and Development (OECD). (2017) Digital Economy Outlook 2017. Available at: https://dx.doi.org/10.1787/9789264276284-en.

Organisation for Economic Co-operation and Development (OECD). (2019) Vectors of Digital Transformation. Available at: OECD Digital Economy Papers No 273. https://www.sipotra.it/wp-content/uploads/2019/03/VECTORS-OF-DIGITAL-TRANSFORMATION.pdf (accessed 4 June 2020).

Paloque-Berges C., Schafer V. (2019) ARPANET (1969–2019). *Internet Histories*, vol. 3, no 1, pp. 1–14. Available at: https://doi.org/10.1080/24701475.2018.1560921.

Polatin-Reuben D., Wright J. (2014) An Internet With BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet. Paper presented at the FOCI'14 Conference, San Diego, 18 August. Available at: https://www.usenix.org/system/files/conference/foci14/foci14-polatin-reuben.pdf (accessed 3 November 2020).

Pozdnyakova U., Mukhomorova I., Golikov V., Sazonov S., Pleshakov G. (2019) Internet of Things as a New Factor of Production in the Conditions of Digital Economy. *Ubiquitous Computing and the Internet of Things: Prerequisites for the Development of ICT* (E. Popkova (ed.)). Springer.

President of Russia. (2016) *Ukaz Prezidenta Rossiyskoy Federatsii ot 05.12.2016 № 646 Ob utverzhdenii Doktriny informatsionnoy bezopasnosti Rossiyskoy Federatsii* [Decree of the President of the Russian Federation dated 05.12.2016 No 646 On Approval of the Doctrine of Information Security of the Russian Federation]. Available at: http://kremlin.ru/acts/bank/41460 (accessed 3 November 2020). (in Russian)

Qi A., Shao G., Zheng W. (2018) Assessing China's Cybersecurity Law. *Computer Law & Security Review*, vol. 34, no 6, pp. 1342–54. Available at: https://doi.org/10.1016/j.clsr.2018.08.007.

Ruggie J.G. (1982) International Regimes, Transactions, and Change: Embedded Liberalism in the Postwar Economic Order. *International Organization*, vol. 36, no 2, pp. 379–415. Available at: https://doi.org/10.1017/S0020818300018993.

Schmitt M.N. (2013) *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press.

Shiroma Y., Afuso H., Suwa R., Kinjo A., Tonooka Y., Kaga T., Nagayama I., Tamaki S., Maharjan G. (2019) Development of Higher Yield and High-Quality Mango Production System Based on Internet of Things. *Electronics and Communications in Japan*, vol. 102, no 6, pp. 33–41. Available at: https://doi.org/10.1002/ecj.12170.

Sholte J.A. (2017) Polycentrism and Democracy in Internet Governance. *The Net and the Nation State* (U. Kohl (ed.)). Cambridge University Press. Available at: https://doi.org/10.1017/9781316534168.012.

Ukolov V., Cherkasov V. (2019) Development of Digital Economy Regulatory Environment in Supply Chains Operations. *International Journal of Supply Chain Management*, vol. 8, no 6. Available at: https://ojs.excelingtech.co.uk/index.php/IJSCM/article/view/4107/2069 (accessed 3 November 2020).

United Nations (UN). (2003) Deklaratsiya printsipov Vsemirnoy vstrechi na vysshem urovne po voprosam informatsionnogo obshchestva Zheneva, 2003 g. – Tunis, 2005 g. Postroyeniye informatsionnogo obshchestva – global'naya zadacha v novom tysyacheletii [Declaration of Principles of the World Summit on the Information Society, Geneva, 2003 – Tunisia, 2005 Building the Information Society: A Global Challenge in the New Millennium]. Available at: https://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-R.pdf (accessed: 13 July 2020). (in Russian)

United Nations Conference on Trade and Development (UNCTAD). (2019) Value Creation and Capture: Implications for Developing Countries. Digital Economy Report 2019. Available at: https://unctad.org/en/PublicationsLibrary/der2019_en.pdf (accessed 3 July 2020).

Van Horenbeeck M. (2018) The Future of Internet Governance and Cyber-Security. *Computer Fraud & Security*, no 5, pp. 6–8. Available at: https://doi.org/10.1016/S1361-3723(18)30042-3.

Wouters J., Verhelst A. (2020) Global'noye upravleniye v sfere kiberbezopasnosti: vzglyad s pozitsii mezhdunarodnogo prava i prava YES [Filling Global Governance Gaps in Cybersecurity: International and European Legal Perspectives]. *Vestnik mezhdunarodnykh organizatsiy* [International Organisations Research Journal], vol. 15, no 2, pp. 141–72. Available at: https://doi.org/10.17323/1996-7845-2020-02-07. (in Russian)

Wu T.S. (1997) Cyberspace Sovereignty? The Internet and the International System. *Harvard Journal of Law & Technology*, vol. 10, no 3. Available at: http://jolt.law.harvard.edu/articles/pdf/v10/10HarvJLTech647.pdf (accessed 3 November 2020).

Zalnieriute M., Milan S. (2019) Internet Architecture and Human Rights: Beyond the Human Rights Gap. *Policy & Internet*, vol. 11, no 1, pp. 6–15. Available at: https://doi.org/10.1002/poi3.200.

Zeng J., Stevens T., Chen Y. (2017) China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty." *Politics & Policy*, vol. 45, no 3, pp. 432–64. Available at: https://doi.org/10.1111/polp.1220.

Zhang L., Chen S. (2019) Tsifrovaya ekonomika Kitaya: vozmozhnosti i riski [China's Digital Economy: Opportunities and Risks]. *Vestnik mezhdunarodnykh organizatsiy* [International Organisations Research Journal], vol. 14, no 2, pp. 275–303. Available at: https://doi.org/10.17323/1996-7845-2019-02-11. (in Russian)