ТОЧКА ЗРЕНИЯ

МЕЖДУНАРОДНОЕ РЕГУЛИРОВАНИЕ КИБЕРПРОСТРАНСТВА: ВОЗМОЖНО ЛИ ЭФФЕКТИВНОЕ ВЗАИМОПОНИМАНИЕ?

Коровкин Владимир Владиславович

Руководитель направления «Инновации и цифровые технологии», профессор бизнес-практики Московской школы управления СКОЛКОВО (Москва, Россия.

Аннотация. *Ключевым вызовом для эффективного правового регулирования киберпространства является его архитектурная трансграничность. Цель данной статьи состоит в анализе противоречий между позициями основных стран – участниц дискуссий по вопросам международного регулирования киберпространства. В связи с малой вероятностью достижения в обозримом будущем широкого международного консенсуса в области киберправа прогнозируется регионализация киберпространства, с созданием союзов, основанных на взаимном доверии участников и единстве взглядов на принципы киберрегулирования.*

Ключевые слова: *цифровизация; киберпространство; киберрегулирование; международная кибербезопасность.*

Для цитирования: Коровкин В.В. Международное регулирование киберпространства: возможно ли эффективное взаимопонимание? // Социальные новации и социальные науки. – Москва: ИНИОН РАН, 2020. – № 1. – С. 60–76.

URL: https://sns-journal.ru/ DOI: 10.31249/snsn/2020.01.05

Введение

Понятие «киберпространство» появилось в научно-фантастической литературе в начале 1980-х годов [Benedikt, 1991 a, p. 1], но уже через несколько лет было введено в научный оборот для описания растущего феномена глобального обмена информацией с помощью компьютерных устройств. В 1990 г. была проведена первая международная научная конференция по киберпространству (в Университете Техаса, Остин), год спустя вышел сборник статей под редакцией архитектора-урбаниста и философа Майкла Бенедикта. В своей программной статье в этом сборнике М. Бенедикт дал такую характеристику этому феномену:

> «Киберпространство – это глобально связанная многомерная искусственная или "виртуальная" реальность, поддерживаемая компьютерами, доступная через компьютеры и создаваемая компьютерами… Киберпространство имеет [свою] географию, физику, природу и [свое] *верховенство человеческого закона»* (выделено мной. – *В. К.*) [Benedikt, 1991 b, p. 122–123].

Примечательно, что вопрос о праве и законе в киберпространстве возник на заре осознания нового феномена. Тридцать лет спустя этот вопрос остается в значительной степени нерешенным, несмотря на многочисленные усилия на национальном и международном уровнях. Ключевым вызовом для эффективного правового регулирования киберпространства является его принципиальная глобальность, трансграничность. При этом имеет место парадокс: с одной стороны, информационные сети, составляющие основу киберпространства, представляются своего рода глобальным общественным благом (подобным мировому океану или атмосфере). С другой стороны, они функционируют и развиваются благодаря усилиями преимущественно частных акторов, которые сосредоточены в весьма небольшом количестве юрисдикций [Коровкин, 2019, с. 152]. Этот парадокс делает относительно малоэффективным национальное регулирование киберпространства. Кроме того, подходы нескольких отдельных суверенов к киберправу определяют де-факто международную правовую практику.

Данная ситуация вызывала и вызывает озабоченность ряда стран. Наиболее определенно высказывались Россия и Китай, которые на протяжении последних двух десятилетий предлагали идею создания международного регулирования киберпространства в виде обязывающей конвенции. Эта идея не находила понимания в США и странах Европейского союза. Ситуация в значительной степени зашла в тупик [Kerttunen, Tikk, 2018], особенно после осложнения общей геополитической ситуации в середине 2010-х годов. В 2017 г. межправительственная группа экспертов под эгидой ООН не смогла выпустить консенсусный документ по итогам заседания, причем пред-

ставители России и США обменялись весьма резкими заявлениями, фактически отказывая друг другу в статусе добронамеренных (bona fide) акторов. Непосредственным поводом для столкновения стала дискуссия вокруг принципиального подхода к кибервойне[1]. Однако круг разногласий между странами гораздо шире.

Характерные цитаты из встречных официальных заявлений показывают глубину взаимного недоверия. По мнению российского спецпредставителя, достижению консенсуса мешают: «…определенные страны, которые стремятся навязать всему миру свои правила игры в информационном пространстве… Основываясь на своих технологических достижениях, они пытаются обеспечить “право сильного” в информационном пространстве» [МИД РФ, 2017]. В свою очередь, спецпредставитель США заявил: «Я прихожу к печальному заключению, что те, кто не желает подтвердить применимость международных правовых норм и принципов [к кибервойне] считают, что их государства свободны действовать… через киберпространство для достижения своих политических целей без каких-либо пределов или ограничений для их действий» [Department of State, 2017].

Создание международного законодательства является во многих отношениях более сложным процессом, чем национальное законотворчество. Международный закон может быть установлен исключительно консенсусом всех участвующих сторон; страны имеют возможность не присоединяться к нему, причем решение о присоединении (ратификация уполномоченными национальными органами власти, обычно парламентами) практически всегда становится результатом сложного внутреннего политического процесса. Акторы международного пространства осознают себя как находящихся в сложной конкурентной ситуации с неравными стартовыми позициями и по этой причине: 1) ищут способы ее усиления и 2) предполагают, что другие участники процесса действуют аналогичным образом. Это приводит к расхождению в декларируемых и реально преследуемых целях. Каждый актор также имеет в своем распоряжении стратегию формального присоединения без намерения реального исполнения принятых на себя обязательств. Подобная стратегия может дать отдельным национальным акторам международное конкурентное преимущество («трагедия общин», предложенная британским экономистом У.Ф. Ллойдом в 1833 г. [Lloyd, 1980]). Возможности международного сообщества в части исключения таких стратегий весьма ограничены, в результате чего общий процесс характеризуется высокой степенью взаимного недоверия.

[1] Позиция России состоит в том, что киберпространство должно быть демилитаризовано и кибервойна исключена с помощью международного законодательства, позиция США сводится к тому, что в той или иной форме агрессивные действия в киберпространстве являются состоявшимся фактом и задачей международного закона должно быть создание норм, регулирующих военные действия в киберпространстве в соответствии со сложившимся военным и гуманитарным правом. Соответствующие заявления были сделаны спецпредставителем МИД РФ Андреем Крутских (https://www.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2804288) и представителем Госдепа США Мишель Маркофф (https://findit.state.gov/search?utf8=%E2%9C%93&affiliate=dos_stategov&sort_by=&query=statement+on+UN+GGE+2017)

Балансирующим осознанием является предвосхищение возможности существенной международной дестабилизации, которая будет иметь для отдельных акторов более опасные последствия, чем следование согласованным правилам. Однако в целом современное международное право не носит такого всеобъемлющего характера, как национальные законодательства. Всегда имеется возможность оставить ту или иную область неурегулированной, что предпочтительнее присоединения к законодательству, нарушающему национальные интересы.

Успешно заключенные и исполняемые международные договоры[1] в результате сводились к (1) гармонизации национального законодательства в областях с давно сложившейся практикой (например – торговое право); (2) созданию норм в отношении действий, имеющих потенциально катастрофические гуманитарные последствия (законы о ведении войны, ограничение ядерных испытаний, запрет химического и бактериологического оружия[2]), или (3) имеющих относительно небольшое значение для национальных интересов (конвенции по космическому пространству и Антарктиде[3]). Определенным исключением является международное морское право. Оно создавалось в необычной ситуации, когда страны с относительно небольшим общим весом в международном пространстве оказались в силу географии владельцами важнейшего ресурса – морских проливов, что давало им достаточно сильную переговорную позицию.

Киберпространство по своей природе отличается от всех перечисленных случаев. Оно возникло относительно недавно и находится в процессе постоянных изменений, что исключает обращение к сложившимся обычаям и практикам. Гуманитарные последствия злоупотреблений в киберпространстве – хотя и значительные – не выглядят сопоставимыми с ядерным, химическим или биологическим конфликтом. В то же время киберпростанство стало одним из ключевых драйверов социально-экономического и политического развития практически во всех странах мира, и это его значение постоянно растет. При этом архитектура нынешнего киберпространства дает существенное преимущество ограниченной группе стран (если не сказать, одной стране). У «малых» участников процесса нет и не предвидится никаких «балансирующих» возможностей для усиления своей позиции. Крупные страны-акторы могут извлечь существенную выгоду из неприсоединения или формального, но не соблюдаемого присоединения к регулированию[4]. В результате создание эффективного, исполняемого, согласованного регулирования киберпространства является задачей

[1] См. список ключевых договоров под эгидой ООН: https://www.un.org/en/sections/issues-depth/international-law-and-justice/index.html

[2] При этом участники соответствующих конвенций продолжали подозревать других участников в их нарушении, ряд нарушений конвенции в отношении химического оружия доказанно имел место (к примеру, ирано-иракская война 1980–1988 гг.) без серьезных немедленных последствий для нарушителей.

[3] В последнем случае присоединение к конвенции не мешает таким странам, как Аргентина и Чили, официально считать часть Антарктиды суверенной территорией.

[4] Примером является позиция Китая, проигнорировавшего Будапештскую конвенцию по киберпреступности, криминализировавшую определенные нарушения в области интеллектуальной собственности, для разрешения ситуации США потребовалось заключение отдельного двустороннего договора в 2015 г.

беспрецедентной сложности с юридической и технической, но прежде всего – с политической стороны.

Осознание всех этих сложностей породило ряд дискуссий в мировой юридической литературе, которые группируются вокруг двух тем: «Является ли международное право действительно правом?»[1] и «Является ли международное право действительно международным?». По первому пункту достаточно радикальная точка зрения была высказана в 1994 г. Ширли Скотт, которая заметила, что «определяющей послевоенной парадигмой в международных отношениях был реализм, который отвергает международное право как практически не имеющее отношения к вопросам “высокой” политики». По ее мнению, последняя в целом основывается на концепции «силы» [Scott, 1994]. Второй дискуссии посвящена, например, книга [Roberts, 2017].

Действительно, необходимо учитывать, что международное законотворчество в любом случае происходит не «с нуля», а оказывается вписанным в тот или иной исторический контекст. Возникновение Интернета как глобального феномена почти совпало по времени с моментом окончания холодной войны и распада «социалистического лагеря». Его развитие происходило параллельно со сложными политическими процессами 1990–2000-х годов. В связи с этим идеологемы времен холодной войны продолжают в большой степени определять взгляды ключевых стейкхолдеров мирового киберпространства на интересы, мотивы и стратегии оппонентов.

Различия в подходах между основными государствами-стейкхолдерами мирового киберпространства неоднократно становились предметом анализа как в отечественной [Зиновьева, 2016; Захаров, 2018], так и в зарубежной литературе [Kerttunen, Tikk, 2018]. Однако данный анализ, как правило, ограничивался ситуативно-техническим рассмотрением разногласий без выяснения их глубинных причин. Цель данной статьи состоит в том, чтобы проанализировать позиции ключевых стран – участниц дискуссий по вопросам международного регулирования киберпространства в контексте сложившейся культуры решения конфликтов частного и общественного. Результаты исследования помогают прийти к более глубокому пониманию позиции оппонентов и формулировать более реалистичные ожидания в отношении возможностей достижения согласия в области международного киберрегулирования.

Метод анализа

Решение поставленной задачи включает, прежде всего, анализ ключевых документов, выражающих позиции сторон в дискуссии по международному регулированию, идущей на протяжении более 20 лет. Принципиально важно вписать эти документы в более широкий контекст взглядов на

[1] «Is international law really a law?», что можно также перевести как «Является ли международный закон действительно законом?», понятийные поля английского термина Law и российских «право» и «закон» пересекаются довольно сложным образом.

государственное управление. Всякий подход к регулированию должен имплицитно или эксплицитно учитывать расстановку приоритетов между частными и общественными интересами в сфере международных информационных сетей и возможную программу действий, создающих приемлемый баланс между этими интересами.

Официальная позиция России по вопросам международного кибер-регулирования сформулирована в представленном в ООН в 2011 г. проекте Конвенции об обеспечении международной информационной безопасности [МИД РФ, 2011], который стал своего рода итогом целой серии инициатив в формате ООН. Хотя формально проект был внесен группой стран, включающей также такого важного стейкхолдера глобального киберпространства как Китай, документ позиционировался как инициатива РФ и был воспринят именно в таком качестве в международной экспертной среде [Kerttunen, Tikk, 2018].

Основным оппонентом российской инициативы в ООН являются США [Демидов, 2013[1]; Хужина, 2015; Захаров, 2018; Prakesh, Baruah, 2014]. К их единомышленникам («like-minded powers») относят Великобританию и Нидерланды [Kerttunen, Tikk, 2018, p. 24]. Суть оппозиции состоит не в предложении сопоставимого альтернативного документа (поскольку поддерживаемая условным «Западом» Будапештская конвенция Совета Европы[2] о киберпреступлениях 2001 г. носит гораздо более ограничивающий характер)[3], а в отвержении самой идеи эффективной глобальной киберконвенции.

Официальным документом, описывающим ключевые подходы США к международному киберрегулированию, является «Международная стратегия в отношении киберпространства» 2011 г. [White House, 2011]. В этом документе излагаются взгляды администрации Барака Обамы на роль киберпространства в социально-экономическом развитии на национальном и глобальном уровне, а также цели и принципы действия США в отношении киберпространства. В 2018 г. администрацией Дональда Трампа была принята «Национальная стратегия в отношении киберпространства», описывающая в большей степени действия в отношении внутреннего пространства (homeland), однако затрагивающая и международный контекст. Важными дополнениями для анализа позиции

[1] В частности, было верно отмечено, что есть значительные расхождения между понятием «информационная безопасность», содержащимся в документе и носящим весьма широкий характер, и многими распространенными трактовками содержания «кибербезопасности», сводящегося к функционированию инфраструктуры компьютерных сетей. По словам автора, «конкуренция России и ее союзников (КНР и другие государства ШОС) с западными государствами в части утверждения на глобальном уровне того или иного понимания роли ИКТ в контексте международной безопасности приобретает черты идеологического противостояния» [Демидов, 2013, с. 137].

[2] Несмотря на то что Конвенция разработана Советом Европы, она открыта для присоединения всех стран. Из крупных неевропейских стран конвенцию ратифицировали на настоящий момент США, Канада, Австралия, Япония и Израиль.

[3] Россия была последовательным критиком Будапештской конвенции, считая, что она, с одной стороны, не носит достаточно всеобъемлющего характера в описании информационных угроз, а с другой стороны, не уважает национальный суверенитет участников (РИА «Новости», «РФ поддерживает разработку конвенции по борьбе с киберпреступностью», 28 октября 2014 г., https://ria.ru/20141028/1030552154.html)

США и их единомышленников являются заявления официальных лиц, сделанные на площадках международных организаций или адресованные СМИ.

Альтернативный «западный» подход к глобальному киберпространству представляет «Международная стратегия в отношении цифрового пространства» Франции [Ministere de l'Europe, 2018]. Эту страну не относят к непосредственному кругу единомышленников США, и в ее стратегии выражается озабоченность по поводу американской цифровой гегемонии. Также немаловажно, что французская «континентальная» правовая культура традиционно противопоставляется англо-американскому обычному праву.

Наконец, позиция одного из основных стейкхолдеров мирового киберпространства, Китая, выражена в принятой в 2017 г. «Национальной стратегии по сотрудничеству в кибепространстве» [Xinhua …, 2017].

Дополнительный контекст исследования задают проекты международного киберрегулирования, созданные частными лицами и организациями преимущественно в рамках «западной» части цифрового пространства, а также ряд инициатив крупных международных корпораций, призванные синхронизировать подходы в области создания безопасных цифровых систем [Stadnik, 2018]. Отдельный интерес представляют две редакции так называемого «Таллиннского руководства по международному закону, применимому к кибервойне» (во второй редакции слово «кибервойна» (cyber warfare) было заменено на «кибероперации» (cyber operations) [Schmitt, 2013; Schmitt, 2017]. Данные документы являются академическими исследованиями, представляющими мнение коллектива видных международных юристов о применимости существующих норм международного права к военным действиям в киберпространстве.

Для достижения цели исследования необходим инструмент комплексного сравнительного анализа перечисленных текстов. К сожалению, правовая компаративистика не имеет пока что единого признанного метода [Van Hoecke, 2015]. Наиболее распространенный так называемый функциональный метод не выявляет расхождения между разными правовыми системами в понимании того, что является или не является проблемой. В частности, применение функционального метода к проектам международного киберрегулирования создает впечатление разногласий в отношении предлагаемых способов решения там, где имеет место более глубокий конфликт идеологий и правовых культур.

Возможное решение проблемы было предложено Г. Франкенбергом, занимавшимся сравнительным анализом национальных конституций. В его модели «конституционной архитектуры» различаются четыре уровня: права и принципы, ценности и обязанности, организационные меры и, наконец, правила конституционных изменений и интерпретации [Frankenberg, 2006]. Поскольку международное киберрегулирование можно представить как попытку создания «конституции гло-

бального киберпространства», данная модель вполне подходит для целей настоящего анализа. Наибольший интерес при этом представляют первые два уровня: прав и принципов, ценностей и обязанностей.

С учетом того, что с практической точки зрения важно, прежде всего, усилить позицию России в области международного киберрегулирования, в центре анализа находится проект конвенции по информационной безопасности, предложенный в ООН в 2011 г., и позиции других стран по отношению к нему.

Результаты анализа

Модель Франкенберга позволяет выявить и формализовать существенные различия в правовых подходах ведущих стран-стейкхолдеров глобального киберпространства на уровнях принципов и ценностей.

Принципы

Российский проект Конвенции по информационной безопасности содержит два ключевых принципа: (1) необходимость отдельного всеобъемлющего регулирования вопросов глобальной информационной безопасности в рамках единого документа и (2) организация глобального киберпространства как совокупности национальных киберпространств, управляемых государствами [МИД РФ, 2011, с. 2].

Первый принцип разделяется и некоторыми авторами альтернативных концепций киберрегулирования. Например, проект договора С. Шольберга имеет следующее вступление:

> «Киберпространство, будучи пятым общим доменом – после суши, моря, воздуха и космоса – требует координации, кооперации и правовых мер среди всех наций. Договор о киберпространстве или серия договоров на уровне ООН… должны стать каркасом (framework) для мира, справедливости и безопасности» [Schjolberg, Ghernaouti-Hélie, 2011, p. I].

Однако группа «США и единомышленники» не поддерживает данный принцип, о чем можно судить по мнению, высказанному министром иностранных дел Великобритании Уильямом Хейгом [Foreign and Commonwealth Office, 2012]. В качестве альтернативы У. Хейг предложил семь принципов сотрудничества между государствами, бизнесами и организациями в киберпространстве: 1) необходимость для правительств действовать в киберпространстве пропорционально и в соответствии с международным законом; 2) необходимость предоставить каждому способность доступа в киберпространство, включая навыки, технологии, уверенность и возможность; 3) необходимость пользователям киберпространства демонстрировать терпимость и уважение к различиям в языке, культуре и идеях; 4) необходимость обеспечить открытость киберпространства для инноваций и самовыражения, свободного обмена идеями и информацией; 5) необходимость уважения

индивидуальных прав на частную жизнь (privacy) и обеспечения необходимой защиты интеллектуальной собственности; 6) необходимость коллективно работать над решением в ответ на угрозу от онлайн-преступников; 7) продвижение конкуренции, обеспечивающей справедливый возврат от инвестиций в сети, услуги и контент [Foreign and Commonwealth Office, 2012].

Таким образом, налицо расхождение между стремлением создать всеобъемлющий, формализованный юридический документ и предложением действовать на основании достаточно ограниченного набора правил, более близкого по языку к политической декларации, чем к законотворчеству. Здесь несложно увидеть общее противоречие между «континентальной» правовой традицией, основанной на правовых кодексах, и англо-американского «обычного права», традиционно скептичного к кодификации.

Российская концепция создана в рамках правовой культуры, считающей, что кодификация – «наиболее совершенная форма развития законодательства», и что она создает «прочный каркас, на котором держится вся правовая материя той или иной отрасли… законодательства» [Рахманина, 2008, с. 32, 36]. Точка зрения обычного права может быть выражена следующим образом: «наличие кодекса не является ни необходимым, ни достаточным условием для достижения этих принципов [свободы, равенства и справедливости]» [Canale, 2009].

Какое-то время ряд правоведов в США в принципе отрицали необходимость создания отдельного регулирования для Интернета, указывая, что практически все связанные с ним проблемы могут быть решены в рамках обычного права. Так называемая дискуссия о «лошадином праве» велась заочно между Ф. Истбруком [Easterbrook, 1996] и Л. Лессигом [Lessig, 1999] в конце 1990-х годов. Позиция первого состояла в том, что отдельное киберправо имеет не более смысла, чем отдельное «лошадиное право» (Law of the Horse), поскольку все необходимые нормы (владение, купля-продажа, правила движения и т.д.) уже содержатся в общем праве. Второй указывал, что киберпространство является более сложным феноменом, его отдельное регулирование необходимо и более того, фактически уже осуществляется изнутри самого киберпространства (см. ниже). Точка зрения Лессига достаточно скоро стала доминирующей – уже в 2001 г. США активно поддержали Будапештскую конвенцию о киберпреступности. Однако сама дискуссия, проходившая на площадках ведущих юридических форумов и журналов, показывает, что специальная кодификация не является правовым инстинктом в рамках англо-американской традиции.

США настаивают, что объем специального регулирования, осуществляемый в рамках Будапештской конвенции, вполне достаточен и не требует существенного расширения. В свою очередь, авторы Таллинских руководств в целом убедительно справляются с задачей интерпретации существующих международных норм, включая гуманитарное право и законы войны, в применении к военным операциям в киберпространстве.

В 2011 г. США окончательно сформулировали свою правовую позицию в отношении к международному киберпространству:

> «Разработка норм поведения государств в киберпространстве не требует переизобретения обычного международного права и не делает существующие международные нормы устаревшими… уникальные атрибуты сетевых технологий требуют дополнительной работы по выяснению того, как применять эти нормы и какое дополнительное понимание может быть необходимо для их расширения» [White House, 2011, p. 9].

Второй принцип российского подхода к международной информационной безопасности (конструирование глобального киберпространства через национальные) также находит понимание у ряда зарубежных авторов. В частности, он разделяется в проекте С. Шольберга, который в значительной мере основан на его опыте сотрудничества с Международным телеграфным союзом (ITU), пытающимся стать центральным международным агентством по управлению глобальным Интернетом (аналогично существующей практике в области телеграфной и телефонной связи).

Однако данный принцип вступает в противоречие с исторически сложившейся архитектурой Интернета, который задумывался как открытое мультистейкхолдерное пространство, в котором суверены присутствуют на равных правах со всеми участниками[1]. Формирование киберпространства происходило в рамках определенной идеологии, наиболее ярким выражением которой была «Декларация независимости киберпространства» американского поэта и политического активиста Джона Перри Барлоу:

> «Я объявляю глобальное социальное пространство, которое мы строим, естественным образом независимым от тирании, которую вы [правительства мира] стремитесь нам навязать. Вы не имеете морального права управлять нами, у вас также нет никаких методов правоприменения, которых нам стоит бояться. Правительства получают законную власть через согласие управляемых. Вы не искали от нас такого согласия и не получали его. Мы вас не приглашали… Киберпространство не лежит в ваших границах. Не думайте, что вы можете построить его… Вы не можете. Это явление природы, и оно растет само по себе через наши коллективные действия» [Barlow, 1996, p. 1].

При всей декларативности этого манифеста он содержит важные указания на то, что архитектура (или природа) цифрового пространства, действительно, создает почти непреодолимые препятствия для его регулирования правительствами. Киберанархизм имеет глубокие корни в

[1] Выделение в свое время домена. gov для государственных организаций ставило их в один ряд с образовательными учреждениями -. edu – и коммерческими компаниями -. com. Формальное наличие страновых доменов не создает достаточных оснований для национального суверенитета (вопреки мнению Уерпманна-Уитзака [Uerpmann-Wittzack, 2010, с. 1256]), поскольку значительное количество ведущих интернет-ресурсов зарегистрировано в межстрановых доменах, число которых было существенно расширено начиная с 2013 г.

движении хакеров, сложившемся в конце 1970-х годов[1]. В книге С. Леви «Хакеры. Герои компьютерной революции» отмечается, что многие из видных компьютерных активистов того времени перекладывали в киберпространство идеи хиппи 1960-х[2] [Levy, 1984].

Как указывает Лессиг, архитектура является одной из модальностей регулирования (наряду с законом, обществом и рынком). Поэтому в момент, когда Интернет привлек внимание государственных регуляторов, он уже эффективно регулировался изнутри. Таким образом, для кардинального изменения модальности регулирования киберпространства необходима, прежде всего, перестройка его архитектуры. По словам Лессига, «…хотя определенные версии киберпространства сопротивляются эффективному регулированию, это не означает, что любая версия киберпространства будет делать то же самое. Или, иначе, возможны версии киберпространства, в которых поведение будет регулироваться, и правительства могут предпринять шаги по усилению этой регулируемости» [Lessig, 1999, p. 506].

Такие идеи фактически были реализованы в достаточно многочисленных проектах создания «управляемого национального Интернета». Прежде всего, это «Великий файрволл» Китая, а также Иран, Туркменистан и т.д., не говоря уже о многочисленных случаях временных мер по ограничению Интернета, принимавшихся правительствами разных стран. Проблема состоит в том, что подобные ограничения неизбежно ставят национальных пользователей в неравные конкурентные условия на глобальном рынке, что является чувствительным для бизнеса и образовательных организаций. Развитые и успешные закрытые национальные сети, вроде французской Minitel, проиграли в свое время рыночную конкуренцию Интернету именно по причине его функционального превосходства [Орловский, Коровкин, 2020].

«Государствоцентричность» подхода российской концепции представляется слабостью даже тем аналитикам, которые в целом ей симпатизируют. Так, О. Демидов указывает, что «логика концепции Конвенции не позволяет документу охватить субъектов, которые в общем-то наполняют мировую систему коммуникаций содержанием и без которых информационный обмен невозможен» [Демидов, 2013, с. 140]. Однако расширить охват с тем, чтобы отразить в нем мультистейкхолдерную модель управления киберпространством невозможно с юридической точки зрения. Это фактически наделило бы субъектов внутригосударственного права разных государств международной правовой субъектностью [Пазюк, 2012, с. 238]. По этой причине реализация российского

[1] Тогда слово «хакер» не имело негативных коннотаций и использовалось для программистов, умеющих решать нестандартные задачи, связанные с организацией компьютерных сетей в условиях неразвитой инфраструктуры. Хотя часть хакеров пользовались несанкционированным доступом к телефонным сетям и довольно свободно относилиась к интеллектуальной собственности, их действия не имели конечной цели нанесения ущерба.

[2] В какой-то мере продолжение этих идей можно проследить в движении за создание децентрализованных криптовалют, основанном на манифесте Сатоши Накамото (псевдоним).

подхода в отношении глобального киберпространства требует де-факто национализации ряда институтов, составляющих сейчас архитектуру Интернета.

Российская правовая школа смотрит на национализацию следующим образом: «…институт национализации необходим для обеспечения поступательного экономического развития страны… позволяет преодолеть индивидуализм участников гражданско-правовых отношений и провести идею общественного интереса (общеполезности, общего блага, публичного интереса)» [Щенникова, 2012][1]. В противоположность этому современная англо-американская правовая школа фактически отказывается рассматривать национализацию как институт, считая ее возможной лишь в качестве чрезвычайно исключительной временной меры (economic emergency) [Davidson, 2014]. Таким образом, архитектурная перестройка глобального киберпространства, необходимая для его организации в виде совокупности национальных киберпространств, представляется в настоящее время нереалистичной.

Ценности

В самом простом выражении ценности задают степень важности вещей, событий или действий и через это определяют принятие сложных коллективных решений. При этом систему ценностей, присущих той или иной культуре, вполне можно реконструировать из анализа развернутых текстов, вычленяя в них центральные понятия.

Подобный анализ российского проекта Конвенции по международной информационной безопасности позволяет выделить следующие концепты, составляющие ценностный каркас документа [МИД РФ, 2011]:

- государственный суверенитет;
- безопасность и стабильность;
- традиционность.

По мнению специалистов, предложенный проект во многом является развитием идей, содержащихся в российских внутренних стратегических документах, применительно к международному праву. А сама ценностная конструкция «суверенитет – стабильность – традиционность» представляет собой перенесение в киберпространство идеологии «суверенной демократии», сформулированной в 2006 г. В. Сурковым (тогда заместителем главы Администрации Президента РФ), которая постепенно превратилась в доминирующую идеологему, предельно редко оспариваемую в отечественном публичном мейнстриме.

[1] При этом, однако, национализацию в России называют спящим институтом в силу отсутствия необходимого законодательства, закон о национализации разрабатывался на протяжении ряда лет, но так и не был принят, в частности в ноябре 2019 г. Госдума большинством голосов отвергла законопроект, предложенный КПРФ. (ИА Regnum, «Госдума отказалась принимать закон о национализации имущества», 12 ноября 2019 г., https://regnum.ru/news/economy/2775635.html).

По отдельности перечисленные ценности разделяются многими участниками глобального киберпространства. Так, китайская «Стратегия по сотрудничеству в киберпространстве» ставит суверенитет на второе место после «мира» в ряду основополагающих принципов, а «защиту суверенности и безопасности» на первое место среди целей. Французская стратегия также обращает внимание на вопросы суверенитета и уделяет заметное внимание сохранению культурной идентичности (прежде всего, путем продвижения в Интернет франкоязычного контента). Признание важности «безопасности» как таковой лежит в основе всех дискуссий по киберрегулированию. Однако ни одна из крупных стран-стейкхолдеров мирового Интернета не оперирует описанной ценностной конструкцией, когда суверенитет государства, стабильность и традиционность рассматриваются как тесно связанная группа концептов.

Подход «США и единомышленников» основан на существенно другой ценностной конструкции. Это не означает, что ценности российской концепции напрямую оспариваются. Просто им приписывается низкий приоритет относительно других ценностных концептов. Международная киберстратегия США 2011 г. открывается вступлением Барака Обамы, в котором утверждается, что «кибербезопасность – это не цель сама по себе, это обязательство, которое наши правительства и общества должны добровольно принять на себя, чтобы дать инновациям расцветать, развивать рынки и улучшать жизни» [White House, 2011].

В ценностях западного мира гораздо выше стоит динамизм – развитие и инновации, – отраженный в четвертом принципе У. Хейга или в следующей фразе из американской Международной стратегии для киберпространства: «США будут проводить международную политику в киберпространстве, которая усилит (empowers) инновации, развивающие нашу экономику и улучшающие жизни здесь и за границей» [White House, 2011, p. 4].

Аналогичным образом обстоит дело с государственностью как основой для суверенитета. Присутствие государства имеет смысл лишь в тех случаях и в той мере, в какой мультистейкхолдерная модель оказывается неэффективной в достижении общественного блага. До тех пор, пока правительства западных стран не видят неустранимых провалов, проистекающих из существующей модели управления киберпространством, они не видят причин вмешиваться. Отсутствие государства в центре ценностной модели почти автоматически исключает важность суверенитета как концепции.

Основной ценностью «западного» подхода является идея равенства всех участников киберпространства, с особенным уважением к коммерческим и академическим игрокам, непосредственно создавшим его. В этом проявляется как ценностный компонент, проистекающий из американского конституционного права на «стремление к счастью» (pursuit of happiness), так и исторически сложившийся мессианизм США, тесно связанный с ценностями свободы и открытости. «Прави-

тельства, которые уважают права своих граждан, не имеют причин бояться свободного Интернета»[1] [Pozner, 2011]. По словам У. Хейга, «существует растущее расхождение мнений и действий между странами, ищущими открытого будущего для Интернета, и теми, кто движется по пути государственного контроля. Мы верим, что недостаточно просто работать с угрозами в области экономики и безопасности без сохранения открытости и свободы, на которых основан его [Интернета] успех» [Foreign & Commonwealth Office, 2012].

Ценности открытости и свободы являются основополагающими и для французской киберстратегии.

Альтернативный ценностный каркас подхода к киберрегулированию США и их единомышленников можно сформулировать как «динамизм (инновации) – равенство всех участников (вплоть до принижения роли государства) – открытость (архитектурная и содержательная)». Несложно видеть, что он противоречит ценностям российской концепции. Однако придание этому противоречию чисто инструментальной перспективы – предположение, что оно является лишь переговорной позицией – глубоко ошибочно. Представители западного действительно не могут оперировать иной картиной мира. В свою очередь, и они глубоко ошибочно приписывают российской концепции лишь тактические цели, не осознавая ценностной конструкции, стоящей за ней.

Типология подходов к киберрегулированию

Полученные результаты согласуются с существующими типологиями отношений государства и общества. Так, Спенсер, Мурта и Линуэй в начале 2000-х годов применили к анализу роли государства в создании новых (инновационных) индустрий классификацию, предложенную Р.Л. Джепперсоном [Jepperson, 2000]. Тот выделил два измерения: тип коллективной агентской структуры (насколько «государственным» является общество) и тип организации общества (насколько оно «корпоративно»), что образовывало четыре возможных квадранта: 1) социальное корпоративное государство; 2) корпоративное государство; 3) либеральное плюралистское государство; 4) государственная нация [Spencer, Murtha, Lenway, 2005, p. 326].

В данной типологии США относились авторами к либерально-плюралистическим государствам. Россия (и другие незападные страны, за исключением Японии) ими не рассматривалась, однако она явно подходит под описание типа «государственная нация». Эти два типа не являются диаметрально противоположными. Они схожи по измерению организации общества – отсутствию сильных негосударственных институтов – «корпораций» в широком смысле слова (включая разного рода профессиональные ассоциации, академические сообщества и т.д.).

[1] Разумеется, это видение не разделяется во многих других странах мира. По мнению Захарова, «США используют угрозы и подкуп, склоняя к собственному пониманию демократии и неолиберальной экономической политики» [Захаров, 2018, с. 133], это утверждение отчасти справедливо, однако опять-таки приписывает инструментальный характер (удержание технического превосходства) действиям, имеющим ценностную природу.

Несколько иная типология может быть предложена, если в качестве измерений использовать роль государства в экономической (государство-организатор и государство-регулятор экономики) и политической (государство – идеологический лидер и деидеологизированное государство) жизни [Korovkin, 2018]. При такой классификации Россия оказывается в категории «супергосударств» (лидирующая роль в экономике и политике), а США и их единомышленники – в строго противоположной категории «государство как сервис».

В обоих случаях видно, что расхождение позиций по международному киберрегулированию имеет под собой глубокие различия во взглядах на роль государства, его мандат действий и способы взаимодействия государства и различных общественных институтов, включая бизнес.

Заключение

Г. Франкенберг указывал, что возможны четыре типа конституции: контракт, манифест, программа и закон [Frankenberg, 2006]. Эффективное международное право возможно лишь как контракт, так как оно требует согласия всех сторон, которое может быть получено лишь при наличии у них достаточно веских выгод. В случае, если зона согласия окажется слишком узкой, контракт вырождается в манифест – формально поддерживаемый всеми участниками, но не имеющий практических последствий в нормировании их действий. Это обстоятельство делает выработку международного законодательства чрезвычайно сложным процессом. Расхождения позиций сторон, безусловно, часто имеют инструментальную природу: стремление обеспечить нации наиболее выгодную конкурентную позицию на глобальных рынках. Однако эти же расхождения могут иметь под собой и более глубокую природу: различие правовых культур (и культур в широком смысле слова), выражающееся в несовместимости принципов и ценностей законотворчества.

Подобную несовместимость демонстрируют официальные материалы подходов к международному киберрегулированию России и США. В дальнейшем целесообразно дополнить исследование анализом позиций других важных стран-стейкхолдеров глобального киберпространства, например Японии или Индии.

Приходится констатировать, что имеющиеся культурные расхождения делают маловероятным достижение в обозримом будущем широкого международного консенсуса в области киберправа. Особую сложность здесь представляет мультистейкхолдерная архитектура киберпространства[1]. Вероятным сценарием является регионализация киберпространства, с созданием в нем союзов, основанных на взаимном доверии участников и единстве их взглядов на ключевые принципы киберрегулирования. Примерами таких союзов являются декларация ШОС, конвенция Африкан-

[1] В истории международного права уже есть пример провала попытки регулирования мультистейкхолдерной среды – долго осаждавшаяся конвенция ООН о транснациональных компаниях так и не была в итоге принята, вопрос постепенно ушел с повестки организации [Hedley, 1999].

ского союза по защите данных и законодательство по защите персональных данных ЕС. В какой-то мере глобальное киберпространство превращается в «лоскутное одеяло» норм и регулирований, затрудняющее действия добросовестных акторов (государственных и негосударственных), но открывающее недобросовестным многочисленные правовые лакуны и лазейки.

Список литературы

Демидов О. Обеспечение международной информационной безопасности и российские национальные интересы // Индекс безопасности. – 2013. – № 1 (104), т. 19, – С. 129–168.

Захаров Т.В. Международное сотрудничество государств в сфере информационной безопасности и правовые подходы к его регулированию // Государство и право в новой информационной реальности. – 2018. – № 1. – С. 119–134.

Зиновьева Е.С. Перспективные тенденции формирования международного режима по обеспечению информационной безопасности // Вестник МГИМО-Университета. – 2016. – № 4(49). – С. 235–247.

Коровкин В.В. Национальные программы цифровой экономики стран Ближнего Востока // Ars Administrandi (Искусство управления). – 2019. – Т. 11, № 1. – С. 151–175.

МИД РФ Конвенция об обеспечении международной информационной безопасности (концепция) / Министерство иностранных дел Российской Федерации. – 2011. – URL: https://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666 (дата обращения 03.04.2020.)

МИД РФ Response of the Special Representative of the President of the Russian Federation for International Cooperation on Information Security Andrey Krutskikh to TASS' Question Concerning the State of International Dialogue in This Sphere // Официальный сайт МИД РФ. – 2017. – 29.06. – URL: https://www.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2804288

Орловский В., Коровкин В. От носорога к единорогу. Как провести компанию через трансформацию в цифровую эпоху и избежать смертельных ловушек. – М.: Бомбара, 2020. – 367 с.

Пазюк А.В. Понятие международного информационного права как комплексной отрасли современного международного права // Актуальні проблеми міжнародних відносин. – 2012. – Випуск 111 (Частина І). – URL: https://digital.report/ponyatie-informatsionnogo-prava/ (дата обращения 02.04.2020).

Рахманина Т.Н. Актуальные вопросы кодификации российского законодательства // Журнал российского права. – 2008. – № 4(136). – С. 30–39.

Хужина А.В. Правовая природа сети Интернет: вопросы регулирования // Вестник ЮУрГУ. Серия «Право». – 2015. – Т. 15, № 1. – С. 101–107.

Щенникова Л.В. Гражданско-правовая наука о национализации // Вестник Пермского университета. Юридические науки. – 2012. – № 4. – С. 179–186.

Barlow J.P. A Declaration of the Independence of Cyberspace 1996 // Electronic Frontier Foundation. – 1996. – URL: https://www.eff.org/cyberspace-independence (дата обращения 02.04.2020).

Benedikt M. Introduction // Cyberspace: first steps / Michael Benedikt (ed.). – Cambridge: MIT Press, 1991 a. – P. 1–25.

Benedikt M. Cyberspace: Some Proposals // Cyberspace: first steps / Michael Benedikt (ed.). – Cambridge: MIT Press,1991 b. – P. 120–138.

Canale D. The Many Faces of the Codification of Law in Modern Continental Europe // A History of the Philosophy of Law in the Civil Law World / D. Canale, P. Grossi, H. Hofmann (ed.). – Dordrech: Springer, 2009. – P. 135–183.

Davidson N.M. Nationalization and Necessity: Takings and a Doctrine of Economic Emergency // Brigham-Kanner Property Rights Conf. (October 27, 2014). – 2014. – (Fordham Law Legal Studies Research Paper; N 2515333). – URL: https://ssrn.com/abstract=2515333 (дата обращения 05.04.2020.)

Department of State Explanation of Position at the Conclusion of the 2016–2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security / Department of State. – 2017. – URL: https://www.state.gov/explanation-of-position-at-the-conclusion-of-the-2016–2017-un-group-of-governmental-experts-gge-on-developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-sec/(дата обращения 05.04.2020).

Department of State International Law in Cyberspace, Remarks Harold Hongju Koh, Legal Advisor U.S. Department of State, USCYBERCOM Inter-Agency Legal Conference, (September 18, 2012) / Department of State. – 2017. – URL: https://2009–2017.state.gov/s/l/releases/remarks/197924.htm -un-group-of-governmental-experts-gge-on-developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-sec/ дата обращения 05.04.2020).

Easterbrook F. Cyberspace and the Law of the Horse / University of Chicago Legal Forum. – 1996. – 207 p.

Foreign and Commonwealth Office An open internet is the only way to suPort security and prosperity for all: Foreign Secretary speech at the Budapest Conference on Cyberspace. – 2012. – URL: https://www.gov.uk/government/organisations/foreign-commonwealth-office-un-group-of-governmental-experts-gge-on-developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-sec/ (дата обращения 03.04.2020).

Frankenberg G. Comparing constitutions: Ideas, ideals, and ideology – toward a layered narrative // International Journal of Constitutional Law. – 2006. – Vol. 4, N 3. – P. 439–459.

Hedley R. Transnational Corporations and Their Regulation: Issues and Strategies // International Journal of Comparative Sociology. – 1999. – Vol. 40, N 2. – P. 215–230.

Jepperson R.L. Institutional Logics: On the Constitutive Dimensions of the Modern Nation-State Polities. – Florence: European University Institute, 2000. – URL: https://cadmus.eui.eu/handle/1814/1676 (дата обращения 05.04.2020.)

Kerttunen M., Tikk E. Parabasis. Cyber-diplomacy in Stalemate / Norwegian Institute of International Affairs. – 2018. – URL: https://www.nupi.no/en/Publications/CRIStin-Pub/Parabasis-Cyber-diplomacy-in-Stalemate (дата обращения 05.04.2020).

Korovkin V. A digitally transformed state // BRICS Business Magazine. – 2018. – Vol. 21, N 2. – P. 46–55.

Levy S. Hackers: heroes of the computer revolution. – Doubleday, 1984. – 464 c.

Lessig L. The Law of the Horse: What Cyberlaw Might Teach // Harvard Law Review. – 1999. – N 113. – P. 501–549.

Lloyd W.F. Lloyd on the Checks to Population // Population and Development Review. – 1980. – N 6(3). – P. 473–496.

Ministere de l'Europe et des Affairs Etrangeres Stratégie internationale de la France pour le numérique / Ministere de l'Europe et des Affairs Etrangeres de France. – 2018. – URL: https://ch.ambafrance.org/Strategie-internationale-de-la-France-pour-le-numerique (дата обращения 05.04.2020).

Pozner M. Internet Freedom and Human Rights // American Rhetoric. – 2011. – URL: https://www.americanrhetoric.com/speeches/michaelposnerinetfreedomhumanrights.htm (дата обращения 03.04.2020).

Prakesh R., Baruah D.M. The UN and Cyberspace Governance // ORF Issue Brief. – 2014. – N 68. – URL: https://www.orfonline.org/wp-content/uploads/2014/03/IssueBrief_68.pdf (дата обращения 05.04.2020).

Roberts A. Is International Law International? – Oxford: Oxford University Press, 2017. – 420 p.

Schjolberg S., Ghernaouti-Helie S. A Global Treaty on Cybersecurity and Cybercrime // AiTOslo. – 2011. – URL: http://pircenter. org/media/content/files/9/13480907190.pdf. (дата обращения 03.04.2020).

Schmitt M. Tallinn Manual on the International Law Applicable to Cyber Warfare. – Cambridge: Cambridge University Press, 2013. – 215 c.

Schmitt M. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. – Cambridge: Cambridge University Press. – 2017. – 30 p.

Scott S.V. International Law as Ideology: Theorizing the Relationship between International Law and International Politics // European Journal of International Law. – 1994. – Vol. 5, N 3. – P. 313–325.

Spencer J., Murtha T., Lenway S. How Governments Matter to New Industry Creation // AMR. – 2005. – N 30. – P. 321–337. – URL: https://doi.org/10.5465/amr.2005.16387889 (дата обращения05.04.2020).

Stadnik I. A New Cybersecurity Diplomacy: Are States Losing Ground in Normmaking? // Russian Council on International Affairs. – 2018. – URL: https://russiancouncil.ru/en/analytics-and-comments/analytics/a-new-cybersecurity-diplomacy-are-states-losing-ground-in-norm-making/ (дата обращения 05.04.2020).

Uerpmann-Wittzack R. Principles of International Internet Law // German Law Journal. – 2010. – Vol. 11, N 11. – P. 1245–1263.

Van Hoecke M. Methodology of Comparative Legal Research // Law and Method. – 2015. – C. 1–35.

White House International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World / Office of President of the United States. – 2011. – URL: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (дата обращения 0504.2020).

Xinhua International Strategy of Cooperation on Cyberspace 2017 // Xinhuanet.com. – 2017. – URL: http://www.xinhuanet.com//english/china/2017–03/01/c_136094371_2.htm (дата обращения 05.04.2020).