DOI: https://www.doi.org/10.32523/2791-0954-2024-11-3-23-35

Киберпространство как новый вид пространства в международном праве

Саидмухторов Алишер Абдухоликович
Кандидат юридических науки, доцент,
Директор научно-исследовательского института политических процессов, дипломатии и проблем глобализации, Академия государственного управления при Президенте Республики Таджикистан,
г. Душанбе, Республика Таджикистан.
e-mail: saidmukhtorov.a@gmail.com
ORCID: 0000-0002-9592-3056; JEL-code: K33 Международное право

Аннотация. В настоящей статье раскрывается сущность понятия киберпространства, вопросы о его существовании в современном международном праве, а также приведены понятия кибербезопасности, киберсуверенитета и кибердипломатии. Сегодня, в виду стремительно развивающихся современных информационных технологий возникает необходимость вести речь о киберпространстве и её составляющих в международном праве. Будучи относительным новшеством, вопрос о киберпространстве в международном праве требует достаточно тщательного анализа и правового регулирования со стороны субъектов международного права. Это необходимо в первую очередь для чёткого определения вопроса отнесения киберпространства к одному из пространств международного права. Прогрессивно развивающиеся новые технологии цифрового века порождают новые вызовы, с которыми международное сообщество должно справиться. Масштабы развития информационных технологий обуславливают формирование новых понятий, механизмов и методов должного реагирования со стороны соответствующих субъектов. С недавних пор в научных кругах преобладает идея: наряду с сухопутным, воздушным, космическим, морским пространством.

***Ключевые слова**:* киберпространство, кибернетика, кибербезопасность, кибердипломатия, киберзащита, кибер суверенитет, киберпреступность, безопасность государств.

Киберкеңістік халықаралық құқықтағы кеңістіктің жаңа түрі ретінде

Саидмухторов Алишер Абдухоликович
Заң ғылымдарының кандидаты, доцент,

Саяси процестер, дипломатия және жаһандану мәселелері ғылыми-зерттеу институтының директоры, Тәжікстан Республикасы Президентінің жанындағы Мемлекеттік басқару академиясы,
Душанбе қ., Тәжікстан Республикасы.
e-mail: saidmukhtorov.a@gmail.com
ORCID: 0000-0002-9592-3056; JEL-code: K33 Халықаралық құқық

Түйіндеме. Бұл мақалада киберкеңістік ұғымының мәні, оның қазіргі халықаралық құқықта бар екені туралы мәселелер қарастырылады, сонымен қатар киберқауіпсіздік, кибер егемендік және кибер дипломатия ұғымдары келтірілген. Бүгінгі таңда қарқынды дамып келе жатқан заманауи ақпараттық технологияларға байланысты киберкеңістік және оның халықаралық құқықтағы компоненттері туралы айту қажеттілігі туындайды. Халықаралық құқықтағы киберкеңістік мәселесі салыстырмалы түрде жаңалық бола отырып, халықаралық құқық субъектілері тарапынан жеткілікті мұқият талдау мен құқықтық реттеуді талап етеді. Бұл, ең алдымен, киберкеңістікті халықаралық құқық кеңістігінің біріне жатқызу мәселесін нақты анықтау үшін қажет. Цифрлық ғасырдың прогрессивті дамып келе жатқан жаңа технологиялары халықаралық қауымдастық шешуі керек жаңа қиындықтарды тудырады. Ақпараттық технологиялардың даму ауқымы тиісті субъектілер тарапынан тиісті жауап берудің жаңа түсініктерін, тетіктері мен әдістерін қалыптастыруды анықтайды. Соңғы уақытта ғылыми ортада «құрлық, әуе, ғарыш, теңіз кеңістігімен қатар, киберкеңістік жақын арада мемлекеттік аумақтың қатарына қосылуы мүмкін» деген идея басым боп келеді.

Негізгі сөздер: киберкеңістік, кибернетика, киберқауіпсіздік, кибердипломатия, киберқорғау, кибер егемендік, мемлекеттердің қауіпсіздігі.

Cyberspace as a new kind of space in international law

Saidmukhtorov Alisher Abdukholikovich
Candidate of Law, Associate Professor,
Director of the research institute political processes, diplomacy and globalization issues, Academy of Public Administration under the President of the Republic of Tajikistan,
Dushanbe, Republic of Tajikistan.
e-mail: saidmukhtorov.a@gmail.com
ORCID: 0000-0002-9592-3056; JEL-code: K33 International law

Abstract: This article reveals the essence of the concept of cyberspace, questions about its existence in modern international law, and also provides the concepts of cybersecurity cybersovereignty, and cyberdiplomacy. Today, in view of the rapidly developing modern information technologies, there is a need to talk about cyberspace and its components in international law. Being a relative innovation, the issue of

cyberspace in international law requires quite careful analysis and legal regulation by subjects of international law. This is necessary, first of all, to clearly define the issue of classifying cyberspace as one of the spaces of international law. The progressively developing new technologies of the digital age are creating new challenges that the international community must cope with. The scale of development of information technologies determines the formation of new concepts, mechanisms and methods of proper response on the part of relevant entities. Recently, an idea has been prevailing in scientific circles: along with land, air, space, and sea space, cyberspace may soon be considered a state territory.

Keywords: cyberspace, cybernetics, cybersecurity, cyberdiplomacy, cyberdefence, cybersovereignty, cybercrime, state security.

Введение. Вопросы применительно к киберпространству в международном праве в последние годы активно дискуссируются, однако данный вопрос не является новым, он обсуждался несколько раз различными научными деятелями международного права, но был отложен, что называется в дальний ящик ввиду недостаточной осведомлённости и существования других, более насущных и актуальных вопросов, требующих реагирования.

Доказательством того, что киберпреступность не является новшеством, свидетельствует тот факт, что первая кибератака произошла в 1834 году, когда пара воров взломала французскую телеграфную систему, чтобы украсть деньги [13].Полтора века спустя, в 1988 году, Роберт Таппан Моррис организовал первую атаку типа «отказ в обслуживании», взломав компьютер в Массачусетском технологическом институте (MIT) и запустив «червя» в сеть MIT. В течение 24 часов он распространился на 6000 из примерно 60 000 компьютеров, которые, как считалось, были подключены к Интернету в то время [14].

В то время как кибертехнологии развивались в конце 1980-х и начале 1990-х годов, киберпространство стало средой бизнеса и областью военных действий в начале 2000-х годов, когда широкополосный доступ в Интернет стал мейнстримом. Широкополосный доступ позволил быстро передавать большие объемы данных и привёл к технологическому прогрессу предприятий и правительств. Повсеместность широкополосного доступа, рост Интернет сетей и распространение смартфонов — все это передало компьютерные технологии в руки предприятий и людей по всему миру. Как и в случае с другими технологическими достижениями на протяжении всей истории, законы и политика, регулирующие киберпространство, значительно отстают от технологий.

Методы исследования. В ходе исследования были использованы следующие научные методы исследования: метод логического анализа, метод сравнительно-правового анализа, метод законодательного анализа, а также метод научного прогноза. Благодаря этим методам удалось раскрыть содержание избранной темы.

Обсуждение. Сегодня мы говорим о киберпространстве в международном праве уже на серьёзном уровне. Но главным вопросом без ответа были — и в значительной степени остаются — степень, сфера действия и способ применения международного права к киберпространству и, в частности, к кибердеятельности государственных субъектов.

Хотя за последнее время и был достигнут прогресс в понимании того, как международное право применяется к деятельности государств в киберпространстве, сохраняется значительная двусмысленность. Существует множество причин, по которым двусмысленность так распространена. Государства могут не желать формулировать конкретные позиции, поскольку они обеспокоены тем, что установление четких позиций может ограничить их собственную свободу действий, или потому что они могли официально не принять национальную позицию по конкретному вопросу. Кроме того, государства часто намеренно скрывают свою кибердеятельность, усложняя определение того, предприняло ли государство действие или воздержалось от него из чувства правового обязательства или из-за интересов своей национальной безопасности.

Киберпространство является продуктом человеческой творческой деятельности, и не обусловлено естественным порядком вещей подобно естественно-природным видам пространств международного права (сухопутное, морское, космическое, недра). В международной научной литературе киберпространство почти всегда ассоциируется с сетью Интернет, что является большим заблуждением, причиной которого является отсутствие единого определения понятия киберпространства. Согласно мнению западного эксперта Ф.Д. Крамера, в западной научной литературе насчитывается около 28 определений понятия киберпространства [10]. Ряд французских научных деятелей предполагают, что киберпространство – ни что иное, как социально-техническая реальность, глубоко сопряженная с политическим контекстом. Весьма интересным является мнение Добринской Д.Е. которая утверждает, что киберпространство это продукт функционирования любых информационно-коммуникационных технологий, включая и интернет) [11].

Исследовательской службой Конгресса США было выдвинуто определение понятия киберпространства как всеохватывающего множества связей между людьми, созданного на базе компьютеров и телекоммуникаций вне зависимости от физического и географического положения. Кроме того, Минобороны США полагает, что киберпространство – это область, в которой применяются различные РЭС (связи, радиолокации, разведки, навигации, автоматизации, управления и наведения) для приёма, передачи, обработки, хранения, трансформации информации и связанная с ними информационная инфраструктура ВС.

Киберпространство представляет собой сочетание компьютеров, мобильных устройств и пользователей, вступающих между собой во взаимодействие виртуально, на расстоянии. Интернет, в свою очередь,

используется только для подключения данных компьютеров и мобильных устройств. Таким образом, киберпространство шире сети интернет, а интернет находится в киберпространстве. В условиях современности киберпространство выступает основным каналом распространения и хранения информации. [4]

При обсуждении вопроса о киберпространстве всплывает один из главных вопросов – вопрос о правовом регулировании киберпространства. В течение долгого времени в научных кругах идёт дискуссия касательно вопроса о том, возможно ли применить действующие международно-правовые нормы к киберпространству или же необходимо выработать абсолютно новые правила регулирования этой области отношений. Грязнов А.С. в своей статье выделяет идеи о регулировании киберпространства. [3] Так, существуют киберлибертарианцы, считающие, что киберпространство не должно быть под юрисдикцией государства и должно оставаться свободным. Существуют также институционалисты, считающие, что необходимо сформировать национальное и международное законодательство в целях правового регулирования киберпространства. Мы больше склоняемся ко второй идее, ведь действительно, если не начать правовое регулирование данного вопроса, он будет расти в масштабах и нести нарастающую угрозу международной безопасности.

Результаты. Если провести краткий обзор, то можно предположить, что к киберпространству могут быть применимы такие принципы международного права, как уважение прав и основных свобод человека, неприменение силы и угрозы силой, невмешательство во внутренние дела государств, принцип сотрудничества государств, суверенное равенство государств. Однако в виду того, что киберпространство имеет определенную специфику, которая обусловлена её виртуальностью глобального информационного пространства, как объекта права, в котором расстояние не имеет значения, общепризнанные принципы и нормы международного права не могут применяться к киберпространству методом простой экстраполяции понятий.

18 сентября 2012 года Гарольд Кох, юридический советник Государственного департамента США, выступил с речью на юридической конференции Киберкомандования США. Это был первый случай, когда Соединенные Штаты официально заявили позицию о том, что нынешнее международное право применяется в киберпространстве. Хотя сегодня это заявление кажется бесспорным, в то время оно стало прорывом. И сегодня мы являемся свидетелями того, что эта позиция принята большинством международного сообщества.

Далее, Группа правительственных экспертов ООН 2012 года (далее ГПЭ 2012), состоящая из представителей 15 государств, повторила вывод США о том, что международное право, и в частности Устав ООН, применяется к деятельности государств в киберпространстве. Также ГПЭ 2012 года пришла к выводу, что государственный суверенитет и международные нормы и принципы, вытекающие из суверенитета, применяются к поведению государств

в киберпространстве. И что государство имеет юрисдикцию над киберинфраструктурой, расположенной на его территории. Далее было сказано, что государства должны выполнять свои международные обязательства в отношении международно-противоправных деяний, приписываемых им.

В докладе ГПЭ 2012 года суверенитет также был определен как основа, на которой строятся права и обязанности государств в отношении кибероперaций, но ГПЭ не определила, каким именно образом суверенитет обязывает государства предпринимать или не предпринимать определенные действия. После заявлений ГПЭ 2012 года было достигнуто некоторое согласие о том, что международное право применяется в киберпространстве, но точный способ его применения оставался в значительной степени неопределенным.

Мировое сообщество особенно засуетилось после событий 2020 года, когда в Америке произошла масштабная кибератака на государственные IT-системы. Эта кибератака оценивается как крупнейшая в США, которая предоставила свободный доступ хакерам завладеть секретными и рабочими документами государственных органов, а также конфиденциальными документами нескольких американских и мировых компаний. Именно после этого события масштаб важности кибербезопасности существенно возрос в масштабах и заставил воспринимать этот вопрос крайне серьёзно. [1] Недавно США снова подверглись кибератаке. Так, в мае 2021 года Colonial Pipeline, оператор крупнейшего трубопровода в США была подвержена кибератаке хакерами. Трубопровод, обеспечивающий поступление порядка 45% топлива, которое потребляется восточным побережьем штатов был временно перекрыт из-за кибератаки. Тогда Федеральное бюро расследований США обвинило в кибератаке преступную группировку DarkSide. [1]

В рамках исследуемого вопроса необходимо указать Таллиннское руководство по международному праву, применимому к кибернетическим войнам, опубликованным в 2013 г. которое содержит 95 правил, которые, по мнению экспертов, отражают существующее конвенционное или обычное международное право и описывают, как эти правовые режимы применяются к действиям государств в кибервойне. Хотя эта основополагающая работа предоставляет выдающуюся основу, для практиков важно отметить, как и само Руководство, что работа представляет собой собрание взглядов отдельных лиц, действующих в своих личных качествах, и не обязательно отражает позицию НАТО, какой-либо организации или какого-либо государства. Тем не менее, Таллиннское руководство представляет собой прекрасную отправную точку, с которой можно начать понимать, как международное право применяется в киберпространстве.

Согласно Таллинскому руководству киберпространство ничем не отличается от иных областей отношений и не требует специальных подходов к его правовому регулированию, а основные принципы международного права, международного гуманитарного права применимы к действиям в киберпространстве. Например, термин «оружие» применим к

кибертехнологиям, а крупномасштабные кибератаки могут считаться вооруженным нападением по смыслу ст. 51 Устава ООН.

Через три года после Таллиннского руководства ГПЭ в 2015 г. подтвердила многие выводы ГПЭ 2012 г., включая применение Устава ООН к деятельности государств в киберпространстве, а также юрисдикцию государств над инфраструктурой киберпространства на их территории и ограничение использования государствами прокси-серверов для совершения международно-противоправных деяний. В докладе ГПЭ 2015 г. также признано неотъемлемое право государств действовать в соответствии со своими обязательствами по Уставу ООН, и была высказана позиция, что государственный суверенитет и соответствующие ему нормы и принципы применяются к киберпространству.

В докладе 2015 года далее говорилось, что установленные правовые принципы, регулирующие вооруженный конфликт, — гуманность, необходимость, пропорциональность и различие — применяются к действиям государств в киберпространстве, но не подробно описывалось применение этих принципов к кибердеятельности. Самое главное, ГПЭ 2015 года признала, что общее понимание того, «как международное право применяется к использованию государством киберпространства, важно для содействия открытой, безопасной, стабильной, доступной и мирной киберсреде.

В 2017 году НАТО созвал большую группу экспертов, которая выпустила второе Таллинское руководство по международному праву, применимому к кибероперациям). Оно содержит 154 правила и, что самое важное, расширяет сферу своего анализа, включая деятельность государств в киберпространстве в мирное время. Таллинское руководство №2 также рассматривает пересекающиеся правовые режимы (например, государственные кибероперации и Конвенция ООН по морскому праву). Как и Таллинское руководство №1, №2.0 отражает взгляды отдельных лиц, а не обязательно взгляды государств, хотя некоторые государства выразили свое согласие с позицией Руководства по суверенитету.

Существует два взгляда на суверенитет. Первый, как правило, заключается в том, что суверенитет является нормой международного права, а нарушение суверенитета государства равносильно нарушению международного обязательства. Это точка зрения Таллиннского руководства №2. Вторая точка зрения заключается в том, что суверенитет — это правовой принцип, отраженный в международном праве, но сам по себе не являющийся правилом. Согласно этой точке зрения, чтобы найти нарушение международного обязательства, нужно сначала найти принцип суверенитета, реализованный в международном праве. Продолжаются дебаты о суверенитете как правиле или принципе, которые имеют последствия для государственных кибероперaций и международных отношений.

В мировой практике в последнее время встречаются случаи, когда представители государственных органонов на различных мероприятиях выражали мнения по вопросам киберпространства. Наиболее весомое и

официальное мнение может быть выражено главой государства, к примеру, в 2019 г. президент Эстонии Керсти Кальюлайд выступила на Международной конференции по киберконфликтам, или CyCon, и представила точку зрения Эстонии на применение международного права в киберпространстве.

Кальюлайд признала, что международное право применяется в киберпространстве и что государства несут юридическую ответственность за свою кибердеятельность. Она также изложила точку зрения Эстонии о том, что государства обязаны укреплять свою устойчивость к киберугрозам. Она заявила, что государства имеют право «приписывать» кибероперации в соответствии с международным правом, что государства имеют право реагировать на вредоносные кибероперации; и что государства могут применять контрмеры, включая коллективные контрмеры, и ссылаться на неотъемлемое право на самооборону. Ссылаясь на право на самооборону, Кальюлайд молчаливо признала, что кибероперации могут при некоторых обстоятельствах быть равносильны применению силы или вооруженному нападению. Стоит отметить, что предполагаемая доктрина коллективных контрмер получила мало внимания в обсуждениях того, как международное право применяется в киберпространстве, и речь Кальюлайд, возможно, была первым случаем, когда государство заняло позицию по этому вопросу.

Важным международно-правовым регулятором является, разумеется Устав ООН, который в п.4 ст 2 гласит: «Все Члены Организации Объединенных Наций воздерживаются в их международных отношениях от угрозы силой или её применения как против территориальной неприкосновенности или политической независимости любого государства, так и каким-либо другим образом, несовместимым с Целями Объединенных Наций». Здесь формулировка «так и каким-либо другим образом» даёт некую свободу усмотрения и вполне позволяет включить и киберпространство.

На сегодняшний день, основным международно-правовым актом, касающимся деятельности в кибепространстве, а именно преступной деятельности в сфере информационных технологий, является Конвенция о преступности в сфере компьютерной информации, принятая 23 ноября 2001 г. в Будапеште. Данная конвенция является самым первым международным договором о преступлениях, совершенных через Интернет и другие компьютерные сети, и касается, в частности, нарушений авторских прав, компьютерных мошенничеств, детской порнографии и нарушений безопасности сети. Она также содержит ряд полномочий и процедур, таких как обыск компьютерных сетей и перехват.

Она подчёркивает необходимость проведения в приоритетном порядке общей политики в области уголовного права, нацеленной на защиту общества от компьютерных преступлений, в том числе путём принятия соответствующих законодательных актов и укрепления международного сотрудничества. Конвенция содержит довольно широкую категорию преступлений в киберпространстве, начиная от противозаконного доступа и перехвата

информационных данных, заканчивая мошенничеством с использованием компьютерных технологий и правонарушений, связанных с детской порнографией. [12]

Важно упомянуть также Дополнительный протокол к Конвенции о преступлениях в сфере компьютерной информации, об инкриминировании расистских актов и совершенного ксенофоба при помощи информационных систем, который был принят в Страсбурге в 2003 г. Согласно ст.3 Доппротокола государства-участницы принимают такие законодательные и иные меры, которые могут потребоваться для того, чтобы квалифицировать в качестве уголовных преступлений в соответствии с её национальным правом, когда это сделано умышленно и противоправно, такое поведение как распространение расистского и ксенофобского материала или обеспечение доступа к нему для общественности через компьютерные системы.

Также, государства принимают все законодательные и другие необходимые меры, которые могут потребоваться для того, чтобы квалифицировать в качестве уголовных преступлений в соответствии с ее национальным правом, когда это сделано умышленно и противоправно, такое поведение, как угроза через компьютерную систему совершения серьезного уголовного преступления, как определено ее внутренним правом, в отношении лиц по причине того, что они принадлежат к группе, отличной по расе, цвету кожи, национальному или этническому происхождению, а также религии, или группы лиц с учетом этих факторов.

Аналогично квалифицируются в качестве уголовных преступлений публичные оскорбления через компьютерную систему лиц по причине того, что они принадлежат к группе, отличной по расе, цвету кожи, национальному или этническому происхождению, а также религии, или группы лиц с учетом этих факторов. Стоит отметить, что именно эта тенденция сейчас обретает популярность. Ввиду того, что общество сегодня является довольно виртуальным и общение людей в основном происходит на различных социальных площадках и мессенджерах, нередки случаи подачи жалоб и обращений в суд по причине так скажем «онлайн-оскорблений».

Ещё одной проблемой в вопросе отнесения киберпространства к международному праву является вопрос о юрисдикции. Как небезызвестно, субъектами международного права выступают государства. В то время как субъектами в киберпространстве могут быть как государства, частные физические лица, различного рода интернет компании, предприятия и иные образования, имеющие свои интересы. Вопрос усложняется ещё и тем, что эти субъекты могут действовать анонимно, что затруднит или же и вовсе сделает невозможным процесс их выслеживания. В этой связи достаточно сложно упорядочить категорию субъектов и выяснить, какие субъекты права легитимны и попадают под действие международного права о киберпространстве, а какие вопросы всё же следует урегулировать. [4]

Нами предлагается, для начала провести работу над созданием определённого нормативного международного правового акта, способного определить понятие киберпространства и способного включать и регулировать следующие вопросы:

a) Вопрос о субъектах и их деятельности в киберпространстве. Здесь необходимо конкретно определить круг субъектов, регулирование их деятельности в киберпространстве, определить действия, относящиеся или не относящиеся к киберугрозе и кибератаке;

b) Киберсуверенитет. Сложности международного права о киберпространстве связаны и с тенденцией к продвижению кибер суверенитета. В первую очередь следует начать с признания киберпространства одним из пространств, на которое государство распространяет свой суверенитет. Кибер суверенитет представляет идею контроля и управления информацией, доступом, коммуникациями, сетями и инфраструктурой в киберпространстве непосредственно, без внешнего вмешательства. Сегодня эта идея популяризируется благодаря таким историческим кейсам и обстоятельствам в киберпространстве как:

- кибераль янс Китая и России по вопросам цифрового суверенитета,
- дела Сноудена и Wikileaks и рост GAFA (Google-Apple-Facebook-Amazon). [4], [6],[7].

c) Вопрос о кибербезопасности. Государства в настоящее время не обладают достаточно прочным щитом, обеспечивающим защиту от кибератак, кибертерроризма и иных преступлений в киберпространстве. Государствам необходимо выстроить надёжный механизм киберзащиты. ООН неоднократно призывает государства осветить тему кибербезопасности и кибертерроризма. Особенную озабоченность вызывает противоправное использование террористами информационно-коммуникационных технологий, то есть Интернет-сеть и цифровых технологий, для вербовки в целях планирования, подстрекательства к совершению, непосредственного совершения и финансирования террористических актов. Подчёркивалась важность многостороннего сотрудничества в борьбе с данной угрозой, в том числе между государствами-членами, международными, региональными и субрегиональными организациями, частным сектором, а также гражданским обществом.

В рамках ООН 15 июня 2017 г. резолюцией 71/291 Генеральной Ассамблеи Организации Объединенных Наций было создано Контртеррористическое управление, которое осуществляет инициативы в осфере новых информационных технологий, в том числе и проект по использованию социальных сетей для сбора информации из открытых источников и цифровых доказательств в целях борьбы с терроризмом и насильственным экстремизмом при соблюдении прав человека.

d) В рамках Контртеррористического управления была разработана Программа по кибербезопасности и использованию новых технологий

направленная на укрепление потенциала государств-членов и частных организаций по предотвращению кибератак террористов на важнейшие объекты инфраструктуры. Программа также направлена на смягчение последствий кибератак на отдельные системы ввиду неправомерного использования технических достижений и их восстановление после кибератак. Она предусматривает противодействие угрозе кибератак, осуществляемых террористическими организациями на критически важную инфраструктуру, а также поощрение использования социальных сетей для сбора информации из открытых источников и цифровых доказательств в целях противодействия онлайновому терроризму и насильственному экстремизму при соблюдении прав человека.

e) Кибердипломатия. Установление сотрудничества государств применительно в киберпространстве. Обмен опыта государствами, проведение конференций и иных научных мероприятий в целях обсуждения плана действий по выстраиванию дипломатических правоотношений;

f) Киберарбитраж. Создание механизма по урегулированию споров, либо отнесение рассмотения киберспоров к уже существующим судебным инстанциям. Следует отметить, что арбитраж касаемо некоторых действий в киберпространстве имеет место, однако он связан с торговлей и преступностью и существует только в национально-правовой системе, а не в международно-правовой. К примеру, арбитражный суд в Гааге обладает потенциалом для рассмотрения в качестве стороны вынесения судебного решения по киберпространству, поскольку он уже имеет полномочия по рассмотрению дел, связанных с энергетикой, космосом, а также окружающей средой. Но требуется полноценное одобрение со стороны государственных субъектов, для того, чтобы выдвигать подобные полномочия, а также наличие органов власти по делам в киберпространстве.

Результаты. Резюмируя всё вышеизложенное, мы может подытожить, что вопрос о киберпространстве хоть и является сейчас одним из актуальнейших, однако он требует длительной обработки и решения обозначенных вопросов, при определении и урегулировании которых можно говорить о самостоятельности киберпространтсва в международном праве. Однако государства не пришли к согласию относительно данных вопросов, что буксирует процесс международной легитимизации киберпространства. Мировое сообщество должно отнестись к этому вопросу достаточно серьёзно в целях предотвращения необратимых потенциальных киберугроз. Мы должны как можно скорее объединить наши усилия с тем, чтобы уменьшить эту угрозу и обеспечить, чтобы новые технологии и впредь оставались силой добра, а не зла.[8]

Список литературы

1. Ведомости. URL: https://www.vedomosti.ru/technology/articles/2017/09/08/732945-ssha-utechka-dannih (дата обращения 15.03.2024)

2. The wall street journal. URL: https://www.wsj.com/articles/fbi-suspects-criminal-group-with-ties-to-eastern-europe-in-pipeline-hack-11620664720 (дата обращения 16.03.2024)

3. Грязнов С.А. Международное правовое регулирование киберпространства // Международный журнал гуманитарных и естественных наук. 2021. №1-3. URL: https://cyberleninka.ru/article/n/mezhdunarodnoe-pravovoe-regulirovanie-kiberprostranstva (дата обращения: 16.03.2024).

4. Данельян А.А. Международно-правовое регулирование киберпространства // Образование и право. 2020.

5. Российский совет по международным делам. Практика цифрового суверенитета в России и КНР. URL: https://russiancouncil.ru/analytics-and-comments/analytics/praktika-tsifrovogo-suvereniteta-v-rossii-i-knr/ (дата обращения 18.03.2024)

6. Дело Эдварда Сноудена. URL: https://tass.ru/spravochnaya-informaciya/627583 (дата обращения 18.03.2024)

7. История судебного преследования Джулиана Ассанжа. URL: https://tass.ru/info/13166619 (дата обращения 20.03.2024)

8. Из речи заместителя Генерального секретаря и главы Контртеррористического управления ООН Владимира Воронкова на параллельном мероприятии по теме «Использование новых и новейших технологий в борьбе с терроризмом» URL: https://www.un.org/counterterrorism/ru/cybersecurity (дата обращения 20.03.2024)

9. Официальный сайт Контртеррористического управления ООН. URL: https://www.un.org/counterterrorism/ru/cct/programme-projects/cybersecurity (дата обращения 21.03.2024)

10. Остроушко А.В., Букалерова Л.А., Шагиева Р. В..Совершенствование понятийного аппарата, связанного с правовым регулированием киберпространства // Евразийская адвокатура. 2023. №3 (62). URL: https://cyberleninka.ru/article/n/sovershenstvovanie-ponyatiynogo-apparata-svyazannogo-s-pravovym-regulirovaniem-kiberprostranstva (дата обращения: 22.03.2024).

11. Добринская Д.Е. Киберпространство: территория современной жизни // Вестник Московского университета. Серия 18. Социология и политология. 2018. №1. URL: https://cyberleninka.ru/article/n/kiberprostranstvo-territoriya-sovremennoy-zhizni (дата обращения: 24.03.2024).

12. Конвенция о преступности в сфере компьютерной информации, 23 ноября 2001 г. Серии европейских договоров - № 185. URL: https://rm.coe.int/1680081580 (дата обращения: 25.03.2024).

13. Том Стэндедж и Сет Стивенсон, Human Insecurity, Slate, 3 октября 2018 г.

14. Федеральное бюро расследований, The Morris Worm, 2 ноября 2018 г.

References

1. Vedomosti. URL: https://www.vedomosti.ru/technology/articles/2017/09/08/732945-ssha-utechka-dannih (data obrashcheniya 15.03.2024)

2. The wall street journal. URL: https://www.wsj.com/articles/fbi-suspects-criminal-group-with-ties-to-eastern-europe-in-pipeline-hack-11620664720 (data obrashcheniya 16.03.2024)

3. Gryaznov S.A. Mezhdunarodnoe pravovoe regulirovanie kiberprostranstva // Mezhdunarodnyj zhurnal gumanitarnyh i estestvennyh nauk. 2021. №1-3. URL: https://cyberleninka.ru/article/n/mezhdunarodnoe-pravovoe-regulirovanie-kiberprostranstva (data obrashcheniya: 16.03.2024).

4. Danel'yan A.A. Mezhdunarodno-pravovoe regulirovanie kiberprostranstva // Obrazovanie i pravo. 2020.

5. Rossijskij sovet po mezhdunarodnym delam. Praktika cifrovogo suvereniteta v Rossii i KNR. URL: https://russiancouncil.ru/analytics-and-comments/analytics/praktika-tsifrovogo-suvereniteta-v-rossii-i-knr/ (data obrashcheniya 18.03.2024)

6. Delo Edvarda Snoudena. URL: https://tass.ru/spravochnaya-informaciya/627583 (data obrashcheniya 18.03.2024)

7. Istoriya sudebnogo presledovaniya Dzhuliana Assanzha. URL: https://tass.ru/info/13166619 (data obrashcheniya 20.03.2024)

8. Iz rechi zamestitelya General'nogo sekretarya i glavy Kontrterroristicheskogo upravleniya OON Vladimira Voronkova na parallel'nom meropriyatii po teme «Ispol'zovanie novyh i novejshih tekhnologij v bor'be s terrorizmom» URL: https://www.un.org/counterterrorism/ru/cybersecurity (data obrashcheniya 20.03.2024)

9. Oficial'nyj sajt Kontrterroristicheskogo upravleniya OON. URL: https://www.un.org/counterterrorism/ru/cct/programme-projects/cybersecurity (data obrashcheniya 21.03.2024)

10. Ostroushko A.V., Bukalerova L.A., SHagieva R.V. Sovershenstvovanie ponyatijnogo apparata, svyazannogo s pravovym regulirovaniem kiberprostranstva // Evrazijskaya advokatura. 2023. №3 (62). URL: https://cyberleninka.ru/article/n/sovershenstvovanie-ponyatiynogo-apparata-svyazannogo-s-pravovym-regulirovaniem-kiberprostranstva (data obrashcheniya: 22.03.2024).

11. Dobrinskaya D.E. Kiberprostranstvo: territoriya sovremennoj zhizni // Vestnik Moskovskogo universiteta. Seriya 18. Sociologiya i politologiya. 2018. №1. URL: https://cyberleninka.ru/article/n/kiberprostranstvo-territoriya-sovremennoy-zhizni (data obrashcheniya: 24.03.2024).

12. Konvenciya o prestupnosti v sfere komp'yuternoj informacii, 23 noyabrya 2001 g. Serii evropejskih dogovorov - № 185. URL: https://rm.coe.int/1680081580 (data obrashcheniya: 25.03.2024).

13. Tom Stendedzh i Set Stivenson, Human Insecurity, Slate, 3 oktyabrya 2018 g.

14. Federal'noe byuro rassledovanij, The Morris Worm, 2 noyabrya 2018 g.