УДК 342.15:341.226.5
DOI 10.52468/2542-1514.2022.6(4).32-44

ПОНЯТИЕ КИБЕРПРОСТРАНСТВА В МЕЖДУНАРОДНОМ ПРАВЕ

К.А. Иванова[1,2], М.Ж. Мылтыкбаев[3], Д.Д. Штодина[3]
[1] *Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации (РАНХиГС), г. Москва, Россия*
[2] *Тюменский государственный университет, г. Тюмень, Россия*
[3] *Московский государственный институт международных отношений (университет) Министерства иностранных дел Российской Федерации, г. Москва, Россия*

Информация о статье
Дата поступления –
9 марта 2022 г.
Дата принятия в печать –
20 сентября 2022 г.
Дата онлайн-размещения –
20 декабря 2022 г.

Ключевые слова
Киберпространство, международное право, международная информационная безопасность, сеть «Интернет», Группа правительственных экспертов ООН, ИКТ, киберрегулирование в международном праве

Рассматривается роль международного права в киберпространстве. Отмечается, что киберпространство в настоящее время является основой глобальных систем торговли, связи и обороны, а также ключевым аспектом критической инфраструктуры, которая поддерживает современную цивилизацию. Технологии и информация распространяются почти мгновенно, а мировая экономика и цепочки поставок интегрированы до беспрецедентной в истории степени. Тем не менее до сих пор в международном праве нет выработанного универсального понятия киберпространства, существуют только подходы на уровне ООН, международных организаций, отдельно выделяются доктринальные подходы. Принципиально важным является выработка универсального понятия киберпространства в силу сохраняющихся значительных уязвимостей и количества угроз в глобальной связи.

THE CONCEPT OF CYBERSPACE IN INTERNATIONAL LAW

Ksenia A. Ivanova[1,2], Madi Zh. Myltykbaev[3], Daria D. Shtodina[3]
[1] *Russian Presidential Academy of National Economy and Public Administration (RANEPA), Moscow, Russia*
[2] *University of Tyumen, Tyumen, Russia*
[3] *MGIMO University, Moscow, Russia*

Article info
Received –
2022 March 09
Accepted –
2022 September 20
Available online –
2022 December 20

Keywords
Cyberspace, international law, international information security, Internet, UN Group of Governmental Experts, ICT, cyber regulation in international law

The subject. The article is devoted to the analysis of approaches in the development of the concept of cyberspace in international law.
The purpose of this article is to try to highlight the attributes of cyberspace, which will allow to resolve existing gaps in the field of universal cyber regulation in international law.
The research presented in this article was conducted by combining various disciplinary approaches, including comparative law, comparative politics and international relations, political theory, and sociology. In addition, the study includes methods of dialectical logic, analysis and synthesis, as well as a formal-legal analysis of UN international legal acts.
The main results and scope of their application. As states pay increasing attention to cyberspace management as the technical architecture that powers the global Internet and governance in cyberspace, in terms of how states, corporations and users can use this technology, the role of international law in cyberspace is increasing, becoming more prominent, becoming more important. At the same time, note that international law has no specific rules for regulating cyberspace. Moreover, the technology is both new and dynamic. Thus, for several years there have been open questions as to whether existing international law applies at all to cyberspace. Cyberspace is now the backbone of global commerce, communication and defense systems, and is a key aspect of the critical infrastructure that sustains our modern civilization. Technology and information spread almost instantaneously, and the global economy and supply chains are integrated to a degree unprecedented in history.

ISSN 2658-4050 (Online)

Nevertheless, there is still no developed universal concept of cyberspace in international law, only approaches at the level of the UN, international organizations, including the First Committee of the UN General Assembly on Disarmament and International Security, the G20, the European Union, the Association of Southeast Asian Nations and the Organization of American States and doctrinal approaches are singled out.
Conclusions. The competition for strategic technology and the competition for advantage in the "information space" is growing, so far without the standard international rules of the road. Moreover, the future is likely to prove even more transformational. The potential threats are also extraordinary: autonomous weapons, cyber warfare, sophisticated disinformation campaigns and geopolitical instability. In such circumstances, it is crucial to develop a universal notion of cyberspace because of the persistent significant vulnerabilities and number of threats in global communications.

1. Введение

Киберпространство широко признаётся как фундаментальный факт повседневной жизни в современном мире. До недавнего времени считалось, что его политическое влияние является низким, что связано с политико-фоновыми условиями, рутинными процессами и решениями. Однако теперь, когда эксперты начали осознавать его влияние на международную политику, национальную безопасность, основные институты и процессы принятия важнейших решений [1], представляется возможным использовать латинское выражение *Hic sunt leones* («Здесь обитают львы») [2], которое обозначало неоткрытые земли. Киберпространство можно отнести именно к такой «земле», которая была фактически «открыта» в XX в., но до сих пор ведутся дискуссии относительно международно-правового режима, который действует в ней.

Учитывая необходимость введения понятийного аппарата, следует, все же, не забывать о том, что единого определения для киберпространства не существует. Карл Саган (Carl Sagan) однажды сказал о том, что современное общество зависит от науки и технологий, но едва ли кто-нибудь имеет представление об этих двух понятиях.

Принято считать, что термин «киберпространство» впервые появился в фантастике, в произведении Уильяма Гибсона (William Gibson) «Нейромант» в 1984 г.: «Киберпространство. Коллективная галлюцинация… Графическое представление данных, извлекаемых из банков памяти любого компьютера в человеческой системе… Световые линии, расчертившие кажущееся пространство разума…» Так как киберпространство обладает своими отличительными чертами, например, виртуальностью, представление о нем на начальном этапе могло сформироваться лишь в литературе.

Позднее, в 1990-е гг., появилась так называемая «Всемирная паутина» (*World Wide Web*, *WWW*) [3], основателем которой стал Тим Бернерс-Ли (Tim Berners-Lee). Не будем останавливаться на рассмотрении истории появления сети «Интернет», подробно генезис информационно-коммуникационных технологий, в том числе сети «Интернет», описан в первой главе первого тома учебника «Международная информационная безопасность: теория и практика» [4]. Отметим, только то что первооткрывателями в этой области являются США. К 1995 г. лишь 1 % населения Земли имел доступ к сети «Интернет» [5], к 2005 г. цифра превысила 1 млрд пользователей по всему миру, в 2010 г. – 2 млрд пользователей, а в 2014 г. показатель достиг критической отметки в 3 млрд человек [6].

Киберпространство – это принципиально новое пространство, которое не может быть не урегулировано нормами права, однако в процессе правоприменения законодателю необходимо учитывать дискуссионные вопросы применимости понятия государственного суверенитета в нем, отсутствия универсального международного договора, позволяющего регулировать поведение государств в киберпространстве, а также единой судебной системы [7].

По мере развития технологий в современном мире, появилась потребность в «демистификации» киберпространства и разработке норм, направленных на регулирование его правового режима.

Для дефиниции киберпространства в международном праве необходимо рассмотреть общее определение данного термина, сложившееся, как было упомянуто выше, в фантастике. Термин «киберпространство» состоит из двух слов: «кибер», относящегося к электронной информации и компьютерным технологиям, и «пространство» – фактической территории, созданной электронной техникой для получения информации через взаимосвязанные

ISSN 2542-1514 (Print)

системы, и связанной с ними инфраструктуре. Киберпространство – это уникальный режим физических и виртуальных объектов, средств аппаратного обеспечения (*hardware*) и программного обслуживания (*software*), т. е. всех компьютерных сетей в мире, включая сеть «Интернет» и другие сети, обособленные или не подключенные к сети «Интернет». Киберпространство намного шире понятия сети «Интернет» и оттого не сводится лишь к использованию сетью «Интернет».

Жаклин Липтон обозначила основные черты, присущие киберпространству:

– глобальное распространение сети «Интернет»;

– специальные нормы, регулирующие поведение в онлайн среде в отличие от норм, регулирующих поведение в обычном, «физическом» мире;

– виды ущерба, понесенного в результате недобросовестного поведения в онлайн среде [8].

В науке встречаются точки зрения, согласно которым не имеет смысла регулировать киберпространство и рассматривать вопрос о применении в нем каких-либо норм, так как данный процесс больше напоминает изучение «права лошади» (*Law of the horse*), так как для изучения используются отдельные, не связанные между собой нормы, которые не представляется возможным унифицировать с целью изучения [9].

Лоуренс Лессиг, напротив, полагает, что с помощью киберпространства можно защитить все базовые ценности человечества. Более того, право киберпространства включает в себя не только законы, прецеденты, статуты, но и все построение сети «Интернет», нормы необязательного характера, различные стандарты, применимые в этой области [10].

В международном праве насчитывается двадцать восемь определений термина «киберпространство», что обусловлено постоянным развитием технологий[1].

Профессоры Хейке Кригер и Джордж Нолте отмечают, что регулирование киберпространства в международном праве может создать определенные вызовы устоявшемуся международному правопорядку [11].

В международном праве уже были схожие проблемы, связанные с регулированием воздушного и космического пространств. Основная сложность состояла в разграничении этих пространств, разработке универсальных международных договоров по регулированию поведения государств в воздушном и космическом пространствах [12].

Применимо ли такое сравнение в контексте киберпространства? Однозначного ответа на этот вопрос дать не представляется возможным.

Франсуа Делерю в своем исследовании, посвященном возможности применения международного права в киберпространстве, выделяет основные дискуссионные тезисы, на которые следует обратить внимание при попытке регулирования данной «территории» международным правом:

– термин «киберпространство» впервые появился в фантастике, это понятие не разрабатывалось инженерами или же специалистами в области техники;

– на данный момент неясным остается вопрос о рассмотрении термина как территории, где могут проводиться военные действия;

– ввиду отсутствия суверенитета государства в киберпространстве, дискуссионным остается вопрос о применимости концепции общего наследия человечества [12].

Можно опровергнуть тезис о киберпространстве как о пятом измерении наряду с земным пространством, водным, воздушным и космическим. В отличие от существующих четырех пространств, у киберпространства нет никакой территории в классическом представлении науки международного права. Напротив, все четыре существующих пространства уже, так или иначе, связаны с использованием виртуальных технологий, зависят от них, например, дистанционное зондирование Земли в космическом праве. Любое ограничение киберпространства носит условный характер и включает в себя среду, состоящую из сети «Интернет» и других компьютеров и телекоммуникационных сетей, подключенных к сети «Интернет» или нет. Сеть «Интернет» представляет собой лишь одну из многочисленных компьютерных сетей. Что касается вопроса о применимости международного права к киберпространству, то ответить на него следует положительно, однако в XXI в. основным вопросом для международного права является не простая констатация применимости существующих норм междуна-

[1] Киберпространство как стратегический инструмент социальной инженерии // Доклад эксперта Центра системных инициатив М.В. Мигулевой на V международной научной конференции «Китай и Россия: государственные стратегии развития», 28.05.2018, Санкт-Петербург. URL: https://center-si.com/analitics/m-v-migulyova-kiberprostranstvo-kak-strategicheskij-instrument-socialnoj-inzhenerii/ (дата обращения: 17.02.2022).

ISSN 2658-4050 (Online)

родного права, а ответ на другой, остро дискуссионный вопрос, как применять эти нормы.

Речь идет о тех аспектах, которые необходимо раскрыть для понимания природы киберпространства, в том числе уже рассмотренного значения термина в международном праве; вопроса о суверенитете и его применимости; источниках регулирования; актуальных проблемах и текущей тенденции регулирования.

2. Суверенитет в киберпространстве: дискуссионные аспекты

Как уже было указано ранее, киберпространство нельзя приравнять к сети «Интернет». «Кибертерритория» транснациональна по своей природе, не имеет единого контролирующего центра и может контролироваться лишь в определенных областях [13]. Ни о каких актах делимитации и демаркации говорить не приходится. Дискуссионным является вопрос о суверенитете государств в киберпространстве. Напомним, что признаками суверенитета государства являются: верховенство государства в пределах его территории и самостоятельность в международных отношениях. Территориальное верховенство означает распространение верховенства государства по всему пространству государственной территории [14]. Именно о территориальном верховенстве и пойдет речь. Киберпространство не может рассматриваться отдельно от государственного суверенитета, так как любые объекты критической информационной инфраструктуры, находящиеся в пределах государства, потенциально могут представлять опасность для других государств, в случае вмешательства в работу данных объектов на территории других государств. Установление суверенитета в этом пространстве могло бы поставить под вопрос классическую концепцию суверенитета государства, ведь речь пойдет о правомочии государства контролировать пространство за пределами государственных границ [15].

В науке международного права долгое время велись споры относительно ограничения суверенитета государства в киберпространстве. Либерально настроенные ученые выступали против какого бы то ни было регулирования со стороны государств и отстаивали право киберсистемы на внутреннее регулирование. По их мнению, киберпространство – это классический пример *terra nullius* («ничейной земли»)[2] , где невозможно применять государственное регулирование. Если продолжить и развить данную идею, то можно предположить, что речь пойдет о некоем «надтерриториальном» пространстве, но в классическом международном праве нет норм, которые могли бы его регулировать.

По мнению Паллави Кханна, ни одно государство не признало «самостоятельный» суверенитет киберпространства в прямо выраженной форме, что дает основания считать характер киберпространства вторичным, зависимым от первичного, основного государственного суверенитета [13]. Отсутствие признаков территориальности у такого пространства позволяет государствам частично наделить его таковыми посредством введения контрольных механизмов для обеспечения безопасности информационных потоков, поступающих через границы государств. В статье Паллави Кханна приводится пример дела с участием компании *Yahoo!*[3], которая отказывала Франции в прекращении продажи с аукциона атрибутов нацизма, ссылаясь на свободное регулирование сети «Интернет». Позднее, французскому суду удалось доказать, что американская компания не проводила торги в правовом вакууме, а распространяла рекламу на территории Франции, где подобные действия по оправданию нацизма запрещены уголовным законом [13].

Этот пример чрезвычайно важен для понимания регулирования действий компаний и государств в киберпространстве [16]. Безусловно, применения концепции классического территориального верховенства в данном пространстве ожидать не приходится, однако государство действует в киберпространстве через серверы, собственную инфраструктуру, находящуюся под его юрисдикцией, следовательно, и будет нести ответственность за противоправные действия.

Что касается суверенитета государства, то необходимость уважения к нему была подтверждена в деле Никарагуа против США [17]. На основании данного решения было признано, что все враж-

[2] Applicability of International Law on Cyber Espionage Intrusions // Ella Shoshan thesis, Faculty of law Stockholm University, Stockholm, 2014. URL: www.diva-portal.org/smash/get/diva2:799485/FullTeXT01 (Date views 17.02.2022).

[3] LICRA v. Yahoo! (Ligue contre le racisme et l'antisémitisme et Union des étudiants juifs de France c. Yahoo! Inc. et Société Yahoo! France), decided by the High Court of Paris (Tribunal de grande instance) in 2000. См. также: Henley J. Yahoo! Cleared in Nazi Case // The Guardian. 12.02.2003. URL: http://www.theguardian.com/technology/2003/feb/12/newmedia.media (дата обращения: 17.02.2022).

дебные кибероперации, направленные против киберинфраструктуры, располагающейся на территории другого государства, подразумевают нарушение суверенитета пострадавшего государства, даже если подобные операции не влекут за собой причинение вреда или ущерба, так как любые враждебные действия приравниваются к незаконному вмешательству посредством воздействия на территорию пострадавшего государства.

Осознав опасность безграничности киберпространства и изъятия его из-под государственного контроля, некоторые государства выдвинули инициативу по регулированию национального сегмента сети «Интернет». Так, Китай, Северная Корея выступают за его полную изоляцию[4]. Причем в последней разрешен доступ лишь к изолированному национальному сегменту сети «Интернет» – «Кванмён»[5]. Несмотря на попытки группы хакеров в 2013 г. подключить северокорейский сегмент к мировой сети, сделать это так и не удалось. Такие законы часто обосновываются необходимостью защиты государственного суверенитета от кибератак со стороны западных государств[6]. В настоящее время сложилась реалистическая концепция суверенитета, которая позволяет государствам использовать свою юрисдикцию на основании принципа территориальности (т. е. государство обладает правом регулировать передачу информации и использование информации лицами в киберпространстве в пределах границ государства). Суверенной власти принадлежит право контроля за аппаратным и программным обеспечением на своей территории. Другим принципом регулирования деятельности в киберпространстве принято считать так называемую «доктрину последствий», согласно которой учитываются последствия противоправных действий, которые могли быть совершены на территории другого государства, но причинили вред первому государству. В Стратегии национальной кибербезопасности США[7] перечислены те действия, которые могут быть отнесены к нарушению суверенитета государства: атаки на сетевое оборудование, использование такого оборудования и другие враждебные действия, совершаемые в киберпространстве, которые могут угрожать миру и стабильности, гражданским свободам и охране частной жизни лиц.

В международном праве не существует запрета на регулирование государством своего сегмента киберинфрастрктуры, однако это право может быть реализовано только в том случае, если государства соблюдают принципы международного права.

3. Источники регулирования поведения государств в киберпространстве

Следует отметить, что основной проблемой на сегодняшний день принято считать отсутствие универсальной конвенции, которая бы позволила урегулировать действия государств в киберпространстве. Основная сфера регулирования киберпространства – это кибербезопасность [18]. Согласно терминологии, составленной Международным Союзом Электросвязи (МСЭ), кибербезопасность включает в себя различные средства[8], направленные на защиту киберпространства как «киберокружающей» среды, защиту организации ее работы, а также защиту лиц, включенных в нее. По мнению профессора Джозефа Найи, вопрос о кибербезопасности должен быть разделен с учетом четырех базовых угроз: шпионаж, преступность, кибервойны, кибертерроризм [19]. Причинами появления этих угроз могут служить недостатки самой сети «Интернет», аппаратного и программного обеспечения и попытки государств и компаний перенести многие объекты критической инфраструктуры в сферу онлайн [20]. Обратим внимание лишь на некоторые источники, направленные на регулирование кибербезопасности.

Для характеристики источников международного права, регулирующих киберпространство, необходимо привести примеры трех подходов к регулированию этого пространства в международном праве: «киберинституционалистский», «киберлибертарианский» и подход «государственников». Киберинституционалисты (например, Тим Ву [21]) вы-

[4] 1680 VI. CYBERSPACE REGULATION AND THE DISCOURSE OF STATE SOVEREIGNTY // Harvard Law Review. 1999. URL: https://cyber.harvard.edu/property00/jurisdiction/hlr.html (Date views 17.02.2022).

[5] Кванмён – национальный интранет на территории КНДР. Создан в 2000 г. по инициативе правительства КНДР и является одной из самых крупных сетей, изолированных от сети «Интернет». Насчитывает от 1 до 5,5 тысяч сайтов.

[6] OpNorthKorea Text Release // Pastebin. 2013. URL: https://pastebin.com/ULEyQma4 (Date views 17.02.2022).

[7] International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World // Executive Office of the President of the United States. 2011. URL: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (Date views 17.02.2022).

[8] UN ITU-T Recommendation X.1205 (04/08): Overview of cybersecurity // The International Telecommunication Union. 2008. URL: https://www.itu.int/rec/T-REC-X.1205-200804-I (Date views 17.02.2022).

ISSN 2658-4050 (Online)

ступают за институционализацию и принятие международно-правовых норм, которые позволили бы регулировать киберсреду. Киберлибертарианцы (например, Джон Барлоу[9]), напротив, отказываются применять какие бы то ни было нормы в киберпространстве, ссылаясь на свободу в сети «Интернет». «Государственники» (например, Джеймс Льюис [22]) уверены в том, что в сложившейся ситуации только государства как первичные субъекты международного права могли бы предпринять усилия по созданию необходимых универсальных норм по регулированию киберпространства [23].

В Статуте Международного суда ООН (ст. 38) приведен перечень источников международного права[10]:

a) международные конвенции, как общие, так и специальные, устанавливающие правила, определенно признанные спорящими государствами;

b) международный обычай как доказательство всеобщей практики, признанной в качестве правовой нормы…

Универсальных международных конвенций, направленных на регулирование поведения государств в киберпространстве, на настоящий момент не существует. Государства не могут договориться о возможностях ограничения суверенитета, создании универсального судебного органа, уполномоченного рассматривать дела в киберпространстве. Немаловажным остается и вопрос о появлении новых субъектов, которые действуют в киберпространстве от своего имени и диктуют правила игры в этой области [24]. Далее кратко рассмотрим противоречия государств и новые инициативы по регулированию кибербезопасности, исходящие в том числе от мировых гигантов в кибериндустрии, таких как *Microsoft*[11].

Для начала предлагаем обратиться к дискуссионному вопросу о применимости международного обычного права в киберпространстве. Сложились ли некие международно-правовые обычаи, которые могли бы быть признаны всеми государствами?

Гэри Браун и Кейра Полет проанализировали применимость международного обычая в «пятом измерении» [25]. Рассуждая о применимости обычая, следует помнить о его двух необходимых элементах, «объективного» («общая практика») и субъективного («признания ее в качестве права»). По их мнению, первая кибератака произошла в Советском Союзе в 1982 г.[12], когда на Транссибирской магистрали произошел взрыв на газопроводе. Сообщалось, что взрыв произошел из-за запуска вредоносной программы и был результатом спецоперации ЦРУ. Позднее кибератаки стали возникать на территории США, например *Moonlight Maze* (1998–2001), *Code Red* (2001), *Mountain View* (2001). В 2010 г. компания *Google* сообщила о неправомерных действиях китайских хакеров, пытавшихся украсть интеллектуальную собственность компании. Хакеры установили вредоносные программы и взломали данные владельцев аккаунтов гугл-почты, которые отстаивали права человека [26]. В результате *Google* была вынуждена ограничить ведение бизнеса в Китае. Однако в данном контексте не идет речь о возникновении международно-правового обычая, так как для этого необходимо наличие действующего субъекта, совершающего данные действия, как, например, в случае с запуском первого спутника в СССР и в дальнейшем, появления принципа неприсвоения космического пространства.

Шпионаж мог бы рассматриваться как пример появления обычной нормы международного права в киберпространстве, но и здесь возникают сложности применения обычая в том понимании, в котором о нем говорится в ст. 38 Статута. В международном обычном праве нет норм, запрещающих осуществлять шпионаж в мирное время. В государствах на национальном уровне могут быть законы, запрещающие подобные действия. Так, примером могут служить США, где шпионаж наказывается смертной казнью[13]. По общему правилу, шпионаж не запрещен международным правом. Говоря о действиях в киберпространстве, следует отнести их по своей природе не к военным действиям, а к шпионажу, так как вредоносные программы внедряются в системы государственных органов и фактически «собирают и

[9] A Declaration of the Independence of Cyberspace // J.P. Barlow, Electronic Frontier Foundation, 1996. URL: https://www.eff.org/cyberspace-independence (Date views 17.02.2022).

[10] Statute of the International Court of Justice // The United Nations, 1945. URL: https://www.icj-cij.org/en/statute (Date views 17.02.2022).

[11] 'Digital Peace Now' launches this weekend // Kate O'Sullivan, Microsoft, 2018. URL: https://blogs.microsoft.com/on-the-issues/2018/09/28/digital-peace-now-launches-this-weekend/ (Date views 17.02.2022).

[12] Stephens B. The Limits of Stuxnet // The Wall Street Journal. Jan. 18, 2011. URL: https://www.wsj.com/articles/SB10001424052748703396604576087632882247372.

[13] 18 U.S.C pt.1, chap. 37 "Espionage and Cencorship", para. 793-98 // The United States Code. URL: https://www.law.cornell.edu/uscode/text/18/part-I/chapter-37 (Date views 17.02.2022).

аккумулируют» накопленную информацию. Точно так же, как и классический шпионаж в международном праве, кибершпионаж подпадает под разрешительный режим, при котором государства сами на основании норм международного права решают вопрос о правомерности тех или иных действий. С одной стороны, кибератаки и другие противоправные действия могут, подобно вооруженному нападению на территорию другого государства [27], привести к конкретным физическим последствиям (взрыв, причинение ущерба, вывод из строя). С другой стороны, если предположить, что подобные действия относятся к боевым, то что делать в том случае, если программа временно выводит из строя электроэнергетическую сеть? В данном примере не были совершены боевые действия, но сеть временно прекратила работу. В таком случае атака носит «околобоевой» характер и также подпадает под определение вооруженного нападения [28]. Для регулирования международным обычным правом необходимо сформировать позицию государств по рассмотрению данных кейсов либо на основании понятия «шпионаж» (разрешительный режим), либо на основании концепции «вооруженного нападения» (запретительный режим в международном праве).

В 2011 г. в США была разработана Стратегия национальной безопасности США[14], где была дана попытка повлиять на развитие обычных норм в киберпространстве. В документе подчеркивается, что для создания таких норм не нужно пересматривать международные обычные нормы, международное право в целом. Все действующие международно-правовые нормы будут действовать и в мирное, и в военное время. Безусловно, нормы, содержащиеся в документе, не могут считаться обычными нормами международного права, но могли бы создать предпосылки для сотрудничества государств ввиду нежелания принимать первичные источники международного права, международные договоры универсального характера. Представляется чрезмерно недальновидным подход к рассмотрению кибершпионажа на основании разрешительного порядка, что может привести к массовым кибератакам в дальнейшем.

Важным шагом на пути к решению проблемы, связанной с кибербезопасностью и регулированием поведения государств в киберпространстве, могло бы стать принятие конвенции, которая включала бы в себя базовые определения и нормы. На сегодняшний день единственным документом, регулирующим киберпреступность, является Будапештская конвенция 2001 г.[15], однако она была принята в Совете Европы и носит региональный характер, хотя участниками конвенции являются в том числе и неевропейские государства.

Как европейские, так и неевропейские государства должны предпринять усилия по определенной адаптации существующих норм международного права к киберпространству, однако на практике это требование вряд ли может быть реализовано в ближайшее время. Так, в 2013 и 2015 гг. группа правительственных экспертов подготовила доклады, в которых было признано и подтверждено применение положений международного права и, в частности, Устава ООН 1945 г. к киберпространству[16]. В 2017 г. в Группе правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций велась дискуссия о возможности применения всех отраслей международного права на кибертерритории[17], например, о возможности применения всех норм международного гуманитарного права в киберпространстве, о возможности применения контрмер, о праве на самооборону. Три государства, Россия, Китай и Куба, последовательно отстаивали необходимость отказа от применения вышеперечисленных режимов, но с соблюдением норм всех других отраслей международного права. Позиция России объясняется тем, что отсутствие специальных норм регулирования киберпространства может послужить пусковым механизмом для развязывания гонки вооружений в «пятом измерении». А.В. Крут-

[14] International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World // Executive Office of the President of the United States. 2011. URL: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (Date views 17.02.2022).

[15] Convention on Cybercrime // Council of Europe. 2001. URL: https://rm.coe.int/1680081561 (Date views 17.02.2022).

[16] UN Doc A/68/98, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security // General Assembly of the United Nations. 2013. URL: https://undocs.org/A/68/98 (Date views 17.02.2022); UN Doc A/70/174, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security // General Assembly of the United Nations, 2015. URL: https://undocs.org/en/A/70/174 (Date views 17.02.2022).

[17] Korzak E. UN GGE on Cybersecurity: The End of an Era? // The Diplomat. 2017. URL: https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/ (Date views 17.02.2022).

ISSN 2658-4050 (Online)

ских[18] заявляет о недопустимости милитаризации киберпространства, недопущении применения силы, уважении государственного суверенитета, прав и свобод человека. По его мнению, в сущесвтующих нормах международного права не учитываются основные признаки киберпространства и вытекающая из них проблема установления источника кибератаки. Для США[19] и Великобритании[20], напротив, вопрос о применении общих норм права не вызывает сомнений, согласно позиции данных государств, не нужно разрабатывать новые нормы международного права для регулирования киберпространства и тем самым поставить под сомнение существующий международный правопорядок, так как в дальнейшем неизбежно придется пересматривать весь каркас уже действующих международно-правовых норм. С другой стороны, если отказаться от принятия каких бы то ни было специальных норм, то достичь консенсуса в позициях государств вряд ли будет возможно, тогда как уровень неопределенности будет возрастать, а развитие, предположительно, новой отрасли международного права будет остановлено. Актуальным остается и вопрос о различиях в терминологии на национальном уровне. Так, если для большинства государств речь идет о регулировании кибербезопасности (*cybersecurity*) [29], где акцент ставится на безопасности в понимании науки международного права, то для России и Китая акцент делается на «информационной безопасности внутри государства» (*information security*) и на защите государственного суверенитета [30].

4. Актуальные проблемы и текущие тенденции регулирования

Осознавая сложность единообразного мнения по многим вопросам, государства идут по пути регионального сотрудничества. ООН, ЕС, СНГ, АСЕАН, ОАГ разрабатывают многочисленные нормы по регулированию кибербезопасности и многим другим аспектам сотрудничества [31], однако повышенное продуцирование норм не может привести к единообразной практике применения в международном праве.

В киберпространстве главными субъектами считаются не только государства, но и компании *Google*, *Facebook*[21], *Microsoft* и др. В 2018 г. компания Майкрософт запустила инициативу *Digital Peace Now*[22] для принятия цифровой Женевской конвенции или так называемой «Женевской конвенции 5.0», которая бы позволяла защитить права граждан от кибератак в мирное время с помощью специализированных компаний, т. е. использовалось *jus contra bellum*, направленное на предупреждение активных ответных действий со стороны государств [12].

Очевидно, что киберпространство не может оставаться «свободной от закона зоной» (*law-free zone*), поэтому Гарольд Хоннжу Кох [32] предлагает использовать сложившийся в США подход к данной проблеме, вызванный нехваткой источников регулирования. Позиция США заключается в применимости всех принципов международного права в киберпространстве, т. е., например, кибератака может подпадать под действие ст. 2 п. 4 Устава ООН, а сами действия необходимо квалифицировать как использование силы в случае соблюдения следующих условий: наличие соответствующего контекста, субъекта, действия, цели, местонахождения, последствия, намерения. В киберсреде могут и должны, по его мнению, применяться меры самозащиты для пострадавших государств, а также необходимо на основе критерия необходимости и пропорциональности применять *jus in bello*. От государств будет требоваться пересмотреть представление о классических видах оружия и включить новые виды кибероружия.

[18] 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 России: офиц сайт. 29.06.2017. URL: https://www.mid.ru/ru/press_service/spokesman/answers/1549172/ (дата обращения: 17.02.2022).

[19] 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 // United States Mission to the United Nations. 23.06.2017. URL: https://usun.usmission.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-tele/ (Date views 17.02.2022).

[20] Cyber and International Law in the 21st Century // J. Wright, speech of the UK Attorney General. 23.05.2018. URL: https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century (Date views: 17.02.2022).

[21] Корпорация *Meta*, владеющая *Facebook*, признана в России экстремистской, ее деятельность на территории Российской Федерации запрещена.

[22] Digital Peace Now // Global movement of digital citizens from over 170 countries, launched by Microsoft in 2018. URL: https://digitalpeacenow.org/ (Date views: 17.02.2022).

Для квалификации деяния необходимо разобраться с вопросом его совершения государством, однако данный вопрос практически не может быть разрешим, так как кибероружие могут приобретать не только государства, но и несубъекты международного права. Попытка уравнять государства с различным уровнем развития технических возможностей в киберпространстве также вряд ли может увенчаться успехом. Таким образом, может возникнуть фрагментация международного права: функциональная (различные нормы и режимы регулирования поведения государств в киберпространстве) и географическая (увеличение региональных договоров и соглашений), не способствующая согласованию позиций государств.

Различные инициативы, центры и неправительственные организации также участвуют в процессе стабилизации международного правопорядка в киберсреде. Так, важную роль играет Глобальная комиссия по стабильности киберпространства, состоящая из 26 выдающихся лиц, специализирующихся в области изучения киберпространства[23].

В рамках такого специализированного учреждения ООН, как Международный союз электросвязи, разрабатываются определения основных терминов, инициативы в области правового регулирования киберпространства. Так, в 2014 г. была запущена инициатива по введению Индекса глобальной кибербезопасности для отслеживания ее уровня в мире[24]. В 2020 г. Россия в данном рейтинге заняла почетное пятое место, а США – первое[25].

Последнее, на чем хотелось бы остановиться, это текущие тенденции в части регулирования киберпространства в международном праве. Группой правительственных экспертов ООН 28 мая 2021 г. был разработан доклад по вопросам применимости норм международного права в киберпространстве[26]. Примечательно, что впервые с 2017 г. сторонам удалось достичь консенсуса по многочисленным вопросам, включенным в повестку дня. Отдельные государства: Россия, Казахстан, Киргизия, Таджикистан, Узбекистан и Китай – предложили принять Международный кодекс поведения в области информационной безопасности. Важнейшим шагом на пути к решению сложившихся проблем в части применения норм международного гуманитарного права стало подтверждение применения данной отрасли к киберпространству во время вооруженного конфликта. Было подтверждено применение всех основополагающих принципов международного права. От государств в данной ситуации требуется взаимное сотрудничество и обмен практикой разрешения спорных ситуаций в киберпространстве, о чем уже говорилось выше.

Однако даже с учетом данных достижений остается неясным, когда же государства смогут разработать конвенцию, которая бы позволила регулировать киберпространство с учетом существующих норм. Можно было бы предположить, что со временем вопрос будет так или иначе решен, как в случае с космическим пространством, в освоении которого участвовали Россия и США, однако не государства играют важную роль и диктуют правила поведения в киберпространстве, а частные компании, в том числе физические лица, корпорации, которые, в свою очередь, не могут считаться субъектами международного права. Далее, остается нерешенным вопрос, связанный с анонимностью поведения в киберпространстве, и вытекающая из этого проблема присвоения деяния. На международном уровне (ООН) не наблюдается прогресса в процессе решения поставленных задач, многие нормы носят характер *soft law*, а не *hard law*, что приводит к их дублированию и несогласованной практике поведения государств.

Майкл П. Фишеркеллер предлагает неоднозначный, на первый взгляд, выход из сложившейся ситуации. Он говорит о необходимости пересмотра подхода к невмешательству в части принуждения в пользу «эксплуатации киберпространства»[27] (использования информации). Не все меры принуждения в

[23] About – Global Commission on the Stability of Cyberspace (GCSC) // Global Commission on the Stability of Cyberspace. URL: https://cyberstability.org/about/ (Date views: 17.02.2022).
[24] Global Cybersecurity Index 2020 // International Telecommunication Union. 2021. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx (Date views: 17.02.2022).
[25] Global Cybersecurity Index 2020 REPORT // International Telecommunication Union. 2021. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (Date views: 17.02.2022).
[26] Letter of transmittal of the report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security // Chair of the Group Guilherme de Aguiar Patriota. 28.05.2021. URL: https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf (Date views: 17.02.2022).
[27] Fischerkeller M.P.Current International Law Is Not an Adequate Regime for Cyberspace // Lawfare. 22.04.2021. URL: https://www.lawfareblog.com/current-international-law-not-adequate-regime-cyberspace (Date views: 17.02.2022).

международном праве могут считаться противоправными, так же, как и не все меры по эксплуатации могут относится к противоправным. Принцип эксплуатации позволит государствам самостоятельно перечислить те действия, которые будут рассматриваться как вмешательство в «национальный сектор» киберпространства (например, государство, как это сделали США, может отнести эксплуатацию интеллектуальной собственности к противоправному действию). Согласно классическому определению, эксплуатация – это противоправное действие, совершаемое в киберпространстве с целью получения информации, однако автор статьи не согласен со столь узким и однобоким представлением об эксплуатации. Вместо этого было бы правильным рассматривать данный термин как использование технологий одним государством для получения выгод от несовершенств в киберпространстве другого государства с целью получения конкурентного преимущества.

Подобные меры не повлияют на изменение ситуации с существующими пробелами в области универсального киберрегулирования в международном праве. Шагами на пути к международному правотворчеству могут стать: проведение международного саммита с участием государств, международных организаций, представителей компаний для согласования проекта будущей конвенции; пересмотр существующего каркаса норм мягкого права с целью выявления единообразных норм; отказ от информационной безопасности в пользу кибербезопасности; начало работы Комиссии международного права ООН для представления проекта соответствующей конвенции.

СПИСОК ЛИТЕРАТУРЫ

1. Choucri N. Cyberpolitics in International Relations / N. Choucri. – The MIT Press, 2012. – 320 p. – DOI: 10.7551/mitpress/7736.001.0001.

2. Roscini M. World Wide Warfare – Jus ad bellum and the Use of Cyber Force / M. Roscini // Max Planck Yearbook of United Nations Law / eds. A. Von Bogdandy, R. Wolfrum, C.E. Philipp. – Leiden : Martinus Nijhoff, 2010. – Vol. 14. – P. 85–130.

3. Kahin B. Coordinating the Internet / B. Kahin, J. H. Keller. – The MIT Press, 1997. – 510 p. – DOI: 10.7551/mitpress/2170.001.0001.

4. Международная информационная безопасность: Теория и практика : в 3 т. / под общ. ред. А. В. Крутских. – 2-е изд. доп. – М. : Аспект Пресс, 2021. – Т. 1. – 384 с.

5. Ceruzzi P. E. Computing: A Concise History / P. E. Ceruzzi. – The MIT Press, 2012. – 199 p. – DOI: 10.7551/mitpress/9426.001.0001.

6. Srinivasan R. Beyond the Valley: How Innovators around the World are Overcoming Inequality and Creating the Technologies of Tomorrow / R. Srinivasan. – The MIT Press, 2019. – 424 p. – DOI: 10.7551/mitpress/11894.001.0001.

7. Biegler S. Beyond Our Control?: Confronting the Limits of Our Legal System in the Age of Cyberspace / S. Biegler. – The MIT Press, 2003. – 472 p. – DOI: 10.7551/mitpress/1583.001.0001.

8. Lipton J. Rethinking Cyberlaw: A New Vision for Internet Law / J. Lipton. – Edward Elgar Publishing LTD, 2015. – 176 p.

9. Frank H. E. Cyberspace and the Law of the Horse / H. E. Frank // University of Chicago Legal Forum. – 1996. – P. 207–216

10. Lessig L. Code and Other Laws of Cyberspace / L. Lessig. – New York : Basic Books, 1999. – 320 p.

11. Krieger H. The International Rule of Law: Rise or Decline? / H. Krieger, G. Nolte, A. Zimmermann. – Oxford : Oxford University Press, 2019. – 378 p. – DOI: 10.1093/oso/9780198843603.001.0001.

12. Delerue F. Cyber Operations and International Law / F. Delerue. – Cambridge : Cambridge University Press, 2020. – 549 p. – DOI: 10.1017/9781108780605.

13. Khanna P. State Sovereignty and Self-Defence in Cyberspace / P. Khanna // BRICS Law Journal. – 2018. – Vol. 5, no. 4. – P. 139–154. – DOI: 10.21684/2412-2343-2018-5-4-139-154.

14. Международное право : учеб. для вузов : в 2 ч. / отв. ред. А. Н. Вылегжанин. – 4-е изд., перераб. и доп. – М. : Юрайт, 2021. – Ч. 1. – 329 с.

15. Kahin B. Borders in Cyberspace: Information Policy and the Global Information Infrastructure / B. Kahin, C. Nesson. – The MIT Press, 1997. – 374 p. – DOI: 10.7551/mitpress/1648.001.0001.

16. Jørgensen R. F. Human Rights in the Age of Platforms / R. F. Jørgensen. – The MIT Press, 2019. – 392 p. – DOI: 10.7551/mitpress/11304.001.0001.

17. Schmitt M. N. The Law of Cyber Warfare: Quo Vadis? / M. N. Schmitt // Stanford Law & Policy Review. – 2014. – Vol. 25, iss. 2. – P. 269–299.

18. Wolff J. You'll See This Message When It Is Too Late: The Legal and Economic Aftermath of Cybersecurity Breaches / J. Wolff. – The MIT Press, 2018. – 336 p. – DOI: 10.7551/mitpress/11336.001.0001.

19. Nye J. S. Cyber Power / J. S. Nye. – Belfer Center for Science and International Affairs, Harvard Kennedy School, May, 2010. – 24 p.

20. Coleman S. Connecting Democracy: Online Consultation and the Flow of Political Communication / S. Coleman, P. M. Shane. – The MIT Press, 2011. – 416 p. – DOI: 10.7551/mitpress/9006.001.0001.

21. Wu T. S. Cyberspace Sovereignty? The Internet and the International System / T. S. Wu // Harvard Journal of Law & Technology. – 1997. – Vol. 10, № 3. – P. 647–666.

22. Lewis J. Sovereignty and the Role of Government in Cyberspace / J. Lewis // Brown Journal of World Affairs. – 2010. – Vol. 16, iss. 2. – P. 55–65.

23. Adonis A. A. International Law on Cyber Security in the Age of Digital Sovereignty / A. A. Adonis // E-International Relations. – Mar 14 2020. – URL: https://www.e-ir.info/2020/03/14/international-law-on-cyber-security-in-the-age-of-digital-sovereignty/.

24. Rheingold H. The Virtual Community: Homesteading on the Electronic Frontier / H. Rheingold. – The MIT Press, 2000. – 447 p. – DOI: 10.7551/mitpress/7105.001.0001.

25. Brown G. The Customary International Law of Cyberspace / G. Brown, K. Poellet // Strategic Studies Quarterly. – 2012. – Vol. 6, iss. 3. – P. 126–145.

26. Barassi V. Child Data Citizen: How Tech Companies Are Profiling Us from Before Birth / V. Barassi. – The MIT Press, 2020. – 232 p. – DOI: 10.7551/mitpress/12415.001.0001.

27. Webb M. Coding Democracy: How Hackers Are Disrupting Power, Surveillance, and Authoritarianism / M. Webb. – The MIT Press, 2020. – 416 p. – DOI: 10.7551/mitpress/11669.001.0001.

28. Schmitt M. N. Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework / M. N. Schmitt // Columbia Journal of Transnational Law. – 1999. – 1998-1999, vol. 3. – P. 885–937.

29. Landau S. Surveillance or Security?: The Risks Posed by New Wiretapping Technologies / S. Landau. – The MIT Press, 2011. – 383 p. – DOI: 10.7551/mitpress/8623.001.0001.

30. Henriksen A. The end of the road for the UN GGE process: The future regulation of cyberspace / A. Henriksen // Journal of Cybersecurity. – 2019. – Vol. 5, iss. 1. – P. 1–9. – DOI: 10.1093/cybsec/tyy009.

31. Jemielniak D. Collaborative Society / D. Jemielniak, A. Przegalinska. – The MIT Press, 2020. – 256 p. – DOI: 10.7551/mitpress/11587.001.0001.

32. Koh H. H. International Law in Cyberspace / H. H. Koh // Harvard International Law Journal Online. – 2012. – Vol. 54. – P. 1–12. – URL: https://harvardilj.org/wp-content/uploads/sites/15/2012/12/Koh-Speech-to-Publish1.pdf (дата обращения: 22.11.2022)

REFERENCES

1. Choucri N. *Cyberpolitics in International Relations*. The MIT Press, 2012. 320 p. DOI: 10.7551/mitpress/7736.001.0001.

2. Roscini M. World Wide Warfare – Jus ad bellum and the Use of Cyber Force, in: Bogdandy A. Von, Wolfrum R., Philipp C.E. (eds.). *Max Planck Yearbook of United Nations Law*. Leiden, Martinus Nijhoff Publ., 2010, vol. 14, pp. 85–130.

3. Kahin B., Keller J.H. *Coordinating the Internet*. The MIT Press, 1997. 510 p. DOI: 10.7551/mitpress/2170.001.0001.

4. Krutskikh A.V. *International information security: theory and practice*, in 3 volumes, 2nd ed. Moscow, Aspekt Press Publ., 2021. Vol. 1. 384 p. (In Russ.).

5. Ceruzzi P.E. *Computing: A Concise History*. The MIT Press, 2012. 199 p. DOI: 10.7551/mitpress/9426.001.0001.

6. Srinivasan R. *Beyond the Valley: How Innovators around the World are Overcoming Inequality and Creating the Technologies of Tomorrow*. The MIT Press, 2019. 424 p. DOI: 10.7551/mitpress/11894.001.0001.

7. Biegler S. *Beyond Our Control?: Confronting the Limits of Our Legal System in the Age of Cyberspace*. The MIT Press, 2003. 472 p. DOI: 10.7551/mitpress/1583.001.0001.

8. Lipton J. *Rethinking Cyberlaw: A New Vision for Internet Law*. Edward Elgar Publishing LTD, 2015. 176 p.

9. Frank H.E. Cyberspace and the Law of the Horse, in: *University of Chicago Legal Forum*, 1996, pp. 207–216

10. Lessig L. *Code and Other Laws of Cyberspace*. New York, Basic Books Publ., 1999. 320 p.

11. Krieger H., Nolte G., Zimmermann A. *The International Rule of Law: Rise or Decline?* Oxford, Oxford University Press, 2019. 378 p. DOI: 10.1093/oso/9780198843603.001.0001.

12. Delerue F. *Cyber Operations and International Law*. Cambridge, Cambridge University Press, 2020. 549 p. DOI: 10.1017/9781108780605.

13. Khanna P. State Sovereignty and Self-Defence in Cyberspace. *BRICS Law Journal*, 2018, vol. 5, no 4, pp. 139–154. DOI: 10.21684/2412-2343-2018-5-4-139-154.

14. Vylegzhanin A.N. (ed.). *International law*, Textbook for universities, in 2 parts. Moscow, Yurait Publ., 2021. Pt. 1. 329 p. (In Russ.).

15. Kahin B., Nesson C. *Borders in Cyberspace: Information Policy and the Global Information Infrastructure*. The MIT Press, 1997. 374 p. DOI: 10.7551/mitpress/1648.001.0001.

16. Jørgensen R.F. *Human Rights in the Age of Platforms*. The MIT Press, 2019. 392 p. DOI: 10.7551/mitpress/11304.001.0001.

17. Schmitt M.N. The Law of Cyber Warfare: Quo Vadis? *Stanford Law & Policy Review*, 2014, Vol. 25, iss. 2, pp. 269–299.

18. Wolff J. *You'll See This Message When It Is Too Late: The Legal and Economic Aftermath of Cybersecurity Breaches*. The MIT Press, 2018. 336 p. DOI: 10.7551/mitpress/11336.001.0001.

19. Nye J.S. *Cyber Power.* Belfer Center for Science and International Affairs, Harvard Kennedy School, May, 2010. 24 p.

20. Coleman S., Shane P.M. *Connecting Democracy: Online Consultation and the Flow of Political Communication*. The MIT Press, 2011. 416 p. DOI: 10.7551/mitpress/9006.001.0001.

21. Wu T.S. Cyberspace Sovereignty? The Internet and the International System. *Harvard Journal of Law & Technology*, 1997, vol. 10, no. 3, pp. 647–666.

22. Lewis J. Sovereignty and the Role of Government in Cyberspace. *Brown Journal of World Affairs*, 2010, vol. 16, iss. 2, pp. 55–65.

23. Adonis A.A. International Law on Cyber Security in the Age of Digital Sovereignty. *E-International Relations*, Mar 14 2020, available at: https://www.e-ir.info/2020/03/14/international-law-on-cyber-security-in-the-age-of-digital-sovereignty/.

24. Rheingold H. *The Virtual Community: Homesteading on the Electronic Frontier*. The MIT Press, 2000. 447 p. DOI: 10.7551/mitpress/7105.001.0001.

25. Brown G., Poellet K. The Customary International Law of Cyberspace. *Strategic Studies Quarterly*, 2012, vol. 6, iss. 3, pp. 126–145.

26. Barassi V. *Child Data Citizen: How Tech Companies Are Profiling Us from Before Birth*. The MIT Press, 2020. 232 p. DOI: 10.7551/mitpress/12415.001.0001.

27. Webb M. *Coding Democracy: How Hackers Are Disrupting Power, Surveillance, and Authoritarianism*. The MIT Press, 2020. 416 p. DOI: 10.7551/mitpress/11669.001.0001.

28. Schmitt M.N. Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. *Columbia Journal of Transnational Law*, 1999. 1998–1999, vol. 3, pp. 885–937.

29. Landau S. *Surveillance or Security?: The Risks Posed by New Wiretapping Technologies*. The MIT Press, 2011. 383 p. DOI: 10.7551/mitpress/8623.001.0001.

30. Henriksen A. The end of the road for the UN GGE process: The future regulation of cyberspace. *Journal of Cybersecurity*, 2019, vol. 5, iss. 1, pp. 1–9. DOI: 10.1093/cybsec/tyy009.

31. Jemielniak D., Przegalinska A. *Collaborative Society*. The MIT Press, 2020. 256 p. DOI: 10.7551/mitpress/11587.001.0001.

ISSN 2542-1514 (Print)

32. Koh H. H. International Law in Cyberspace. *Harvard International Law Journal Online*, 2012, vol. 54, pp. 1–12, available at: https://harvardilj.org/wp-content/uploads/sites/15/2012/12/Koh-Speech-to-Publish1.pdf (accessed date: 22.11.2022).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Иванова Ксения Алексеевна – кандидат юридических наук, [1] директор научно-образовательного Центра местного самоуправления Института управления и регионального развития, [2] доцент кафедры конституционного и муниципального права
[1] *Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации (РАНХиГС)*
[2] *Тюменский государственный университет*
[1] 119571, Россия, г. Москва, пр. Вернадского, 84
[2] 625003, Россия, г. Тюмень, ул. Володарского, 6
E-mail: ivanova-ka@ranepa.ru
SPIN-код РИНЦ: 6610-9218; AuthorID: 695216

Мылтыкбаев Мади Женискалиевич – аспирант кафедры международного права
Московский государственный институт международных отношений (университет) Министерства иностранных дел Российской Федерации
119454, Россия, г. Москва, пр. Вернадского, 76
E-mail: myltykbaev@my.mgimo.ru
ORCID: 0000-0003-3261-9927
ResearcherID: AAA-3864-2019
SPIN-код РИНЦ: 6952-1510; AuthorID: 1028441

Штодина Дарья Дмитриевна – аспирант кафедры международного права
Московский государственный институт международных отношений (университет) Министерства иностранных дел Российской Федерации
119454, Россия, г. Москва, пр. Вернадского, 76
E-mail: dashashtodina96@gmail.com
ORCID: 0000-0003-4730-9614
ResearcherID: AAE-5310-2022
SPIN-код РИНЦ: 3795-6159; AuthorID: 1136990

INFORMATION ABOUT AUTHORS

Ksenia A. Ivanova – PhD in Law; [1] Director, Center of Local Authorities of the Institute of Management and Regional Development; [2] Associate Professor, Department of Constitutional and Municipal Law
[1] *Russian Presidential Academy of National Economy and Public Administration (RANEPA)*
[2] *University of Tyumen*
[1] 84, Vernadskogo pr., Moscow, 119571, Russia
[2] 6, Volodarskogo ul., Tyumen, 625003, Russia
E-mail: ivanova-ka@ranepa.ru
RSCI SPIN-code: 6610-9218; AuthorID: 695216

Madi Zh. Myltykbaev – Post-graduate student, International Law Department
MGIMO University
76, Vernadskogo pr., Moscow, 119454, Russia
E-mail: myltykbaev@my.mgimo.ru
ORCID: 0000-0003-3261-9927
ResearcherID: AAA-3864-2019
RSCI SPIN-code: 6952-1510; AuthorID: 1028441

Daria D. Shtodina – Post-graduate student, International Law Department
MGIMO University
76, Vernadskogo pr., Moscow, 119454, Russia
E-mail: dashashtodina96@gmail.com
ORCID: 0000-0003-4730-9614
ResearcherID: AAE-5310-2022
RSCI SPIN-code: 3795-6159; AuthorID: 1136990

БИБЛИОГРАФИЧЕСКОЕ ОПИСАНИЕ СТАТЬИ

Иванова К.А. Понятие киберпространства в международном праве / К.А. Иванова, М.Ж. Мылтыкбаев, Д.Д. Штодина // Правоприменение. – 2022. – Т. 6, № 4. – С. 32–44. – DOI: 10.52468/ 2542-1514.2022. 6(4).32-44.

BIBLIOGRAPHIC DESCRIPTION

Ivanova K.A., Myltykbaev M.Zh., Shtodina D.D. The concept of cyberspace in international law. *Pravoprimenenie = Law Enforcement Review*, 2022, vol. 6, no. 4, pp. 32–44. DOI: 10.52468/2542-1514. 2022.6(4).32-44. (In Russ.).