КОВРИГИН Дмитрий Эльдарович – аспирант департамента политологии факультета социальных наук и массовых коммуникаций Финансового университета при Правительстве РФ (125993, Россия, г. Москва, ГСП-3, Ленинградский пр-кт, 49; dmitrykovr@gmail.com)

ГРАНИЦЫ ГОСУДАРСТВЕННОГО СУВЕРЕНИТЕТА НАЦИОНАЛЬНОГО СЕГМЕНТА КИБЕРПРОСТРАНСТВА

Аннотация. *Целью данной статьи является изучение феномена киберпространства как нового социального института. Анализируются различные интерпретации понятия киберпространства в российских и зарубежных исследованиях. Национальный сегмент киберпространства включает как самостоятельные сегменты общества и государства, так и общий сегмент общества и государства. Автор определяет киберпространство как гибридное пространство, включающее совокупность технической инфраструктуры и субъектов коммуникационных, технологических, регуляторных процессов. Автор исследует проблему определения границ государственного суверенитета в национальном сегменте киберпространства и заключает, что границам государственного суверенитета в национальном сегменте киберпространства соответствует система подчиненных юрисдикции государства взаимоотношений участников коммуникационных, технологических, регуляторных процессов киберпространства.*

Ключевые слова: *киберпространство, государственное регулирование, национальный сегмент киберпространства, границы киберпространства*

С распространением Интернета началось развитие киберпространства. 69,0% населения мира пользуются Интернетом. В России насчитывается примерно 129,8 млн пользователей Интернета, что составляет 89,0% всего населения[1], а также насчитывалось 227,3 млн мобильных подключений. Сам термин «киберпространство» позаимствован современной наукой из научно-фантастического рассказа Уильяма Гибсона «Сожжение Хром» (*Burning Chrom*, 1982 г.) [Данельян 2020: 262].

М. Лакоми определяет киберпространство как нематериальное пространство, которое основано на передаче цифровых сигналов и электромагнитного излучения [Lakomy 2015: 83]. При этом киберпространство функционирует благодаря инфраструктуре ИКТ, производящей и передающей данные сигналы. Данная область предназначена для обработки, хранения и передачи информации в цифровом формате. Д.Э. Деннинг определяет киберпространство как информационное пространство, созданное совокупностью всех компьютерных сетей [Denning 1999: 24]. Схожее определение дал Г.Дж. Рэттрей, в соответствии с которым киберпространство – это физическая область, являющаяся результатом создания информационных систем и сетей, которые обеспечивают взаимодействие благодаря электронной коммуникации [Rattray 2004: 30]. Г. Пиларский определяет киберпространство как среду, которую используют в основном для человеческого общения и социального взаимодействия [Pilarski 2020: 99]. А.А. Данельян определяет киберпространство как комбинацию компьютеров, мобильных устройств, а также пользователей, взаимодействующих между собой на расстоянии. Особо подчеркивается, что киберпространство шире, чем Интернет, который используется для подключения устройств. Таким образом, Интернет находится внутри киберпространства. А.А. Данельян ука-

[1] Internet USAGE Statistics. The Internet Big Picture World Internet Users and 2022 Population Stats. URL: datareportal.com/reports/digital-2022-russian-federation (accessed 16.12.2022).

зывает на то, что на современном этапе киберпространство можно назвать основным каналом распространения информации [Данельян 2020: 262]. В свою очередь, Б. Уильямс определяет киберпространство, как искусственную область, которая формируется при подключении всех устройств, позволяющих перемещать большие объемы данных с высокой скоростью[1].

Киберпространство – это многосоставное понятие. Д. Кларк выделил четыре уровня киберпространства. Первый – это физический уровень (технологическое обеспечение, необходимое для функционирования киберпространства: ПК, серверы, суперкомпьютеры, Интернет и другие виды сетей и каналов связи). Поскольку технологические центры, точки передачи данных, хранилища данных находятся в одном месте, они подпадают под государственное регулирование. Второй – это логический уровень (ПО, приложения, алгоритмы, базы данных). Третий – это уровень контента, или информационный уровень (информация, контент, циркулирующий в киберпространстве). Четвертый – это социальный уровень (все люди, которые влияют на формирование киберпространства, – от производителей ПО и руководителей *IT*-компаний до обычных пользователей социальных сетей) [Clark 2010: 1]. В соответствии с определением Дж. Басселл, под киберпространством понимается «аморфный и предположительно "виртуальный" мир, который образован связями между устройствами, обладающими поддержкой, а также компонентами самой инфраструктуры Интернета»[2], что делает определение киберпространства и Интернета не релевантными друг другу.

В документах Министерства обороны США киберпространство трактуется как глобальная область в информационной среде, которая состоит из взаимозависимых сетей инфраструктур информационных технологий и постоянных данных, таких как Интернет, телекоммуникационные сети, компьютерные системы, встроенные процессоры и контроллеры[3]. В Глоссарии терминов НАТО киберпространство определяется как глобальная область, которая состоит из всей совокупности взаимосвязанных коммуникационных, информационных технологий и других электронных сетей, систем и данных. В него входят разделенные и независимые системы для хранения, обработки и передачи данных[4]. Европейская комиссия определила киберпространство как виртуальное пространство, в котором электронные данные компьютеров циркулируют по всему миру[5]. В данных определениях рассматриваются информационный, структурный и технологический уровни киберпространства, но не уделяется внимание людям и коммуникационному процессу между ними, для чего данное пространство и существует.

А.Е. Войскунский считает такие термины, как киберсреда, киберпространство и интернет-пространство, синонимами. Виртуальное пространство, несмотря на свою нематериальность, обладает определенными топологическими признаками, среди которых можно выделить расстояния, маршруты,

---

[1] Cyberspace: What is it, where is it and who cares? URL: armedforcesjournal.com/cyberspace-what-is-it-where-is-itand-who-cares/ (accessed 02.01.2023).

[2] Cyberspace. URL: www.britannica.com/topic/cyberspace (accessed 27.01.2023).

[3] Department of Defense Dictionary of Military and Associated Terms. URL: fas.org/irp/doddir/dod/jp1_02.pdf (accessed 02.01.2023).

[4] NATO Glossary of Terms and Definitions AAP-06 Edition 2018. URL: nso.nato.int/nso/ZPUBLIC/_BRANCHINFO/TERMINOLOGY_PUBLIC/NON-CLASSIFIED%20NATO%20GLOSSARIES/AAP-6.PDF (accessed 02.01.2023).

[5] Glossary and Acronyms (Archived). URL: ec.europa.eu/information_society/tl/help/glossary/index_en.htm#c (accessed 02.01.2023).

скорость, очередность, трафики и перевалочные пункты пересылки сообщений [Войскунский 2020: 440].

Институты общества находят свое отражение в киберпространстве и трансформируются под его воздействием. Киберпространство как является инструментом других институтов общества, так и само обладает определенными функциями института [Мигулева 2020: 201].

В зарубежных исследованиях более популярны термины «киберсреда» и «киберпространство», а в российском – «информационное пространство» или «Интернет». В.Л. Гирич и В.Н. Чуприна определяют информационное пространство как совокупность информационных ресурсов и инфраструктур, составляющих компьютерные сети, на государственном и межгосударственном уровнях [Гирич, Чуприна 2007: 1]. Также в данную систему входят телекоммуникационные системы, сети общего пользования вместе с иными трансграничными каналами передачи информации. В указе Президента РФ «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» информационное пространство определяется как «совокупность информационных ресурсов, созданных субъектами информационной сферы, средств взаимодействия таких субъектов, их информационных систем и необходимой информационной инфраструктуры»[1].

А.В. Манойло указывает, что информационное пространство состоит из трех элементов: информационного поля, информационных потоков, а также каналов коммуникации средств массовой информации и массовой коммуникации [Манойло 2003: 71-73]. Производители и потребители информации являются как объектами, так и субъектами данного пространства. Таким образом, можно утверждать, что информационное пространство есть многокомпонентная структура, базирующаяся на каналах коммуникации [Добровольская 2014: 144].

Киберпространство – это составной элемент информационного пространства, основывающийся на совокупности всех цифровых устройств, осуществляющих передачу информации, всех программ, контролирующих потоки данной информации, всей информации, находящейся в обращении и в доступе, и всех людей, взаимодействующих с этой информацией. Данное пространство поддерживается и регулируется компаниями, отвечающими за технику и программы. Киберпространство обладает признаками физического пространства, у сообщений в нем есть точка отправки и получения, маршрут следования, скорость движения, расстояние, которое необходимо преодолеть, и время движения. Данное пространство обладает гибридным характером, т.к. его элементы являются как физическими (люди и техника), так и виртуальными (программы и информация).

Таким образом, можно определить киберпространство как созданное для обмена информацией гибридное пространство, формируемое из совокупности всех информационных устройств, хранящих, обрабатывающих и передающих информацию, субъектов коммуникационных, технологических, регуляторных процессов.

Следствием мировой технологической трансформации стал рост трансграничного влияния цифровых корпораций, которые не только занимаются сбором информации о своих пользователях, но и стремятся получить монополию на предоставление права на коммуникацию. Это является прямой угрозой для

[1] Указ Президента РФ «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» от 09.05.2017. № 203. Доступ: http://www.kremlin.ru/acts/bank/41919 (проверено 23.12.2022).

информационной безопасности не только отдельного человека, но и государства в целом. Как отмечает С.В. Володенков, следствием данного процесса стало включение государственного суверенитета в принципы цифровой политики [Володенков, Федорченко 2022: 91].

Киберпространство стало новой сферой общественных отношений, которую государство как главный общественный институт должно регулировать. Так, благодаря социальным сетям повышается легкость организации массовых политических акций, что уже демонстрирует необходимость развития государственного регулирования [Дорожкин, Гаеткулов 2022: 118]. Киберпространство является новым типом пространства, и, как следствие, в нем можно устанавливать территории и границы. В соответствии с законом РФ «О Государственной границе Российской Федерации» под государственной границей понимается «линия и проходящая по этой линии вертикальная поверхность, определяющие пределы государственной территории»[1]. Границы государства определяют пределы действия государственного суверенитета в пространстве. Невозможно применить все свойства реальных физических границ государства и государственной территории к киберпространству из-за его изменчивости и частичной нематериальности. Это заставляет искать новое определение границ, которое подойдет для современной гибридной реальности. Происходит разработка систем наименований, терминов и категорий, а также регулирования новых технологий [Мухаметов 2020: 59].

В пределах своей территории современное государство осуществляет полную юрисдикцию, что верно не только в отношении материального, но и виртуального пространства. Право государства на независимое управление в национальном сегменте киберпространства является наиболее часто используемым признаком суверенитета государства в киберпространстве [Даниленков 2017: 157]. Часто используется подход, в соответствии с которым суверенитет государства осуществляется в форме контроля над физическим уровнем киберпространства, в частности его техническим обеспечением. Но техническая и технологическая базы одного государства тесно взаимосвязаны с другими государствами, персонализированные и анонимные акторы динамичны, а информационный контент и коммуникации трансграничны.

Из-за экстратерриториальной природы киберпространства встает проблема разграничения территориальной и экстратерриториальной юрисдикции современных государств [Липкина 2021: 156]. Интернациональность киберпространства и легкая доступность в нем информации порождает ситуации как отсутствия юрисдикции, так и мультиюрисдикции. В случае отсутствия юрисдикции ни один из судов не считает себя ответственным за ситуацию, а в случае мультиюрисдикции возникает конфликт юрисдикций, т.е. несколько судов признают себя компетентными в разрешении дела. Второй вариант наиболее распространен в условиях киберпространства [Терентьева 2021: 238].

Суверенитет всего киберпространства невозможен, т.к. управление *IT*-инфраструктурой, поддерживающей его функционирование, распределено между множеством акторов (физические и юридические лица, независимые компании, государственные компании, государства, союзы государств и т.д.). Таким образом, ни один из акторов не может владеть всеми элементами данной системы, а как следствие – и контролировать все киберпространство.

---

[1] Закон РФ от 01.04.1993 N 4730-1 (ред. от 30.12.2021) «О Государственной границе Российской Федерации». Доступ: https://www.consultant.ru/document/cons_doc_LAW_3140/6deec6b3c7f8b22d3272c9f1368efacd85dac515/ (проверено 09.01.2023).

Контроль за национальным сегментом глобального киберпространства возможен, как видно на примере «Великого китайского файрвола».

Суверенитет государства основывается на праве осуществлять свою власть на данной территории. Это дает государству контроль над физическими основами киберпространства, расположенными на его территории или подпадающими под его юрисдикцию. Сюда входит и контроль за дата-центрами, пунктами передачи данных, контроль за компаниями, работающими в данной сфере, контроль за гражданами государства, взаимодействующими с всеобщим (мировым) киберпространством, а также за действиями иностранных граждан, взаимодействующих с вышеперечисленными элементами. Также в сферу регулирования государством входит информация, производимая, хранящаяся и распространяемая подконтрольными государству субъектами. Национальная кибербезопасность включает в себя не только правовое регулирование данного пространства, но и развитие цифровой культуры граждан [Никипорец-Такигава, Бучнев 2020: 73].

Границы государственного суверенитета в национальном сегменте киберпространства определяются системой подчиненных юрисдикции государства взаимоотношений участников коммуникационных, технологических, регуляторных процессов киберпространства.

Список литературы

Войскунский А.Е. 2020. Психология киберсреды: два исследовательских подхода. – *Экопсихологические исследования – 6: экология детства и психология устойчивого развития*. № 6. С. 439-443.

Володенков С.В., Федорченко С.Н. 2022.Традиционные политические институты в условиях цифровизации: риски и перспективы трансформации. – *Дискурс-Пи*. Т. 19. № 1. С. 84-103.

Гирич В.Л., Чуприна В.Н. 2007. Глобальное информационное пространство и проблема доступа к мировым информационным ресурсам. – *Российская государственная библиотека*. Доступ: http: olden.rsl.ru/upload/mba2007/mba2007_05.pdf (проверено 23.12.2022).

Данельян А.А. 2020. Международно-правовое регулирование киберпространства. – *Образование и право*. № 1. С. 261-269.

Даниленков А.В. 2017. Государственный суверенитет Российской Федерации в информационно-телекоммуникационной сети «Интернет». – *Lex Russica*. № 7(128). С. 154-165.

Добровольская И.А. 2014. Понятие «Информационное пространство»: различные подходы к его изучению и особенности. – *Вестник РУДН*. Сер. Литературоведение, журналистика. № 4. С. 140-147.

Дорожкин Ю.Н., Гаеткулов Э.Н. 2022. Цифровая трансформация гражданского протестного участия в современной России. – *Гуманитарные науки. Вестник Финансового университета*. Т. 12. № 2. С. 115-121.

Липкина Н.Н. 2021. Принципы установления экстратерриториальной юрисдикции государства в киберпространстве в контексте правовых позиций Европейского суда по правам человека. – *Правовая политика и правовая жизнь*. № 2. С. 153-160.

Манойло А.В. 2003. *Государственная информационная политика в особых условиях:* монография. М.: Изд-во МИФИ. 388 с.

Мигулева М.В. 2020. Киберпространство как социальный институт: признаки, функции, характеристики. – *Дискурс-Пи*. № 4(41). С. 199-212.

Мухаметов Д.Р. 2020 Политические риски и барьеры цифровизации. – *Гуманитарные науки. Вестник Финансового университета*. Т. 10. № 4. С. 58-64.

Никипорец-Такигава Г.Ю., Бучнев Е.В. 2022. Методологические проблемы формирования концепции национальной кибербезопасности Российской Федерации. – *Гуманитарные науки. Вестник Финансового университета*. Т. 12. № 1. С. 70-74.

Терентьева Л.В. 2021. Установление судебной юрисдикции по спорам в киберпространстве на примере США. – *Право. Журнал Высшей школы экономики*. № 2. С. 236-260.

Clark D. 2010. *Characterizing Cyberspace: Past, Present and Future*. ECIR Working Paper No. 2010-3. MIT Political Science Department. 18 p.

Denning D. 1999. *Information Warfare and Security.* N.Y.: ACM Press. 522 p.

Lakomy M. 2015 *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*. Katowice: Wydawnictwo Uniwersytetu Śląskiego. 448 p.

Pilarski G. 2020. Cyberspace as a Tool of Contemporary Propaganda. – *Safety & Defense*. Vol. 6. Is. P. 95-108.

Rattray G.T. 2004. *Strategic Warfare in Cyberspace*. MIT Press. 517 p.

KOVRIGIN Dmitry Eldarovich, postgraduate student of the Department of Political Science, Faculty of Social Sciences and Mass Communications, Financial University under the Government of the Russian Federation (49 Leningradsky Ave, GSP-3, Moscow, Russia, 125993; dmitrykovr@gmail.com)

THE BOUNDARIES OF STATE SOVEREIGNTY OF THE NATIONAL SEGMENT OF CYBERSPACE

Abstract. *The aim of this article is to study the phenomenon of cyberspace as a new social institution. Various interpretations of the concept of cyberspace in Russian and foreign studies are analyzed. The national segment of cyberspace is considered as a new institution, including both independent segments of society and the state, and a common segment of society and the state. The author defines cyberspace as a hybrid space that includes a set of technical infrastructure and subjects of communication, technological, regulatory processes. The author explores the problem of defining the boundaries of state sovereignty in the national segment of cyberspace, and concludes that the boundaries of state sovereignty in the national segment of cyberspace correspond to the system of relations of participants in the communication, technological, regulatory processes of cyberspace subordinate to the jurisdiction of the state.*

Keywords: *cyberspace, state regulation, national segment of cyberspace, boundaries of cyberspace*