Vestnik RUDN. International Relations. ISSN 2313-0660 (print), ISSN 2313-0679 (online)
Вестник РУДН. Серия: МЕЖДУНАРОДНЫЕ ОТНОШЕНИЯ
2022 Vol. 22 No. 2 238—255
http://journals.rudn.ru/international-relations

DOI: 10.22363/2313-0660-2022-22-2-238-255

Научная статья / Research article

Секьюритизация информационного пространства: от конструирования норм до создания правовых режимов

М.С. Рамич ✉, Д.А. Пискунов

Российский университет дружбы народов, Москва, Российская Федерация
✉ramich-ms@rudn.ru

Аннотация. С развитием информационно-коммуникационных технологий (ИКТ) сеть Интернет стала приобретать большее значение с точки зрения национальной безопасности, экономического развития и мирового лидерства. Конфликты и спорные вопросы, возникающие в информационном пространстве, требуют согласования норм и выработки инструментов правового регулирования. Авторы статьи рассматривают процесс конструирования норм в информационном пространстве с точки зрения теории «сетевого общества» М. Кастельса и теории секьюритизации. По мнению М. Кастельса, в «сетевом обществе» произошла смена ключевых вызовов и угроз, а управление им стало осуществляться за счет инструментов контроля над информацией и формирования фреймов. Вместе с тем авторы, анализируя развитие сети Интернет с точки зрения концепции секьюритизации, приходят к выводу, что информационное пространство стало полноценным политическим пространством с центральным положением «цифрового суверенитета» и информационной безопасности. В статье впервые предлагается комплексная периодизация процесса трансформации международных отношений в информационном пространстве. Возникновение в информационном пространстве точек напряженности, которые несут экономические и политические риски, побуждает государственных акторов к формированию предварительного регулирования и согласованию норм поведения в информационном пространстве. Такой процесс конструирования предварительного регулирования был начат под эгидой ООН в рамках двух механизмов, созданных США и Россией. Эти механизмы стали площадкой для продвижения концепций регулирования и создания правовых режимов. В заключении авторы анализируют иерархию акторов в глобальном управлении информационным пространством с целью оценить влияние акторов на создание правовых режимов. Основными критериями оценки выступают способность влиять на глобальные цепочки производства высокотехнологичных товаров, проводить наступательные и оборонительные кибероперации и влиять на формирование международно-правовых режимов. Среди таких акторов авторы выделяют две группы: rule maker, способных воздействовать на глобальное информационное пространство и конструировать правовые режимы, и rule taker, которые выступают объектом конкуренции держав в информационном пространстве.

Ключевые слова: сетевое общество, информационное пространство, секьюритизация, США, КНР, Россия

Для цитирования: *Рамич М. С., Пискунов Д. А.* Секьюритизация информационного пространства: от конструирования норм до создания правовых режимов // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2022. Т. 22, № 2. С. 238—255. https://doi.org/10.22363/2313-0660-2022-22-2-238-255

The Securitization of Cyberspace: From Rulemaking to Establishing Legal Regimes

Mirzet S. Ramich ✉, **Danil A. Piskunov**

Peoples' Friendship University of Russia (RUDN University), Moscow, Russian Federation

✉ramich-ms@rudn.ru

Abstract. With the development of information and communication technologies (ICTs), the Internet has become increasingly important in terms of national security, economic development, and global leadership. Apparently, conflicts and contentious issues in cyberspace requires creating rules and development of regulation. The authors examine the process of making up rules in cyberspace from the perspective of M. Castells' network society theory and B. Buzan' securitization theory. According to M. Castells, key challenges have gradually altered in the network society and power relations and social management are based on the control of communication and information which embraces a network society. Furthermore, the authors investigate the development of the Internet in the context of securitization theory. It is stressed that cyberspace has become a full-fledged political space with the central position of digital sovereignty and information security. The article for the first time proposes a comprehensive periodization of international relations' transformation in cyberspace. Afterwards, the authors consider the appearance of tensions between actors in cyber space, which include political and economic threats. It encourages state actors to establish a preliminary regulation and to agree on norms regulating state behavior in cyberspace. These mechanisms have become a venue for promoting different concepts of cyber law and establishing legal regimes. In conclusion the authors analyze the hierarchy of actors in global Internet governance to assess the actors' influence on the establishment of legal regimes in cyberspace. The main assessment criteria are as follows: ability to influence global production chains of high-tech goods, ability to conduct offensive and defensive cyber operations, and influence on the formation of international legal regimes. The authors divide actors into two major groups — rule-markers capable of influencing the global information space and constructing legal regimes, and rule-takers that are an object of great powers competition in cyberspace.

Key words: network society, cyberspace, securitization, US, China, Russia

For citation: Ramich, M. S., & Piskunov, D. A. (2022). The securitization of cyberspace: From rulemaking to establishing legal regimes. *Vestnik RUDN. International Relations*, 22(2), 238—255. https://doi.org/10.22363/2313-0660-2022-22-2-238-255

Введение

Развитие и внедрение информационно-коммуникационных технологий (ИКТ) в конце XX — начале XXI в. привело к повышению уровня цифровизации общества и экономики государств. В таких условиях с точки зрения национальной безопасности государства на первый план выходит информационная безопасность, которая подразумевает обеспечение функционирования инфраструктурных объектов, ограничение иностранного влияния и управление внутренним сегментом сети Интернет. Критическая важность информационной безопасности обусловлена, во-первых, отсутствием всеобъемлющего правового регулирования отношений между государствами в киберпространстве, во-вторых, присутствием негосударственных акторов в сети Интернет, влияющих на информационную безопасность государств и, в-третьих, ролью информационной безопасности в процессах социального управления обществом.

В сети Интернет возникают точки напряженности и конфликты, которые подталкивают государства к выработке норм и правил взаимодействия в киберпространстве. Такие конфликты свидетельствуют о критической важности управления информационным пространством и обеспечения безопасности национальных объектов инфраструктуры. Этот факт усиливается тем, что в постбиполярный период фактор ядерного оружия и жестко-силового противостояния становится

менее актуальным[1]. Это ведет к формированию предпосылок к выработке правил и норм ответственного поведения в информационном пространстве для государственных акторов.

С точки зрения регулирования киберпространства можно выделить два подхода — концепцию Запада (США + ЕС) и концепцию развивающихся стран (Китай + Россия) (Международная информационная безопасность: теория и практика, 2019; Зиновьева, 2019b). В них сформированы принципы в отношении таких ключевых вопросов, как информационная безопасность, развитие сети Интернет, глобальное управление киберпространством, администрирование внутренней сети Интернет и т. д. (Дегтерев, Рамич, Пискунов, 2021, с. 9). Конкуренция двух концепций обусловлена не только преимуществами с точки зрения национальной безопасности, но и усиливающимся противостоянием США и КНР на мировой арене (Данилин, 2020b; Дегтерев, Рамич, Цвык, 2021, с. 220).

Ключевым аспектом американо-китайской конфронтации выступает именно технологическая сфера, где обе стороны продвигают свои технологические экосистемы, начиная от концепций управления Интернетом и заканчивая технологическими сервисами и передовыми разработками (Данилин, 2020a; Xingdong & Du, 2019, p. 47). Технологическая конкуренция США и КНР важна ввиду того, что сегодня социальные сети и другие сервисы оказывают большое влияние на распространение социальных ценностей, идей и норм, которые формируют основу социального управления и создание образа восприятия государства (Castells, 2013). С точки зрения информационного влияния США и КНР конкурируют за глобальное распространение социальных приложений (TikTok, WeChat, Facebook[2], Google и др.) своих технологических корпораций (Данилин, 2020b).

Развитие сети Интернет и повсеместное внедрение ИКТ привело к оформлению «сетевого общества», в котором власть конструируется посредством контроля над коммуникацией в сети (Castells, 2011). В контексте теории «сетевого общества» М. Кастельса релевантным становится рассмотрение власти в формирующемся глобальном сетевом обществе, в котором власть того или иного актора будет конструироваться за счет установленных норм и правил поведения в киберпространстве.

Подходящим примером формирования правил поведения выступает регулирование в сфере ядерного оружия (Nye, 2011, p. 18). Дж. Най проводит сравнительный анализ конструирования норм и правил в сфере ядерного оружия и в киберпространстве (Nye, 2011, p. 22). По мнению американского исследователя, опыт конструирования правил поведения в ядерной сфере применим к информационному пространству ввиду того, что сеть Интернет и информационная безопасность выходят на первый план для государств с высоким уровнем цифровизации экономики и использования ИКТ на инфраструктурных объектах военного и гражданского назначения (Nye, 2016, p. 46).

В данной работе используется методологический инструментарий, в основе которого лежат теория «сетевого общества» и теория секьюритизации (раздел I), которые позволяют комплексно исследовать вопрос секьюритизации информационного пространства и предложить авторскую периодизацию этого процесса в зависимости от характера угроз и межгосударственного взаимодействия (раздел II). Проблемы отсутствия регулирования в информационном пространстве были показаны на примере точек напряженности (раздел III), после чего дается обзор процесса предрегулирования в данной сфере и представлены основные проекты международно-правовых режимов (раздел IV). В завершающей части статьи авторы предлагают свой взгляд на иерархию системы глобального

[1] Lewis J. A. Technological Competition and China // Center for Strategic and International Studies. November 30, 2018. URL: https://www.csis.org/analysis/technological-competition-and-china (accessed: 26.02.2022). См. также: (Дегтерев, Рамич, Пискунов, 2021; Zhao, 2021, p. 3).

[2] 21.03.2022 г. Тверской районный суд г. Москвы удовлетворил иск Генпрокуратуры РФ и признал деятельность соцсетей Instagram и Facebook, принадлежащих Meta, экстремистской, запретив их работу в России.

управления в информационном пространстве (раздел V). В заключении резюмируются основные положения по каждому из исследованных аспектов и даются прогнозы относительно будущего системы глобального управления в информационном пространстве.

I. Методология

Выбор методологического инструментария обусловливается комплексным характером проблем в информационном пространстве, для анализа которых необходимо использовать междисциплинарный подход. В данной статье основу методологии составляют теория секьюритизации и теория «сетевого общества».

В XXI в. информационное пространство стало полноценным политическим пространством, на которое частично сместился фокус во всех сферах международных отношений, начиная от социально-экономического взаимодействия и заканчивая вопросами международной безопасности. Трансформацию характера угроз и межгосударственного взаимодействия в информационном пространстве можно проследить через призму теории секьюритизации, которая была предложена представителями Копенгагенской школы (Buzan, 1983; Buzan & Wæver, 2003; Buzan & Hansen, 2009; Hansen & Nissenbaum, 2009). Данная теория обеспечивает устойчивую методологическую основу для исследования вопросов безопасности в информационном пространстве, так как проблемы в цифровом домене не существуют в вакууме и чаще всего носят глобальный характер, оказывая влияние на международную систему без привязки к государственным границам (Hjalmarsson, 2013, p. 4). В данной статье авторы предлагают сопоставить трансформацию проблем безопасности и международного регулирования информационного пространства, сравнив характер угроз, основных акторов и международные правовые режимы, чтобы проследить хронологию секьюритизации информационного пространства начиная с момента создания Интернета (табл. 1). Технологическое развитие и увеличение пользователей ИКТ создало прецедент для перехода угроз из физического домена в цифровой, где система взаимодействия между акторами представляется анархичной и не контролируется общепринятыми нормативно-правовыми режимами.

За счет специфики информационного пространства изменился и характер так называемых «узких мест», или точек напряженности, в информационном пространстве. Если изначально наиболее уязвимыми местами цифрового домена считалась критическая инфраструктура — корневые серверы и т. д., то вместе с эволюцией характера взаимодействия и угроз точки напряженности стали «виртуальными».

В социальной сфере также происходили беспрецедентные трансформации. Менялся характер поведения пользователей, а государства, в свою очередь, адаптировали свою политику к новым реалиям. Общество стало переходить на коммуникацию посредством устройств, подключенных к глобальной сети Интернет. На данный момент более 4,8 млрд человек используют Интернет, и большая часть (90 %) выходят в Интернет с мобильных устройств[3]. Вместе с тем стали происходить изменения в природе власти в обществе. Традиционная власть, как правило, применяющая методы наказания и запугивания, стала трансформироваться в сетевую власть, которая реализуется посредством создания (*framing*) идей и контроля над коммуникацией (Castells, 2011; 2013). Теория «сетевого общества» позволяет рассматривать власть государства в сетевом обществе как критический аспект национальной безопасности, так как иностранное влияние на общество извне способно подорвать установленные идеи и фреймы общества и впоследствии получить механизмы управления обществом.

По М. Кастельсу, властные отношения в сетевом обществе являются основой, а созданные в нем институты и нормы необходимы для продвижения интересов и ценностей этой власти (Castells, 2011). Главной характеристикой такого общества является формирование властных отношений, в которых властную позицию занимают институты управления сетевым обществом, в том числе медиа-

[3] Digital Around the World // DataReportal. URL: https://datareportal.com/global-digital-overview (accessed: 08.01.2022).

компании, технологические компании и политические институты, осуществляющие глобальное управление и надзор.

Будучи новым политическим пространством, информационное пространство играет важную роль не только в рамках вопросов влияния и управления в сетевом обществе, но и в контексте современных международных экономических и политических отношений. Такие отношения, формируемые между государственными и негосударственными акторами, требуют правил поведения и норм, однако на данный момент отсутствует полноценное регулирование взаимоотношений в этой сфере. Релевантным примером конструирования норм поведения является выработка правил поведения в сфере ядерного оружия, описанная Дж. Наем (Nye, 2011).

II. Секьюритизация информационного пространства

Процесс секьюритизации в информационном пространстве можно разделить на несколько этапов в зависимости от основных акторов, характера угроз и международно-правового контекста. Сеть Интернет, которая стала основным полем обмена информацией в XXI в., изначально использовалась для решения узкоспециализированных задач. Основным направлением работы на первых этапах была научная и коммуникационная составляющая, поэтому новые угрозы безопасности на этих этапах не формировались. Аналогичным образом до начала 2000-х гг. нельзя было говорить о глобальном характере развития цифрового пространства.

В контексте сравнения с процессом развития ядерных технологий можно проследить четкую параллель. До начала Второй мировой войны их развитие в целом ограничивалось научной и энергетической сферами. Однако мировая война и открытие контролируемых термоядерных реакций стали теми причинами, которые способствовали распространению ядерных технологий на военную сферу. Таким образом, ядерное оружие и угроза тотальной ядерной войны стали основными вопросами в сфере международной безопасности во время холодной войны и остаются таковыми и в настоящее время.

Если говорить о киберпространстве и международной информационной безопасности, то разработка международных норм и правил поведения отставала от процесса развития ИКТ, что послужило причиной возникновения целого ряда новых вызовов и угроз в цифровом домене. В киберпространстве решающую роль играет технологическое развитие, которое также оказало значительное влияние на развитие межгосударственного взаимодействия в рамках морского и воздушного пространств (Rattray, 2009).

На политическом уровне киберпространство было включено в систему обеспечения национальной и международной безопасности в начале 2000-х гг. Как и в случае с другими новыми вызовами и угрозами, международное внимание к кибербезопасности было связано с ускорением процесса глобализации. После терактов 11 сентября 2001 г. многие государства задумались о том, какие вызовы могут происходить из мировой сети и какие возможности она может предоставить, принимая во внимание, что цифровой домен напрямую не контролируется национальными институтами (Stevens, 2012, p. 164).

Именно в 2001 г. был принят первый международный документ, который регулировал вопросы кибербезопасности, — Конвенция Совета Европы о киберпреступности (*The Budapest Convention on Cybercrime, the Budapest Convention*)[4]. В 2003 г. в рамках ООН была подписана Декларация принципов построения информационного общества[5], а в 2005 г. были приняты Тунисское обязательство[6] и Тунисская повестка по информационному обществу[7]. Подписание этих

[4] Budapest Convention on Cybercrime // Council of Europe. November 23, 2001. URL: https://rm.coe.int/1680081561 (accessed: 08.01.2022).

[5] Declaration of Principles “Building the Information Society: A Global Challenge in the New Millennium” // International Telecommunication Union. December 12, 2003. URL: https://digitallibrary.un.org/record/533621/files/S03-WSIS-DOC-0004%21%21PDF-E.pdf (accessed: 08.01.2022).

[6] Tunis Commitment (WSIS-05/TUNIS/DOC/7-E) // International Telecommunication Union. November 18, 2005. URL: https://www.itu.int/net/wsis/docs2/tunis/off/7.html (accessed: 08.01.2022).

[7] Tunis Agenda for the Information society (WSIS-05/TUNIS/DOC/6(Rev.1)-E) // International

документов стало предпосылкой к созданию в 2006 г. Всемирного форума по управлению Интернетом[8].

Данный этап стал важной вехой в процессе признания международных вопросов, связанных с обеспечением международной безопасности в информационном пространстве, так как были даны определения новым вызовам и угрозам, созданы новые форматы взаимодействия. Однако в рамках этого процесса не было полноценного охвата всех вопросов, связанных с регулированием Интернета, что было обусловлено восприятием глобальной сети исключительно как средства связи. Ситуация изменилась к началу 2010-х гг., когда Интернет и информационное пространство стали системообразующим элементом научно-технического и экономического развития большинства стан мира.

В 2010-е гг. увеличилось количество пользователей информационных технологий, для государств это означало необходимость регулирования нового политического пространства. Именно в это время большой охват начали получать протоколы связи 4-го поколения (4G)[9], которые выступили драйвером развития мобильного Интернета и значительно увеличили доступность сетевых ресурсов. Угрозы в информационном пространстве одновременно были и «реальными», и «виртуальными» — это угрозы для физических элементов сети или критической инфраструктуры и угрозы, которые исходят непосредственно из сетевого пространства и среди которых — широкий спектр международных угроз, начиная от нарушения авторских прав до ведения незаконной политической деятельности (Deibert & Rohozinski, 2010, pp. 29—30).

Значительно выросло число зафиксированных межгосударственных киберинцидентов. Если за 2003—2009 гг. было зафиксировано всего 66 подобных инцидентов, то только за 2017 г. их число превысило 71 случай, а в 2018 и 2019 гг. составило 114 и 116 соответственно[10]. Помимо этого, информационно-коммуникационные технологии стали одним из основных факторов в событиях «арабской весны»[11] и в целом использовались для организации «цветных революций» (Манойло, 2014). Для государств, которые не обладали достаточным уровнем технологий и опытом противодействия новым видам угроз, риски, исходящие из информационного пространства, стали одной из серьезных угроз для национального суверенитета и стабильности. В это же время технологически развитые государства получили возможность использовать новые инструменты для достижения своих внешнеполитических целей.

В 2015 г. был утвержден доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, который объединил достижения работы трех групп экспертов в 2010, 2013 и 2015 гг. Данный документ обобщил понятия угроз в информационном пространстве и предложил нормы и правила поведения для государств[12]. В 2013 г. Центр передового опыта совместной киберзащиты НАТО опубликовал Таллиннское руководство по международному праву, применимому к кибернетическим войнам. В 2017 г. вышло второе издание, и в настоящее время идет работа над третьей версией. Отличительной особенностью документа стало то, что там рассматривалась возможность физического военного ответа на

Telecommunication Union. November 18, 2005. URL: https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html (accessed: 08.01.2022).

[8] Управление через Интернет // Отдел государственных учреждений и цифрового правительства Департамента ООН по экономическим и социальным вопросам. URL: https://publicadministration.un.org/ru/internetgovernance (дата обращения: 08.01.2022).

[9] В 2009 г. в Стокгольме и Осло были запущены первые коммерческие сети 4G. Далее на новые протоколы связи стали переходить и другие страны. В некоторых странах процесс перехода до сих пор не завершен.

[10] Significant Cyber Incidents // Center of Strategic International Studies. URL: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents (accessed: 01.02.2022).

[11] Eriksson M., Franke U., Granåsen M., Lindahl D. Social Media and ICT during the Arab Spring // FOI Report. 2013. P. 46. URL: https://www.foi.se/rest-api/report/FOI-R--3702--SE (accessed: 08.01.2022).

[12] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security A/70/174 // General Assembly of the United Nations. July 22, 2015. URL: https://namib.online/wp-content/uploads/2020/04/Report-of-the-UN-Group-of-Governmental-Experts-on-Developments-in-the-Field-of-Information-of-22-July-2015.pdf (accessed: 08.01.2022).

кибератаки[13]. Во второй версии была дана классификация кибератак, которые можно считать нарушением суверенитета страны (повлекшие за собой человеческие жертвы или физический урон)[14]. Вместе с принятием таких документов был запущен процесс создания международных нормативно-правовых режимов для регулирования поведения государств в информационном пространстве.

В процессе секьюритизации информационного пространства страны начали наращивать свои наступательные и оборонительные потенциалы, что фактически привело к «дилемме безопасности» в киберпространстве. В таких условиях сильные государства могут одновременно устанавливать удобные для них правила и сами их нарушать, проводя политику двойных стандартов, в это же время более слабые государства не могут ничего им противопоставить (Buchanan, 2017, pp. 192—193). Таким образом, технологически более развитые государства получили большее влияние в киберпространстве, так как начали реализовывать свои проекты в новом политическом пространстве раньше других.

В данных условиях особенно актуальной стала проблема атрибуции враждебных действий в информационном пространстве. В большинстве своем речь идет о кибератаках и киберпреступлениях, которые совершаются хакерскими группами, принадлежность которых к тому или иному государству практически невозможно определить. Несмотря на появление специализированных учреждений по упреждению инцидентов в информационном пространстве, вопрос атрибуции сохраняет комплексный характер (Зиновьева, 2019а, с. 58). Ряд стран прилагали усилия для налаживания обмена разведданными и компьютерной информацией о вредоносной активности в информационном пространстве на их территории. Так, в Европейском союзе вопрос атрибуции регламентирован в рамках Будапештской конвенции 2001 г., к которой также присоединились США, Канада, Япония, Австралия и др.[15] Вместе с тем Россия и страны Шанхайской организации сотрудничества (ШОС) также применяют практику обмена разведданными при координации соответствующих ведомств[16]. В соглашении между Россией и Китаем об обеспечении международной информационной безопасности также предусмотрен пункт обмена информацией, разведданными о вредоносной активности в информационном пространстве[17]. Тем самым приобретается опыт работы с установлением авторства атаки в информационном пространстве.

На частном уровне ведущие международные ИТ-компании по разработке систем защиты от вирусов, хакерских атак и иных киберугроз в атрибуции кибератаки используют метод анализа кода, или так называемого «почерка хакеров»[18]. Например, атрибуция атак в «Лаборатории Касперского» — это процесс сопоставления новых результатов инцидентов с накопленным опытом. Международная компания по информационной безопасности с целью успешной атрибуции атак создала базу данных *Kaspersky Threat Attribution Engine*, которая проводит анализ вредоносных программ и сопоставляет их с ранее сохраненной информацией[19].

[13] Tallinn Manual on the International Law Applicable to Cyber Warfare / ed. by M. N. Schmitt. Cambridge; New York : Cambridge University Press, 2013. https://doi.org/10.1017/CBO9781139169288

[14] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations / ed. by M. N. Schmitt. Cambridge : Cambridge University Press, 2017. https://doi.org/10.1017/9781316822524

[15] The Budapest Convention and its Protocols // Council of Europe. URL: https://www.coe.int/en/web/cybercrime/the-budapest-convention (accessed: 01.02.2022).

[16] Документы // Шанхайская организация сотрудничества. URL: http://rus.sectsco.org/politics/ (дата обращения: 01.02.2022).

[17] Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности // Официальный интернет-портал правовой информации. 08.05.2015. URL: http://publication.pravo.gov.ru/Document/View/0001201608100001?rangeSize=1 (дата обращения: 01.02.2022).

[18] Оманд Д. Атрибуция кибератаки является политическим решением, это не судебный процесс // Ядерный Контроль. 2017. № 4 (486). URL: http://www.pircenter.org/articles/2099-atribuciya-kiberataki-yavlyaetsya-politicheskim-resheniem-eto-ne-sudebnyj-process (дата обращения: 01.02.2022).

[19] Kaspersky Threat Attribution Engine // Kaspersky. URL: https://media.kaspersky.com/ru/business-security/enterprise/Kaspersky_Threat_Attribution_Engine_Product_Datasheet-ru.pdf (дата обращения: 01.02.2022).

Таблица 1

Хронология процесса секьюритизации информационного пространства в 1970—2020-е гг.

Компонент/ Период	1970-е - 2000-е Интернет ради науки	2000-е Формирование цифрового домена	2010-е Секьюритизация киберпространства	2020 - н.в. Переход к метавселенным
Стандарт связи	2G	3G	4G	5G
Акторы	Отдельные государственные и частные структуры	Государства, негосударственные акторы, международные организации	Государства, негосударственные акторы, международные организации	Государства, негосударственные акторы, международные организации
Масштаб угроз	Локальный характер угроз	Локальный характер угроз	Международный характер угроз	Международный характер угроз
Характер угроз	Промышленный шпионаж, физическое воздействие на критическую инфраструктуру	Основа теневой экономки, угроза физической инфраструктуре	Появление нового типа вызовов и угроз безопасности, межгосударственные кибератаки	Преобладание угроз, исходящих из информационного пространства (виртуальных), над физическими угрозами (реальными)
Режимы	–	Формирование базовых международно-правовых режимов, международное сотрудничество в сфере обеспечения кибербезопасности	Борьба между различными подходами к международно-правовому регулированию информационного пространства	Формирование глобальных цифровых экосистем, увеличение цифрового разрыва, борьба за лидерство в технологической сфере

Источник: составлено авторами.

В рамках следующего этапа развития информационного пространства большее внимание стало уделяться созданию цифровых экосистем, которые предназначены для максимальной концентрации пользователей вокруг группы связанных приложений. Для обработки больших объемов данных потребовались протоколы связи с более высокой скоростью, поэтому начался ускоренный переход на сети 5G. Примером цифровой экосистемы, применяемой как на государственном, так и на частном уровне, является Microsoft 365. Необходимо учитывать тот факт, что данные пользователей хранятся и обрабатываются на серверах компании поставщика цифровых услуг, что создает потенциальные уязвимости для сохранности секретной информации и персональных данных. На 2021 г. большую часть серверов для облачных технологий предоставляют следующие компании: Amazon (США) — 33 %, Microsoft (США) — 21 %, Google (США) — 10 %, Alibaba (КНР) — 6 %, IBM (США) — 4 %, Salesforce (США) — 3 %, Tencent (КНР) — 3 % и Oracle (США) — 2 %[20]. Данная статистика наглядно иллюстрирует, что большую часть рынка облачных технологий контролируют компании из США, единственными конкурентами которых являются китайские компании, обеспечивающие работу облачных сервисов в Китае. О конкуренции на глобальном рынке на данный момент не может быть и речи. В странах, которые придерживаются принципов цифрового суверенитета, на законодательном уровне ограничивается трансграничная передача персональных данных и информации. Из-за специфики информационного пространства цифровой суверенитет в политическом понимании приведет к технологической изоляции страны. Таким образом, в информационном пространстве можно либо обеспечить суверенитет в пределах политических границ, либо добиться глобальной совместимости Интернета, которая будет означать взаимозависимость (Mueller, 2020, p. 798).

К началу 2020-х гг. в информационное пространство стало полноценным политическим

[20] As Quarterly Cloud Spending Jumps to Over $50B, Microsoft Looms Larger in Amazon's Rear Mirror // Synergy Research Group. February 3, 2022. URL: https://www.srgresearch.com/articles/as-quarterly-cloud-spending-jumps-to-over-50b-microsoft-looms-larger-in-amazons-rear-mirror (accessed: 26.02.2022).

пространством, которое занимает центральное место в процессах международного социально-экономического и технологического развития. К началу четвертого этапа стала особенно очевидной проблема цифрового суверенитета, который не может полностью соответствовать политическим границам государства. В это же время страны разделились на несколько объединений, которые выступают за различные формы регулирования межгосударственных отношений в информационном пространстве. США и развитые страны выступают за модель мультистейкхолдеризма в управлении цифровым доменом, в то время как Россия, Китай и развивающиеся страны выступают за многосторонний подход (Дегтерев, Рамич, Пискунов, 2021). Однако помимо государственных инициатив популяризация технологий блокчейн позволяет говорить о создании автономных децентрализованных систем вне государственного контроля[21].

III. Потенциальные точки напряженности

Возникающие в информационном пространстве вызовы и угрозы привели к тому, что сфера ИКТ стала рассматриваться в качестве одной из основных сфер национальной безопасности (Hansen & Nissenbaum, 2009). К таким угрозам можно отнести нарушение функционирования объектов критической инфраструктуры, внешнее влияние во внутреннем информационном пространстве и т. д.

Авторы рассматривают точки напряженности в информационном пространстве и анализируют возможные сферы совпадения интересов и конструирования правил поведения в сети Интернет. По аналогии с ядерной сферой государственные акторы начали согласовывать негласные правила и нормы в сфере ядерного оружия с целью минимизировать риски его распространения, эскалации конфликта и т. д. (Nye, 2011). Основой для согласования первичных негласных норм в ядерной сфере стал опыт конфликтов и кризисов с возможным использованием ядерного оружия. Конфликты в информационном пространстве с использованием вредоносного программного обеспечения (ПО) могут привести к «Карибскому кризису 2.0», который станет общей проблемой ведущих стран (Международная информационная безопасность…, 2021). Такая проблема станет стимулом для создания регулирования в информационном пространстве, так как ее решение требует совместных действий и взаимных обязательств по соблюдению норм.

С учетом специфики информационного пространства безопасность может быть разделена на два измерения: материальные риски для критической инфраструктуры, протоколов и оборудования и риски, возникающие в информационном пространстве без физического ущерба (Deibert & Rohozinski, 2010). В данном разделе будут рассмотрены конфликты и точки напряженности между акторами в ряде сфер, затрагивающих информационную безопасность: критическая инфраструктура, внешнее влияние и социальные приложения, технологическая безопасность и устойчивость цепочек поставок, а также суверенное управление внутренним сегментом сети Интернет.

С точки зрения рисков для физической инфраструктуры, находящейся под юрисдикцией государства, следует упомянуть кейс атаки на трубопровод Colonial Pipeline и JBS Foods, вследствие которой снабжение газом Восточного побережья США было приостановлено на пять дней, а пищевая компания JBS Foods вынуждена была приостановить работу заводов[22]. В результате нарушения функционирования инфраструктурных объектов администрация Дж. Байдена выпустила меморандум о защите критической инфраструктуры[23]. Подобные атаки были произве-

[21] Weyl G., Ohlhaver P., Buterin V. Decentralized Society: Finding Web3's Soul // Social Science Research Network. May 11, 2022. URL: https://ssrn.com/abstract=4105763 (accessed: 26.05.2022).

[22] JBS and Colonial Pipeline Hacks Highlight How Large Food and Energy Companies Have Become Prime Targets // South China Morning Post. June 4, 2021. URL: https://www.scmp.com/tech/tech-trends/article/3135990/jbs-and-colonial-pipeline-hacks-highlight-how-large-food-and (accessed: 08.01.2021).

[23] Fact Sheet: Biden Administration Announces Further Actions to Protect U.S. Critical Infrastructure // The White House. July 28, 2021. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/fact-sheet-

дены в 2019 г. и на российские энергетические системы. Авторство атак приписывают США[24]. Для обоих государств защита критической инфраструктуры отвечает задачам национальной безопасности. В 2013 г. США выделили 16 секторов и признали, что атаки на объекты критической инфраструктуры подрывают национальную безопасность, а также воздействуют на экономическую и социально-гуманитарную безопасность[25]. Россия в 2017 г. также приняла закон о безопасности критической информационной инфраструктуры[26].

С точки зрения законодательной системы КНР в сфере кибербезопасности следует отметить ряд документов, которые транслируют подходы внутреннего регулирования КНР на уровень глобального управления. В первую очередь необходимо выделить Закон о безопасности сети Интернет (в российской литературе именуется законом о кибербезопасности)[27]. Законодательный акт, принятый в 2017 г., закрепил понятие цифрового суверенитета (网络空间主权) и требования к сетевым операторам хранить персональные данные граждан на территории КНР. В дополнение к этому в Законе была определена система защиты критической инфраструктуры КНР. В 2021 г. Госсовет КНР опубликовал сразу ряд документов, конкретизирующих внутреннюю политику КНР в сфере кибербезопасности: Расширенное положение о защите критической инфраструктуры[28], Закон о безопасности данных[29] и Закон о защите персональных данных[30].

Кроме того, следует отметить напряженность между США и Китаем в сфере развития сетей 5G. На основе анализа указанных правовых документов можно сделать вывод, что КНР с целью обеспечения национальной безопасности принимает меры по локализации данных, созданию системы защиты критической инфраструктуры и регулирует импорт иностранных технологий.

Вместе с тем с точки зрения теории «сетевого общества», в котором власть конструируется путем формирования образов и фреймов, государственным акторам важно контролировать информационное пространство и контент в социальных приложениях и сервисах с целью ограничить иностранное влияние и обеспечить внутреннюю стабильность. Китай активно фильтрует поступающие потоки информации с помощью Золотого щита (*Great Firewall*) и блокирует иностранные приложения, в том числе Google, Facebook и др. (Понька, Рамич, У, 2020). Соответственно, согласно «Белой книге» по управлению Интернетом, Китай реализует

biden-administration-announces-further-actions-to-protect-u-s-critical-infrastructure/ (accessed: 08.01.2021).

[24] U.S. Escalates Online Attacks on Russia's Power Grid // The New York Times. June 15, 2019. URL: https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html?action=click&module=Top%20Stories&pgtype=Homepage (accessed: 08.01.2021).

[25] Critical Infrastructure Sectors // Cybersecurity and Infrastructure Security Agency. October 21, 2020. URL: https://www.cisa.gov/critical-infrastructure-sectors (accessed: 08.01.2021).

[26] Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Официальный интернет-портал правовой информации. 26.07.2017. URL: http://publication.pravo.gov.ru/Document/View/0001201707260023?index=0&rangeSize=1 (дата обращения: 08.01.2021).

[27] Zhonghua renmin gongheguo wangluoanquanfa quanwen (2017 nianshishi) // Wu yang xian ren min zheng fu [Закон о безопасности сети Интернет Китайской Народной Республики (вступил в силу в 2017 г.) // Народное правительство округа Мэян]. (На китайском языке). URL: http://www.wuyang.gov.cn/fazhizaixian/falvfagui/20200419/38978.html (дата обращения: 08.01.20221).

[28] Guanjianxinxi jichusheshi anquanbaohu tiaoli // Zhonghua renmin gongheguo guowuyuanling [Положение о защите критической информационной инфраструктуры // Постановление Госсовета Китайской Народной Республики]. 01.09.2021. URL: https://digichina.stanford.edu/work/translation-critical-information-infrastructure-security-protection-regulations-effective-sept-1-2021/ (дата обращения: 08.01.2021). (На китайском языке).

[29] Data Security Law of the People's Republic of China // The National People's Congress of the People's Republic of China. June 10, 2021. URL: http://www.npc.gov.cn/englishnpc/c23934/202112/1abd8829788946ecab270e469b13c39c.shtml (accessed: 08.01.2021).

[30] Zhonghua renmin gongheguo geren xinxi baohufa // Quanguo renmin daibiao dahui [Закон Китайской Народной Республики о защите личной информации // Всекитайское собрание народных представителей Китайской Народной Республики]. 20.08.2021. URL: http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml (дата обращения: 08.01.2021). (На китайском языке).

принцип суверенитета и право на государственное управление внутренним информационном пространством[31]. Иным примером секьюритизации проблемы иностранного влияния является блокировка социальных приложений TikTok и WeChat. При президенте Д. Трампе США пытались заблокировать работу этих приложений, указывая на обработку персональных данных технологиями искусственного интеллекта, блокировку определенного контента и влияние на социальную стабильность (Williams, 2020).

В дополнение к этому следует отметить государственное управление сетью Интернет в ходе внутренних конфликтов. Государства с целью ограничить иностранное влияние, координацию протестов и распространение информации блокируют использование сети Интернет и ограничивают распространение информации. В ходе массовых протестов в 2020 г. в Беларуси правительство отключило доступ в Интернет. Также частным мобильным провайдерам было выдвинуто требование — устанавливать доступ в Интернет через Национальный центр обмена трафиком[32]. Это обеспечило контроль правительства Беларуси над доступом во всемирную паутину, предоставляемым частными компаниями. Таким же образом поступило правительство Республики Казахстан, ограничив доступ в Интернет на всей территории страны. Ввиду того, что протестующие использовали защищенные социальные сети, власти Казахстана отключали Интернет на время протестов с целью остановить распространение информации и координацию народных выступлений[33]. Всего в 2021 г. было зафиксировано 182 отключения Интернета в 34 странах, где имели место протестные движения[34].

Иным аспектом информационной безопасности является стабильность производственных цепочек поставок комплектующих и полупроводников. Обеспечение поставок полупроводников является ключевой задачей с точки зрения экономической и технологической безопасности. Полупроводниковый кризис, разразившийся в период пандемии COVID-19 и спровоцированный целым рядом факторов, мотивировал государства к контролю производственных цепочек и инвестированию в эту отрасль.

Китай в период обострения конкуренции с США во время президентства Д. Трампа, руководствуясь задачами национальной безопасности, начал активно работать над безопасностью в сфере полупроводников, в том числе разработками технологий и их производством. В 2020 г. Госсовет КНР предложил технологическим компаниям перенести процесс разработки (*research and development*, R&D), дизайна, производства, тестирования и упаковки полупроводников в Китай[35]. Эта программа направлена на то, чтобы аккумулировать производство на своей территории и получить необходимые разработки в сфере полупроводников.

После прихода Д. Байдена к власти США начали активно работать над обеспечением безопасности поставок полупроводников. По распоряжению Дж. Байдена был составлен доклад, посвященный отрасли полупроводников США[36]. Тем не менее цепочка

[31] Full Text: White Paper on the Internet in China // China Daily. June 08, 2010. URL: https://www.chinadaily.com.cn/china/2010-06/08/content_9950198.htm (accessed: 08.01.2021).

[32] Белорусский «Национальный центр обмена трафиком» объяснил проблемы доступа к Интернету в стране внешней атакой // D-Russia. 12.08.2020. URL: https://d-russia.ru/belorusskij-nacionalnyj-centr-obmena-trafikom-objasnil-problemy-dostupa-k-internetu-v-strane-vneshnej-atakoj.html (дата обращения: 08.01.2021).

[33] Kazakhstan's Largest City Almaty, Back Online after Clashes, Blackout // Hindustan Times. January 10, 2022. URL: https://www.hindustantimes.com/world-news/kazakhstans-largest-city-almaty-back-online-after-clashes-blackout-101641788351208.html (accessed: 08.03.2022).

[34] Keep it On // Access now. URL: https://www.accessnow.org/keepiton/ (accessed: 08.01.2021).

[35] Xinshiqi cujin jicheng dianlu chanyehe ruanjianchanye gaozhiliangfazhande ruogan ganzheng zhengce // Zhonghua renmin gongheguo zhongyangrenmin zhengfu [Политика Государственного совета Китая по содействию качественному развитию индустрии интегральных схем (ИС) и программного обеспечения в новую эпоху // Правительство Китайской Народной Республики]. 27.07.2020. URL: http://www.gov.cn/zhengce/content/2020-08/04/content_5532370.htm (дата обращения: 08.01.2021). (На китайском языке).

[36] Building Resilient Supply Chains, Revitalizing American Manufactures, and Fostering Broad-Based Growth. 100-Day Reviews under Executive Order 14017 // The White House. June 2021. URL: https://www.whitehouse.gov/wp-content/uploads/2021/06/

добавленной стоимости представляет собой участие ряда экономик в процессе производства. В этой связи на фоне конфронтации с Китаем США намерены вернуть на свою территорию такие производственные процессы, как сбор, упаковка и тестирование, которые ввиду меньших экономических издержек в настоящее время осуществляются в Китае. Ключевой уязвимостью здесь выступает зависимость от производственного сектора КНР и потенциальная нестабильность производственных цепочек, что может привести к нехватке полупроводников. С целью исследовать уязвимые места в этой отрасли США провели саммит с представителями частных компаний, в том числе TSMC, Samsung, Qualcomm и Apple, и предложили финансирование на создание объектов по производству чипов в США[37].

С появлением сети Интернет в качестве новой уязвимости стал выступать контроль над управлением корневыми серверами и фильтрация информации. Так называемые *choke points* — это критические узлы в информационном пространстве, от которых зависит функционирование информационных систем, критической инфраструктуры и обмен данными в сети Интернет[38]. К таким критическим узлам относятся экосистемы, создаваемые технологическими корпорациями, более известными как «большая пятерка»[39] (Google, Amazon, Facebook, Microsoft, Apple (GAFAM)). Сервисы и приложения корпораций GAFAM используются как частными компаниями, так и государственными учреждениями, то есть от стабильности функционирования центров обработки данных и работы служб технологической корпорации зависит безопасность объектов, на которых функционируют эти сервисы. Схожая экосистема сетевых приложений создана Китаем. В рамках такой системы платежные системы, обработка и хранение данных, распространение информации зависит от функционирования экосистем, создаваемых Alibaba, Tencent и Huawei.

Данные примеры напряженности в информационном пространстве могут стать решающим фактором для согласования норм. По аналогии с ядерной сферой, когда государства были заинтересованы в уменьшении рисков для национальной безопасности, государственные и негосударственные акторы путем конструирования кодекса поведения могут обеспечить информационную безопасность. Нарушение работы критической инфраструктуры и нестабильность цепочек поставок влечет экономические издержки для государственных акторов. Социальное и суверенное управление внутренним сегментом сети Интернет становится неотъемлемой частью национальной политики в сфере безопасности. Тем самым государственные акторы с привлечением частных сторон могут уменьшить трения в этих областях.

IV. Формирование предварительного регулирования в информационном пространстве

Конкуренция между державами определяет контроль над современными рычагами власти — глобальными правилами и институтами, стандартами и технологиями[40]. Международные правила поведения в информационном пространстве также являются объектом конкуренции между державами (РФ и США) и представляют рычаг силы, который определит доминирование одного из подходов к регулированию. Как и институты, созданные после Второй мировой войны,

100-day-supply-chain-review-report.pdf (accessed: 08.01.2022).

[37] Readout of Biden Administration Convening to Discuss and Address Semiconductor Supply Chain // The White House. September 23, 2021. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/23/readout-of-biden-administration-convening-to-discuss-and-address-semiconductor-supply-chain/ (accessed: 08.01.2022).

[38] Farrell H., Newman A. Choke Points // Harvard Business Review. January-February 2020. URL: https://hbr.org/2020/01/choke-points (accessed: 01.02.2022).

[39] Sen C. The 'Big Five' Could Destroy the Tech Ecosystem // Bloomberg. November 15, 2017. URL: https://web.archive.org/web/20201109030953/https://www.bloomberg.com/opinion/articles/2017-11-15/the-big-five-could-destroy-the-tech-ecosystem (accessed: 08.01.2022).

[40] Lewis J. A. Technological Competition and China // Center for Strategic and International Studies. November 30, 2018. URL: https://www.csis.org/analysis/technological-competition-and-china (accessed: 26.02.2022).

предрегулирование (*soft law*) информационного пространства, механизмы и институты, вырабатывающие консенсус между акторами международных отношений, становятся критическим элементом с точки зрения силы и влияния того или иного государства в международной системе.

Ведущие державы в создании предрегулирования в информационном пространстве — это США и Россия. Оба государства продвигают свои концепции международных правил поведения в информационном пространстве, что происходит в том числе в рамках ООН. Россия и США выдвинули противоположные по содержанию резолюции в рамках сессий Генеральной Ассамблеи ООН до 2021 г. (Levinson, 2021, p. 2). Со своей стороны Российская Федерация, понимая важность и значимость информационного пространства с точки зрения безопасности и экономического развития, инициировала процесс выработки и обсуждения норм поведения в рамках ООН. В 1998 г. была подготовлена первая резолюция «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности» (A/RES/53/70)[41]. Процесс выработки предрегулирования был институционализирован в 2004 г. с созданием Группы правительственных экспертов (ГПЭ) ООН[42]. Целью ГПЭ стала выработка норм регулирования в информационном пространстве. В результате деятельности ГПЭ ООН был принят ряд докладов, однако в 2017 г. Группа не смогла прийти к консенсусу[43]. Это стало причиной создания нового механизма, призванного сделать процесс выработки регулирования инклюзивным: в 2018 г. Россия внесла предложение организовать новый формат определения норм и создать Рабочую группу открытого состава (РГОС)[44].

Страны «коллективного Запада» (США, Франция, Великобритания, Канада, Германия и др.) выступили против резолюции о создании РГОС. Напротив, в 2018 г. США представили собственную резолюцию по безопасности ИКТ «Поощрение ответственного поведения государств в киберпространстве» (*Advancing responsible State behaviour in cyberspace in the context of international security*), в которой был определен новый мандат действия ГПЭ ООН[45]. В дополнение к этому в 2021 г. Россия и США стали главными соавторами резолюции Генеральной Ассамблеи ООН (A/RES/76/19)[46], которая признавала деятельность обоих форматов и стала свидетельством сближения позиций двух держав[47]. Таким образом, ГПЭ и РГОС ООН — механизмы создания правовых режимов и продвижения концепций правового регулирования в информационном пространстве.

[41] Resolution A/RES/53/70 “Developments in the Field of Information and Telecommunications in the Context of International Security” // General Assembly of the United Nations. January 4, 1999. URL: https://digitallibrary.un.org/record/265311/files/A_RES_53_70-EN.pdf (accessed: 01.02.2022).

[42] Resolution A/RES/58/32 “Developments in the Field of Information and Telecommunications in the Context of International Security” // General Assembly of the United Nations. December 18, 2003. URL: https://digitallibrary.un.org/record/507790 (accessed: 01.02.2022).

[43] Ответ спецпредставителя Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности А.В. Крутских на вопрос информагентства ТАСС о состоянии международного диалога в этой сфере // Министерство иностранных дел Российской Федерации. 29.06.2017. URL: https://web.archive.org/web/20170705020039/http://www.mid.ru/ru/mezdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/UsCUTiw2pO53/content/id/2804288 (дата обращения: 27.02.2022).

[44] «Инциденты онлайн могут привести к развязыванию полномасштабной войны офлайн» // Коммерсантъ. 06.06.2019. URL: https://www.kommersant.ru/doc/3992579 (дата обращения: 27.02.2022).

[45] Resolution A/RES/73/266 “Advancing Responsible State Behavior in Cyberspace in the Context of International Security” // General Assembly of the United Nations. January 2, 2019. URL: https://digitallibrary.un.org/record/1658328/files/A_RES_73_266-EN.pdf (accessed: 01.02.2022).

[46] Resolution A/RES/76/19 “Developments in the Field of Information and Telecommunications in the Context of International Security, and Advancing Responsible State Behaviour in the Use of Information and Communications Technologies” // General Assembly of the United Nations. December 8, 2021. URL: https://digitallibrary.un.org/record/3951137 (accessed: 27.02.2022).

[47] Зиновьева Е., Зинченко А. Россия и США налаживают сотрудничество в сфере информационной безопасности // Российский совет по международным делам. 09.11.2021. URL: https://russiancouncil.ru/analytics-and-comments/analytics/rossiya-i-ssha-nalazhivayut-sotrudnichestvo-v-sfere-informatsionnoy-bezopasnosti/ (дата обращения: 27.02.2022).

Россия и США в стратегиях и концепциях определяют принципы предварительного регулирования, на основе которых идет согласование норм в рамках механизмов ООН. Согласно международной стратегии для киберпространства, США выступают за принятие стандартизированных процедур надзора за кибероперациями и обеспечение доступа к сети Интернет (Davis & Lewis, 2019, p. 163). Глобальное управление киберпространством должно осуществляться с широким участием негосударственных акторов, в том числе телекоммуникационных и технологических корпораций, некоммерческих организаций и научно-технических кругов. Государства несут ответственность за защиту информационной инфраструктуры[48].

Россия и Китай продвигают право на суверенное управление информационным пространством и ограничивают доступ к компьютерной информации, находящейся на их территории. Концепция международной информационной безопасности (МИБ), подписанная государствами — членами ШОС, определяет возможность установления суверенных норм и механизмов управления своим информационным пространством и свободу в реализации своих суверенных интересов в информационной сфере (Зиновьева, 2019b). В целях защиты конституционного строя, обороны и безопасности государства могут ограничивать доступ к сети Интернет (Международная информационная безопасность: теория и практика, 2019). Ключевую роль в глобальном управлении информационным пространством играют государственные акторы, в то время как негосударственные участники выполняют консультативную роль. Важным аспектом подхода России и Китая является уважение роли всех государств в конструировании норм и правил поведения в информационном пространстве.

Исходя из вышеприведенного анализа, видно, что подходы России и США противоположны в вопросах управления Интернетом, регулирования национального сегмента сети Интернет и его развития. Тем не менее общие интересы в сфере информационной безопасности заставляют Россию и США вести диалог по проблеме создания правового регулирования.

Таким образом, можно сделать вывод, что предрегулирование в информационном пространстве происходит через механизмы России и США, созданные в рамках ООН. Эти механизмы также выступают в качестве ключевого инструмента для продвижения своей концепции и создания правовых режимов.

V. Иерархия глобального управления в информационном пространстве

В условиях недостатка регулирования в информационном пространстве и конфликта нескольких проектов нормативно-правового регулирования этой сферы можно говорить о конкуренции за право установления норм в новом политическом пространстве.

В глобальном масштабе мощь государства традиционно оценивается по факту обладания какими-либо ресурсами, технологиями или же количественными показателями мощи (Дегтерев, 2020; Баланс сил в ключевых регионах мира…, 2021). В информационном пространстве полный комплекс таких критериев еще не был выработан. Однако основным критерием влияния, который обеспечивает лидерство в цифровом домене, является способность контролировать глобальные цепочки производства технологических продуктов, от которых зависит возможность использования и функционирования сети, проведения наступательных и оборонительных кибероперация и оказание влияния на формирование международно-правовых режимов в этой сфере.

Контроль над цепочками поставок высокотехнологичной продукции позволяет государствам влиять на доступность технологий. Так, ограничение по производству полупроводников является одним из наиболее серьезных сдерживающих факторов для Китая в технологической сфере. На данный момент передовые процессоры выпускаются несколькими компаниями: TSMC (Тайвань) — 54 % мирового рынка, Samsung (Республика

[48] International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World // The White House. May 2011. URL: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (accessed: 01.02.2022).

Корея) — 17 % мирового рынка, Global Foundries (США) — 7 % мирового рынка, SMIC (КНР) — 5 % мирового рынка[49]. В это же время TSMC, Samsung и крупнейший производитель компьютерных чипов Intel напрямую зависят от поставок фотолитографического оборудования компании ASML (Нидерланды), которая контролирует 62 % мирового рынка и не имеет конкурентов, кроме японских компаний Canon и Nikon[50]. Фактически контроль над этими компаниями играет определяющую роль в развитии глобальных технологических процессов, а наибольшее влияние на систему оказывают США, Китай, страны ЕС, Япония и Республика Корея.

Потенциалы стран в сфере кибербезопасности сложно оценить по причине защиты информации о реальных потенциалах кибервойск и проводимых кибероперациях. Однако Международный союз электросвязи (МСЭ) выпускает регулярный рейтинг кибербезопасности стран мира, согласно которому среди наиболее влиятельных акторов в информационном пространстве высоким потенциалом в сфере кибербезопасности обладают США (1-е место), Южная Корея (4-е место), Российская Федерация (5-е место), Япония (7-е место), Индия (10-е место), Турция (11-е место) и Китай (33-е место)[51].

На формирование международных режимов в сфере регулирования информационного пространства на данный момент наибольшее влияние оказывают два государства — это Российская Федерация и США. Как было упомянуто ранее, эти две страны объединили вокруг себя большинство государств мира и продвигают два проекта международного регулирования, которым на настоящий момент не было представлено весомых альтернатив.

На основе указанных критериев авторы представляют иерархию глобального управления в информационном пространстве следующим образом:

– I уровень — это полный контроль над всеми тремя сферами, который обеспечивает лидерство в глобальном управлении информационным пространством;

– II уровень — контроль над большинством сфер (двумя из трех), который позволяет оказывать наибольшее влияние на систему глобального управления информационным пространством;

– III уровень — контроль над одной из ключевых сфер, который позволяет оказывать влияние на международные отношения в информационном пространстве;

– IV уровень — опосредованный контроль, который позволяет принимать участие, но не контролировать процессы в информационном пространстве (рис. 1).

Данная модель была построена с использованием методологических наработок Т. Маурера, который предложил классификацию акторов для выявления места прокси в классификации угроз в киберпространстве (Maurer, 2018, p. 16).

На начало 2020-х гг. США остаются единственным государством, которое может одновременно контролировать глобальные цепочки производства высокотехнологичных товаров, обладают внушительным киберпотенциалом и оказывают влияние на формирование международно-правовых режимов. США стремятся сохранить свое лидерство в информационном пространстве, формируя коалицию развивающихся государств, заинтересованных в сохранении существующего миропорядка. В то же время значительное влияние на систему глобального управления оказывают Россия, Китай и страны Европейского союза, так как они обладают внушительным влиянием в информационном пространстве и формируют основные тренды. Вместе с тем важные поставщики высокотехнологичных товаров, а также страны, которые активно используют кибероперации для решения внешнеполитических задач, зачастую

[49] 2 Charts Show How Much the World Depends on Taiwan for Semiconductors // CNBC. March 15, 2021. URL: https://www.cnbc.com/2021/03/16/2-charts-show-how-much-the-world-depends-on-taiwan-for-semiconductors.html (accessed: 26.02.2022).

[50] How ASML Became Chipmaking's Biggest Monopoly // The Economist. February 29, 2020. URL: https://www.economist.com/business/2020/02/29/how-asml-became-chipmakings-biggest-monopoly (accessed: 26.02.2022).

[51] Global Cybersecurity Index 2020 // International Telecommunication Union. 2020. URL: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E/ (accessed: 26.02.2022).

Рис. 1. Иерархия системы глобального управления в информационном пространстве
Примечание: Rule makers — акторы, оказывающие влияние на выработку международных норм, rule takers — акторы, принимающие установленные нормы и следующие им.
Источник: составлено авторами.

выступают совместно с акторами I и II уровня, не имея возможности в одиночку воздействовать на систему глобального управления. Страны с низким уровнем технологического развития и негосударственные акторы оказывают опосредованное влияние на информационное пространство и скорее являются объектом конкуренции для более крупных акторов, а также не оказывают значительного влияния на систему глобального управления информационным пространством.

Заключение

В ходе длительного процесса эволюции угроз в информационном пространстве цифровой домен стал полноценным пространством как для межгосударственного сотрудничества, так и для конкуренции. Особая природа информационного пространства, которое одновременно находится в физической и виртуальной средах, стала причиной для изобретения принципиально новых подходов для его регулирования и противодействия новым угрозам.

В рамках четырех этапов секьюритизации, которые были рассмотрены в статье, изменились акторы, масштаб и характер угроз, а также международно-правовые режимы в информационном пространстве. Несмотря на это, до сих пор сохраняется недостаток регулирования, который позволяет более сильным государствам оказывать большее влияние на международные процессы, формируя нормы и правила, поддерживающие их лидерство. Это порождает коренной конфликт интересов между существующим гегемоном — США и странами, которые стремятся к трансформации системы глобального управления в информационном пространстве, — РФ и КНР.

На данный момент мы можем наблюдать процесс предрегулирования в информационном пространстве, в рамках которого можно выделить несколько проектов всеобъемлющих международно-правовых режимов, которые конкурируют между собой. В то же

время страны, поддерживающие эти проекты, принимают указанные в них положения в рамках ограниченных международных форматов. В случае с США и европейскими странами — это отдельные соглашения НАТО и ЕС, а в случае с РФ и КНР — это отдельные документы в рамках ШОС и БРИКС.

Сама система глобального управления информационным пространством иерархична, и влияние на формирование новых норм и правил может оказывать ограниченный ряд государств — это США, РФ, КНР и страны ЕС. Другие участники этих процессов зачастую не выступают в качестве самостоятельных акторов и включены в одно из существующих объединений.

Принимая во внимание указанные факторы, можно предположить, что будет предложен альтернативный вариант государственным проектам регулирования информационного пространства — децентрализованная модель на основе блокчейн-технологий, которая позволит негосударственным акторам в большей степени влиять на систему глобального управления в информационном пространстве.

Поступила в редакцию / Received: 27.02.2022
Доработана после рецензирования / Revised: 01.04.2022
Принята к публикации / Accepted: 18.04.2022

Библиографический список

Баланс сил в ключевых регионах мира: концептуализация и прикладной анализ / под ред. Д. А. Дегтерева, М. А. Никулина, М. С. Рамича. Москва : РУДН, 2021.

Данилин И. В. Американо-китайская технологическая война: риски и возможности для КНР и глобального технологического сектора // Сравнительная политика. 2020a. Т. 11, № 4. С. 160—176. https://doi.org/10.24411/2221-3279-2020-10056

Данилин И. В. Концептуализация стратегии США в технологической войне против КНР: экономика, политика, технонационализм // Международная аналитика. 2020b. Т. 11, № 4. С. 21—38.

Дегтерев Д. А. Оценка современной расстановки сил на международной арене и формирование многополярного мира. Москва : Русайнс, 2020.

Дегтерев Д. А., Рамич М. С., Цвык А. В. США — КНР: «властный транзит» и контуры «конфликтной биполярности» // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2021. Т. 21, № 2. С. 210—231. https://doi.org/10.22363/2313-0660-2021-21-2-210-231

Дегтерев Д. А., Рамич М. С., Пискунов Д. А. Подходы США и КНР к глобальному управлению киберпространством: «новая биполярность» в «сетевом обществе» // Вестник международных организаций. 2021. Т. 16, № 3. С. 7—33. https://doi.org/10.17323/1996-7845-2021-03-01

Зиновьева Е. С. Киберсдерживание и цифровая дилемма безопасности в американском экспертном дискурсе // Международные процессы. 2019a. Т. 17, № 3. С. 51—65. https://doi.org/10.17994/IT.2019.17.3.58.4

Зиновьева Е. С. Международное сотрудничество по обеспечению информационной безопасности: субъекты и тенденции эволюции: дис. … д-ра полит. наук: 23.00.04. Москва : МГИМО, 2019b.

Манойло А. В. Информационный фактор цветных революций и современных технологий демонтажа политических режимов // Вестник МГИМО-Университета. 2014. № 6 (39). С. 61—67. https://doi.org/10.24833/2071-8160-2014-6-39-61-67

Международная информационная безопасность: новая геополитическая реальность / под ред. Е. С. Зиновьевой, М. Б. Алборовой. Москва : Аспект Пресс, 2021.

Международная информационная безопасность: теория и практика : в 3 т. Т. 1 / под общ. ред. А. В. Крутских. Москва : Аспект Пресс, 2019.

Понька Т. И., Рамич М. С., У Ю. Информационная политика и информационная безопасность КНР: развитие, подходы и реализация // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2020. Т. 20, № 2. С. 382—394. https://doi.org/10.22363/2313-0660-2020-20-2-382-394

Buchanan B. The Cybersecurity Dilemma: Hacking, Trust and Fear between Nations. New York, NY : Oxford University Press, 2017.

Buzan B. People, States, and Fear: The National Security Problem in International Relations. Brighton : Wheatsheaf Books, 1983.

Buzan B., Hansen L. The Evolution of International Security Studies. Cambridge : Cambridge University Press, 2009.

Buzan B., Wæver O. Regions and Powers: The Structure of International Security. Cambridge : Cambridge University Press, 2003. https://doi.org/10.1017/CBO9780511491252

Castells M. Communication Power. Oxford : Oxford University Press, 2013.

Castells M. Network Theory. A Network Theory of Power // International Journal of Communication. 2011. Vol. 5, no. 15. P. 773—787.

Davis J. A., Lewis C. Beyond the United Nations Group of Governmental Experts: Norms of Responsible Nation-State Behavior in Cyberspace // The Cyber Defense Review. 2019. P. 161—168.

Deibert R. J., Rohozinski R. Risking Security: Policies and Paradoxes of Cyberspace Security // International Political Sociology. 2010. Vol. 4, no. 1. P. 15—32. https://doi.org/10.1111/j.1749-5687.2009.00088.x

Hansen L., Nissenbaum H. Digital Disaster, Cyber Security, and the Copenhagen School // International Studies Quarterly. 2009. Vol. 53, no. 4. P. 1155—1175. https://doi.org/10.1111/j.1468-2478.2009.00572.x

Hjalmarsson O. The Securitization of Cyberspace. How the Web Was Won // Lund University Libraries. 2013. P. 1—28. URL: http://lup.lub.lu.se/student-papers/record/3357990 (accessed: 26.02.2022).

Levinson N. S. Idea Entrepreneurs: The United Nations Open-Ended Working Group & Cybersecurity // Telecommunications Policy. 2021. Vol. 45, no. 6. P. 1—11. https://doi.org/10.1016/j.telpol.2021.102142

Maurer T. Cyber Mercenaries: The State, Hackers, and Power. Cambridge : Cambridge University Press, 2018. https://doi.org/10.1017/9781316422724

Mueller M. L. Against Sovereignty in Cyberspace // International Studies Review. 2020. Vol. 22, no. 4. P. 779—801. https://doi.org/10.1093/isr/viz044

Nye J. S. Deterrence and Dissuasion in Cyberspace // International Security. 2016. Vol. 41, no. 3. P. 44—71. https://doi.org/10.1162/ISEC_a_00266

Nye J. S. Nuclear Lessons for Cyber Security? // Strategic Studies Quarterly. 2011. Vol. 5, no. 4. P. 18—38.

Rattray G. J. An Environmental Approach to Understanding Cyberpower // Cyberpower and National Security / ed. by F. D. Kramer, S. H. Starr, L. K. Wentz. Washington, DC : National Defense University Press, Potomac Books, 2009. P. 253—274.

Stevens T. A Cyberwar of Ideas? Deterrence and Norms in Cyberspace // Contemporary Security Policy. 2012. Vol. 33, no. 1. P. 148—170. https://doi.org/10.1080/13523260.2012.659597

Williams R. D. Beyond Huawei and TikTok: Untangling US Concerns Over Chinese Tech Companies and Digital Security // Working Paper for the Penn Project on the Future of U.S. — China Relations. 2020. P. 1—44. URL: https://www.brookings.edu/wp-content/uploads/2020/10/FP_20201030_huawei_tiktok_williams.pdf (accessed: 26.02.2022).

Xingdong F., Du L. Zhongmei keji jingzhengde weilai qushiyanjiu — quanqiu keji chuangxin qudongxiade chanye youshi zhuanyi、chongtu yuzai pingheng // Renminluntan xueshuqianyan [Изучение будущих тенденций китайско-американской технологической конкуренции — интенсивность, конфликт и перебалансирование, обусловленные глобальными технологическими инновациями // Народный форум Академические границы]. 2019. Vol. 4, no 24. P. 46—59. (На китайском языке). https://doi.org/10.16619/j.cnki.rmltxsqy.2019.24.004

Zhao S. The US — China Rivalry in the Emerging Bipolar World: Hostility, Alignment, and Power Balance // Journal of Contemporary China. 2021. Vol. 31, no. 134. P. 169—185. https://doi.org/10.1080/10670564.2021.1945733

Сведения об авторах: *Рамич Мирзет Сафетович* — ассистент кафедры теории и истории международных отношений Российского университета дружбы народов; ORCID: 0000-0003-1479-2785; e-mail: ramich-ms@rudn.ru

Пискунов Данил Андреевич — студент кафедры теории и истории международных отношений Российского университета дружбы народов; ORCID: 0000-0002-4321-3191; e-mail: piskunov_da@mail.ru