DOI: 10.17803/1994-1471.2020.110.1.133-141

Н. А. Молчанов*,
Е. К. Матевосова**

Концептуально-политический и формально-юридический анализ Парижского призыва к доверию и безопасности в киберпространстве и российские инициативы в области международного права

Аннотация. Состояние международной безопасности в современном мире напрямую зависит от защищенности киберпространства. Авторы статьи исследуют инициативы по обеспечению кибербезопасности, рассматривая их наиболее значимые юридические и политические аспекты. Статья содержит научно-экспертную оценку документа, принятого 12 ноября 2018 г., — Парижского призыва к доверию и безопасности в киберпространстве. Учитывая, что Россия является лидером по инициативам в международных форматах обсуждения проблем кибербезопасности, авторы статьи обращаются к российской позиции по ряду ключевых вопросов в рамках данной проблематики, указывая на то, что предложения российской стороны опережают, в частности по своему регулятивному потенциалу, многие другие международные инициативы. Авторы формулируют вывод о том, что меры укрепления доверия между государствами в отсутствии обязательных международно-правовых норм лишены инструментальной роли в разрешении многих проблем обеспечения безопасности в стремительно изменяющемся киберпространстве. Условием эффективного международного правотворчества в области информационной безопасности является диалог юристов, политиков и технических специалистов.

Ключевые слова: международная безопасность; информационная безопасность; кибербезопасность; киберпространство; киберпреступность; международное право; Парижский призыв; российские инициативы; меры доверия; информатизация общества.

* *Молчанов Николай Андреевич*, доктор военных наук, профессор кафедры интеграционного и европейского права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА), заслуженный деятель науки РФ
Садовая-Кудринская ул., д. 9, каб. 543, г. Москва, Россия, 125993
namolchanov@msal.ru

** *Матевосова Елена Константиновна*, кандидат юридических наук, доцент кафедры теории государства и права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)
Садовая-Кудринская ул., д. 9, каб. 455, г. Москва, Россия, 125993
ekmatevosova@msal.ru

Для цитирования: *Молчанов Н. А., Матевосова Е. К.* Концептуально-политический и формально-юридический анализ Парижского призыва к доверию и безопасности в киберпространстве и российские инициативы в области международного права // Актуальные проблемы российского права. — 2020. — Т. 15. — № 1. — С. 133—141. — DOI: 10.17803/1994-1471.2020.110.1.133-141.

Conceptual Political and Formal Legal Analysis of the Paris Call for Trust and Security in Cyberspace and Russian Initiatives in the Field of International Law

Nikolay A. Molchanov, Dr. Sci. (Military Sciences), Professor of the Department of Integration and European Law at Kutafin Moscow State Law University (MSAL), Honored Scientist of the Russian Federation
ul. Sadovaya-Kudrinskaya, d. 9, Moscow, Russia, 125993
namolchanov@msal.ru

Elena K. Matevosova, Cand. Sci. (Law), Associate Professor of the Department of Theory of State and Law at Kutafin Moscow State Law University (MSAL)
ul. Sadovaya-Kudrinskaya, d. 9, Moscow, Russia, 125993
ekmatevosova@msal.ru

Abstract. The state of international security in the modern world directly depends on the security of cyberspace. The authors of the paper explore cybersecurity initiatives, considering their most significant legal and political aspects. The paper contains a scientific and expert assessment of the document adopted on November 12, 2018 — the Paris Call for Trust and Security in Cyberspace. Given that Russia leads in initiatives in international formats for discussing cybersecurity issues, the authors of the paper turn to the Russian position on a number of key issues within this framework, indicating that the proposals of the Russian side are ahead of many other international initiatives, in particular in terms of their regulatory potential.
The authors conclude that confidence-building measures between states in the absence of binding international legal norms are deprived of an instrumental role in resolving many security problems in rapidly changing cyberspace. A prerequisite for effective international law-making in the field of information security is a dialogue between lawyers, politicians and technical experts.
Keywords: international security; information security; cybersecurity; cyberspace; cybercrime; international law; Paris call; Russian initiatives; confidence building measures; informatization of society.
Cite as: Molchanov NA, Matevosova EK. Kontseptualno-politicheskiy i formalno-yuridicheskiy analiz parizhskogo prizyva k doveriyu i bezopasnosti v kiberprostranstve i rossiyskie initsiativy v oblasti mezhdunarodnogo prava [Conceptual political and formal legal analysis of the Paris Call for Trust and Security in Cyberspace and Russian initiatives in the field of international law]. *Aktualnye problemy rossiyskogo prava*. 2020;15(1):133-141. DOI: 10.17803/1994-1471.2020.110.1.133-141.

Формирование единой нормативно непротиворечивой и практически функциональной глобальной системы обеспечения информационной безопасности остается в ряду наиболее важных проблем международной повестки дня.

В наши кризисные времена снижения авторитета международного права все чаще раздаются призывы к сохранению мира и безопасности. Международное сообщество, исчерпав правовые средства, призывает к международной морали, но зов международного разума лишь далеким эхом слышен тем государствам, которые, произвольно освобождая себя от юридических обязательств, намеренно разрушают международное право.

12 ноября 2018 г. на XIII Форуме по управлению Интернетом, проведенном в штаб-квартире

ЮНЕСКО в Париже (в рамках Парижской цифровой недели, включающей также мероприятия, посвященные новым технологиям и цифровой трансформации государств и демократий), Президент Франции Э. Макрон выступил с Парижским призывом к доверию и безопасности в киберпространстве[1] (фр. яз.: Appel de Paris pour la confiance et la sécurité dans le cyberspace). Документ был поддержан 58 странами, 115 международными и региональными организациями, 284 частными компаниями и корпорациями[2].

Формально-юридический и концептуально-политический анализ Парижского призыва предполагает прежде всего определение его документального статуса и, соответственно, правовой силы. Современной международной нормотворческой практике известны различные по названию, закреплению и содержанию документы как императивного, так и рекомендательного характера. Вариации согласования воли договаривающихся государств и иных субъектов международного общения зависят от многих условий и факторов, обусловленных как сущностью самой разрешаемой проблемы, так и некими внешними очевидными и скрытыми детерминантами. К примеру, международная конференция (в значении обобщающего термина), которая, согласно устоявшемуся в праве международных договоров подходу, является временным органом, создаваемым участвующими государствами, призванным обсуждать поставленные перед ним вопросы и принимать согласованные решения, может обратиться ко всем участникам этой (и даже другой) «конференции» (и «совещания», и «конвенции», и т.д.) с призывом рассмотреть возможность сделать то или иное заявление на национальном уровне. Представляется, что рассуждения о том, является ли Парижский призыв собственно призывом, или обращением, или заявлением, или каким-либо иным синонимичным воззванием из терминологического аппарата русского языка (с учетом перевода с французского и лексикографии современной дипломатии), никак не предопределяют правового характера данного призыва, поскольку очевидна его исключительно декларативная роль в отсутствие каких-либо прямых и обеспеченных юридических обязательств государств, частных компаний и общественных организаций, добровольно призыв подписавших[3]. Принимая во внимание репрезентативный состав участников и круг обсуждаемых вопросов, оформленных в итоговый «призывный» документ, Парижский форум, имея высокое политическое значение, претендовал на то, чтобы перевернуть страницу в многолетней дискуссии о международной кибербезопасности, однако ни юридически, ни организационно данный форум совершить этот прорыв пока не в состоянии.

В настоящее время политическая ответственность государств в киберпространстве в отсутствие императивных международных норм базируется прежде всего на морали. Международная мораль есть система норм, оценок, предписаний, образцов поведения, выполняющих функции морального регулирования в системе международных отношений, в формировании ценностей культуры мира, в становлении демократического и ненасильственного мироустройства[4]. Парижский призыв к сотрудничеству, взаимной поддержке, справедливости, уважению, свободе, в сущности, выражает основы системы международной морали.

Глашатаи нового киберпорядка призывают сделать киберпространство более надежным, безопасным и стабильным, открытым, доступным и мирным.

Парижский призыв подтверждает, что международное право — вместе с добровольными

[1] См.: официальный сайт Постоянного представительства Франции в Европейском Союзе. URL: https://ue.delegfrance.org (дата обращения: 30.06.2019).

[2] Российская Федерация не является подписантом Парижского призыва.

[3] См. полный список сторон-участников, подписавших Парижский призыв к доверию и безопасности в киберпространстве: URL: https://ue.delegfrance.org (дата обращения: 30.06.2019).

[4] См.: *Капто А. С.* Современная цивилизация: вызовы и альтернативы. М. : Издательство Московского университета, 2013. С. 137.

нормами ответственного поведения государств в мирное время и мерами по развитию доверия и укреплению потенциала, разработанными в рамках Организации Объединенных Наций, — составляет фундамент международного мира и безопасности в киберпространстве.

В Призыве утверждается (и его участниками подтверждается), что международное право, в том числе весь Устав ООН, международное гуманитарное право и международное обычное право применимы к использованию государствами информационно-коммуникационных технологий.

Устав ООН, подписанный 26 июня 1945 г. в г. Сан-Франциско по завершении Конференции ООН по созданию международной организации (и вступивший в силу 24 октября 1945 г.), является так называемой конституцией мирового сообщества. Однако конституирующие мировой порядок положения Устава ООН как международного договора особого рода, будучи в целом применимы к разрешению любой международной проблемы, не отвечают на многие вопросы обеспечения международной информационной безопасности, которые, надо признать, возникли перед стремящимся к всеобщему миру человечеству гораздо позднее принятия данного Устава, а потому ссылка на него есть некий «протокольный» подход «механического» перечисления основных источников современного международного права.

В российской и зарубежной доктрине и практике международных отношений «международное гуманитарное право» (или «право вооруженных конфликтов»), как правило, консенсуально определяется как свод обычных и договорных норм, применяемых в период вооруженных конфликтов[5]. До настоящего времени юридически не зафиксирован ни один факт злонамеренного использования информационно-коммуникационных технологий, произошедших в период вооруженного конфликта, а тем более ведения так называемой информационной войны[6] (не в публицистическом, а нормативном научно-экспертном значении). На международных дискуссионных площадках многие годы нет единства мнений о необходимости легализации «информационной войны» («кибервойны»), принятия правил ее ведения. А признание потенциального применения международного гуманитарного права (с учетом существующих проблем его действия[7]) к соответствующим вооруженным конфликтам требует интенсификации международного правотворчества по дополнению гуманитарного права нормами, непосредственно связанными с использованием цифровых технологий.

Выявление норм обычного международного права — сложнейшая задача юридико-политического исследования. Как установила Комиссия международного права ООН, для определения существования и содержания нормы обычного международного права необходимо выявить, имеется ли всеобщая практика, признанная в качестве правовой нормы (opinio juris), при этом уделяя внимание общему контексту, характеру нормы, а также конкретным обстоятельствам, в которых могут быть обнаружены каждые из

---

[5] См.: *Бекяшев К. А.* Международное публичное право : учебник. М., 2019. С. 941.

[6] Информационная война — противоборство между двумя или более государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим структурам, подрыва политической, экономической и социальной систем, массированной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны (см.: Соглашение между Правительствами государств — членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности (вместе с Перечнем основных понятий и видов угроз, их источников и признаков), заключено в г. Екатеринбурге 16.06.2009 // Бюллетень международных договоров. 2012. № 1. С. 13—21).

[7] *Henckaerts J.-M.* Study on customary international humanitarian law: A contribution to the understanding and respect for the rule of law in armed conflict // International Review of the Red Cross. 27.04.2010. Pp. 175—212.

этих свидетельств[8]. Сегодня применимое к отношениям в киберпространстве обычное международное право пока партикулярно, действует только между ограниченным кругом государств, для которых складывается соответствующая практика в силу регионального (локального) сотрудничества.

Парижский призыв называет Конвенцию о преступности в сфере компьютерной информации (так называемая Будапештская конвенция по борьбе с киберпреступностью[9]) важнейшим инструментом улучшения безопасности цифровых продуктов, укрепления защиты от преступников и стимулирования сотрудничества между всеми заинтересованными сторонами. Упоминание Будапештской конвенции вызывает немалое удивление, так как, во-первых, данная Конвенция, заключенная в Будапеште 23 ноября 2001 г., устарела, превратившись в реликвию начала печальной истории киберэры, во-вторых, многие из ее положений, по оценкам специалистов (российских и, что важно отметить, зарубежных), имеют серьезные «пороки», угрожающие национальным интересам государств не в меньшей степени, чем сама киберпреступность. Либо текст указанной Конвенции должен быть существенно изменен, либо должен быть принят новый конвенционный акт с принципиально иными, жизнеспособными положениями. Убеждение мировой общественности в возможном реанимированном действии Будапештской конвенции есть следствие или грубого непрофессионализма, или умышленного введения в заблуждение, однако и то и другое абсолютно недопустимо.

Участники Парижского призыва осуждают злонамеренную кибердеятельность в мирное время, которая угрожает критическим инфраструктурам. При всех усилиях международного сообщества количество компьютерных инцидентов только возрастает, и, бесспорно, нарушение функционирования объекта критической инфраструктуры государства является серьезной угрозой национальной и региональной безопасности. Прекращение работы сетей электросвязи, в частности в 2019 г. в таких странах, как Венесуэла, Аргентина, Бразилия, Уругвай и Парагвай, может быть результатом целенаправленных кибератак. Не предрешая споры экспертов, в том числе юридически квалифицирующих данный инцидент, можно утверждать, что подобные нарушения не получают должной правовой оценки, а само по себе международное осуждение без негативных для виновных сторон последствий не препятствует новым планомерным атакам.

Парижский призыв содержит, можно сказать, «подразумеваемый» (при системном толковании его положений и связи с рядом применимых к киберотношениям международных документов) перечень мер по развитию доверия в киберпространстве. Укрепление доверия представляет собой определенную конструкцию, вырабатываемую на глобальном и региональном уровнях, исходя из соответствующих задач ООН и предметной области решения конкретной проблемы. Следует признать, что текстуальная определенность и оценка эффективности мер укрепления доверия в киберпространстве достигается прежде всего в рамках регионального международного сотрудничества, что подтверждается актами, принимаемыми на мероприятиях международного формата. Так, главы государств и правительств стран — членов Ассоциации государств Юго-Восточной Азии (АСЕАН), собравшиеся по случаю проведения 13-го Восточноазиатского саммита (ВАС) в Сингапуре 15 ноября 2018 г., определили такие совместные меры, признав, что «практические меры по укреплению доверия необходимы для обеспечения стабильности и предсказуемости в киберпространстве»[10]. В этой связи следует

[8] Доклад Комиссии международного права. 70-я сессия Генеральной Ассамблеи ООН (30 апреля — 1 июня и 2 июля — 10 августа 2018 г.) // URL: http://legal.un.org (дата обращения: 30.06.2019).

[9] Конвенция о преступности в сфере компьютерной информации (ETS № 185) (заключена в г. Будапеште 23.11.2001) // Документ опубликован не был. СПС «КонсультантПлюс».

[10] Заявление лидеров стран — участниц Восточноазиатского саммита по углублению сотрудничества в области безопасности использования информационно-коммуникационных технологий и цифровой экономики // Документ опубликован не был. СПС «КонсультантПлюс».

отметить, что, как было провозглашено Резолюцией ООН № 45/62 от 4 декабря 1990 г., укрепление доверия является продолжительным динамичным процессом и существуют различные типы мер укрепления доверия, на характер которых влияют специфические ситуации в конкретных регионах[11]. Соглашаясь с необходимостью «регионального учета»[12] в выработке и реализации мер укрепления доверия в киберпространстве (в том числе на примере Парижского призыва), все-таки полагаем целесообразным согласование и закрепление общих, унифицированных глобальных мер, которые должны «вплетаться» в государственную внутреннюю и внешнюю политику каждого государства.

Результатом работы Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности с 2010 г. является общий вывод о том, что именно добровольные меры укрепления доверия могут способствовать повышению степени доверия и установлению доверительных отношений между государствами[13].

Как отмечает В. А. Садовничий, «принятие норм безопасной деятельности в киберпространстве — императив нашего времени»[14]. И все же главный вопрос состоит в том, какими преимущественно нормами должны быть урегулированы отношения в киберпространстве — политически рекомендательными или юридически обязывающими? Отказ многих государств от бремени любых обязательств ответственного поведения подтверждает приоритет рекомендательных норм, однако их индекс эффективности, несмотря на предпринимаемые нормотворческие усилия, продолжает оставаться низким.

Подписанты Парижского призыва заявляют, что решительно настроены действовать сообща в существующих инстанциях и через соответствующие организации, институты, механизмы и процессы. Как представляется, выступление с Парижским призывом с мировой трибуны и стало необходимым по причине отсутствия таких инстанций и механизмов, а потому подобное заявление не отличается реалистичностью и кажется лишь словесным украшением.

Одной из целей сотрудничества участников Парижского призыва является развитие возможностей по «предотвращению вмешательства со стороны иностранных субъектов, направленного на дестабилизацию избирательных процессов посредством злонамеренной кибердеятельности». Указание на «иностранных субъектов» в призыве, обращенном ко всему миру, имеет, как кажется, весьма неопределенный смысл (можно полагать и отсутствие смысла как такового), но вместе с тем свидетельствует о «злонамеренности» его авторов-вдохновителей, в столь кратком по объему и фрагментарно-усеченном по содержанию призыве позволивших, с учетом конфликтно-кризисных

[11] Резолюция № 45/62 Генеральной Ассамблеи ООН «Рассмотрение осуществления рекомендаций и решений, принятых Генеральной Ассамблеей на ее десятой специальной сессии» (вместе с Декларацией о провозглашении 90-х годов третьим Десятилетием разоружения), принята 04.12.1990 на 54-м пленарном заседании 45-й сессии Генеральной Ассамблеи ООН // Система официальной документации ООН. URL: https://documents.un.org/prod/ods.nsf (дата обращения: 30.06.2019).

[12] См. также: Решение № 1202 Постоянного совета ОБСЕ от 10 марта 2016 г. «Меры укрепления доверия в рамках ОБСЕ с целью сокращения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий» // URL: https://www.osce.org (дата обращения: 30.06.2019).

[13] См.: Резолюция № A/RES/73/266 Генеральной Ассамблеи ООН «Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности», принята 22.12.2018 на 56-м пленарном заседании 73-й сессии Генеральной Ассамблеи ООН // Система официальной документации ООН. URL: https://documents.un.org/prod/ods.nsf (дата обращения: 30.06.2019).

[14] Выступление В. А. Садовничего на V международном форуме «Партнерство государства, бизнеса и гражданского общества при обеспечении информационной безопасности и противодействии терроризму» // URL: http://www.iisi.msu.ru/articles/article28/ (дата обращения: 30.06.2019).

международных реалий, явную политическую ангажированность.

Участники Парижской цифровой недели, призывающие к мировому киберпорядку, договорились встретиться в 2019 г. на Парижском форуме мира и Форуме по управлению Интернетом в Берлине для мониторинга продвижения по обозначенным в Парижском призыве основным вопросам. Не преследуя цели резкой критики этого предложения, заметим, что такое обсуждение будет сведено к новым по форме, но старым по посылу призывам.

В своих оценочных комментариях рассматриваемой французской инициативы Департамент информации и печати МИД России указывает на ряд не только неоспоримо ценных, но и «сомнительных» положений[15]. В частности, «предлагаемый французами мультистейкхолдеровый подход к цифровой среде предусматривает уравнивание в правах государств и негосударственных игроков и тем самым размывает ключевую роль государств в обеспечении кибербезопасности». Слишком большое количество заинтересованных сторон усложняет процесс обсуждения проблем; интересы государств и негосударственных субъектов не могут быть между собой сопоставимы и в полной мере друг с другом сочетаемы. Не следует игнорировать позиции негосударственных акторов киберпространства, но весьма важно избегать любого давления со стороны субъектов, навязывающих свои частные интересы.

Именно Российская Федерация сегодня является инициатором и активным участником международных договоренностей в области глобальной информационной безопасности. Равноправное партнерство стран, независимо от их «цифрового потенциала», признающих необходимость устранения существующих и предупреждения потенциальных угроз в рассматриваемой области, — главное условие достижения реальных положительных результатов, которое отстаивает Россия на протяжении многих лет. Российская сторона предлагает такие модели нормативного решения ряда вопросов в информационной сфере, в особенности киберпространства, которые, во-первых, отличаются универсализмом, без нарушения баланса международных и национальных интересов, а во-вторых, даже во многом опережают свое время, исключая ситуативность выбора нормативных средств, учитывая динамику научного прогресса в разработке и внедрении все более новых информационных технологий.

Примечательно, что, несмотря на усугубляющееся в целом конфликтное состояние международных отношений, в частности политическое обострение отношений России со странами, жестко диктующими собственные правила игры с заранее известными итогами, российские проектно-нормативные инициативы все же получают международную поддержку, поскольку, как представляется, «законы большой политики» отступают перед «законами разума и всеобщности», подкрепленными международной моралью, формальное отрицание которой неспособно поставить под сомнение ее фактическое существование.

5 декабря 2018 г. ознаменовано принятием Генеральной Ассамблеей ООН российского проекта резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»[16], содержащего ряд новаций в подходах к обеспечению ответственного поведения государств в информационном пространстве. Особо следует отметить, что с 2019 г. в целях придания переговорному процессу в ООН по безопасности в сфере использования информационно-коммуникационных технологий более демократического, инклюзив-

[15] См.: официальный сайт Министерства иностранных дел Российской Федерации. URL: http://www.mid.ru (дата обращения: 30.06.2019).

[16] Резолюция № A/RES/73/27 Генеральной Ассамблеи ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», принята 05.12.2018 на 45-м пленарном заседании 73-й сессии Генеральной Ассамблеи ООН // Система официальной документации ООН. URL: https://documents.un.org/prod/ods.nsf (дата обращения: 30.06.2019).

ного и транспарентного характера созывается рабочая группа открытого состава[17] (под эгидой Комиссии по предупреждению преступности и уголовному правосудию) для продолжения в качестве приоритета дальнейшей выработки соответствующих норм, правил и принципов. Наравне с указанным структурным нововведением с 2019 г. сформирована (на основе справедливого географического распределения) очередная Группа правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, комплексный доклад о результатах работы которой ожидается, соответственно, в 2021 г.

А 17 декабря 2018 г. российский «цифровой взгляд» на общую проблему вновь получает необходимую поддержку — Генеральная Ассамблея ООН принимает российский проект резолюции «Противодействие использованию информационно-коммуникационных технологий в преступных целях»[18], которая является значимым этапом в активизации международного сотрудничества, перехода от «протяжных» призывов к совместным действиям.

Россия, несомненно, несмотря на значительные политические препятствия, будет продолжать продвигать свои инициативы на международной арене, но, как заметил А. В. Крутских, «устраивать в ООН “гладиаторские бои” по теме международной информационной безопасности — не тот вариант, за который мы выступаем»[19]. Диалог о путях разрешения конфликтных ситуаций в киберпространстве не должен создавать бóльшую конфронтацию между странами.

Технический прогресс организовал мировую цифровую революцию, под флагами которой возник совершенно новый тип государства — цифровое государство, развивающее уже цифровую экономику, новый вид государственного суверенитета — информационный суверенитет и новое поколение прав человека — цифровые права. Распространение информационных технологий достигло такого уровня, что при характеристике практически любых современных процессов и явлений требуется дополнение главного прилагательного «цифровой».

Только суверенное государство способно обеспечивать эффективность государственно-правовых институтов, прогрессивность экономических процессов и реализацию прав и свобод человека. По мнению А. А. Кокошина, реальным суверенитетом, т.е. способностью государства на деле (а не декларативно) самостоятельно проводить свою политику, обладает сравнительно небольшое число стран, и это не только современный феномен, так было на протяжении практически всей мировой истории[20]. Сегодня сохранение и укрепление государственного суверенитета зависит от устойчивости суверенитета информационного, и, следовательно, можно заключить, что государств, обладающих так называемым реальным суверенитетом, становится все меньше, поскольку новые вызовы и угрозы в киберпространстве усиливают зависимость одних государств от других, в особенности при неравновесности их цифрового потенциала.

Сегодня «информационные общества» отдельных национальных юрисдикций включены в единое глобальное информационное пространство и вместе с тем разобщены вследствие множества противоречий и конфликтов, возникающих за его пределами, но ставших его неотъемлемой частью. Общество оказывается в ловушке научно-технических достижений, вредоносность которых может превысить их неоспоримо высокую полезность.

---

[17] 3—4 июня 2019 г. в г. Нью-Йорке была проведена первая организационная сессия рабочей группы, определившая основные направления ее деятельности.

[18] Резолюция № A/RES/73/187 Генеральной Ассамблеи ООН «Противодействие использованию информационно-коммуникационных технологий в преступных целях», принята 17.12.2018 на 56-м пленарном заседании 73-й сессии Генеральной Ассамблеи ООН // Система официальной документации ООН. URL: https://documents.un.org/prod/ods.nsf (дата обращения: 30.06.2019).

[19] См.: *Крутских А. В.* России нечего скрывать и нечего бояться // Коммерсантъ. № 53. 27.03.2019. С. 6.

[20] См.: *Кокошин А. А.* Реальный суверенитет в современной мирополитической системе. Изд. 3-е, расшир. и доп. М., 2006. С. 63.

Позволяя некоторое философское отступление, полагаем в определенной степени уместным обращение к словам немецкого мыслителя Иммануила Канта, который писал: «Две вещи наполняют душу постоянно новым и возрастающим удивлением и благоговением и тем больше, чем чаще и внимательнее занимается ими размышление: звездное небо надо мной и нравственный закон во мне»[21]. Создание искусственного интеллекта человеком, когда-то камнем добывавшего огонь, вызывает почтение перед интеллектом естественным: виртуальное киберпространство мыслимо с тем же трудом, что и звездное небо; а нравственные законы, живущие в нас и составляющие ядро международной морали, вызывают изумление: человек, опутывая себя прочными нитями киберсети, сохраняет нравственные силы, чтобы выбраться из этой западни, призывая к взаимопомощи.

Коррелятивная связь правовых, организационных и технических мер обеспечения кибербезопасности требует от экспертного обсуждения, любого вида и уровня, тесного сотрудничества юристов, политиков и специалистов в поиске ответов на вопросы о том, какие обязательства государства готовы и должны на себя принимать, каким образом осуществлять контроль за их надлежащим исполнением и насколько предлагаемые меры реализуемы согласно внутренним «законам и механике» самого киберпространства.

БИБЛИОГРАФИЯ

1. *Бекяшев К. А.* Международное публичное право : учебник. — М., 2019. — 1048 с.
2. *Кант И.* Критика практического разума и основоположение к метафизике нравов : полн. пер. с прим. и прил. / сост. Н. Смирнов. — С.-Петербург, 1879. — 192 с.
3. *Капто А. С.* Современная цивилизация: вызовы и альтернативы. — М. : Изд-во Московского университета, 2013. — 304 с.
4. *Кокошин А. А.* Реальный суверенитет в современной мирополитической системе. — Изд. 3-е, расшир. и доп. — М., 2006. — 180 с.
5. *Henckaerts J.-M*. Study on customary international humanitarian law: A contribution to the understanding and respect for the rule of law in armed conflict // International Review of the Red Cross. — 27.04.2010. — Pp. 175—212.

Материал поступил в редакцию 12 июля 2019 г.

REFERENCES (TRANSLITERATION)

1. Bekyashev K. A. Mezhdunarodnoe publichnoe pravo : uchebnik. — M., 2019. — 1048 s.
2. Kant I. Kritika prakticheskogo razuma i osnovopolozhenie k metafizike nravov : poln. per. s prim. i pril. / sost. N. Smirnov. — S.-Peterburg, 1879. — 192 s.
3. Kapto A. S. Sovremennaya civilizaciya: vyzovy i al'ternativy. — M. : Izd-vo Moskovskogo universiteta, 2013. — 304 s.
4. Kokoshin A. A. Real'nyj suverenitet v sovremennoj miropoliticheskoj sisteme. — Izd. 3-e, rasshir. i dop. — M., 2006. — 180 s.
5. Henckaerts J.-M. Study on customary international humanitarian law: A contribution to the understanding and respect for the rule of law in armed conflict // International Review of the Red Cross. — 27.04.2010. — Rp. 175—212.

[21] *Кант И.* Критика практического разума и основоположение к метафизике нравов : полн. пер. с прим. и прил. / сост. Н. Смирнов. С.-Петербург, 1879. С. 190.