

ОБЩИЕ ВОПРОСЫ ГОСУДАРСТВА И ПРАВА

GENERAL QUESTIONS OF THE STATE AND LAW

УДК 341.211:004(470)

DOI dx.doi.org/10.24866/1813-3274/2018-3/9-20

О. И. Мирошниченко¹

Дальневосточный федеральный университет, г. Владивосток, Россия

E-mail: olga-star.05@mail.ru

Д. С. Проскурина²

Дальневосточный федеральный университет, г. Владивосток, Россия

E-mail: sl.thsl@dvfu.ru

ГОСУДАРСТВЕННЫЙ СУВЕРЕНИТЕТ: ДИФФЕРЕНЦИАЦИЯ КАТЕГОРИИ В УСЛОВИЯХ КИБЕРРЕАЛИЙ³

Аннотация. Ключевой идеей исследования является вопрос о соотношении таких категорий, как «государственный суверенитет» и «киберпространство». Авторы считают, что существующая теория права и позитивное правовое регулирование на настоящем этапе не предлагают разумных вариантов взаимодействия и сосуществования указанных понятий. В условиях кардинальных изменений существующих реалий, произошедших за последние 30 лет, встаёт вопрос о дифференциации правового регулирования, которое всё ещё рассчитано в большей степени на существовавшие в XX столетии общественные отношения. Сегодня технический прогресс существенно опережает социальное, в частности, правовое регулирование, которое, в свою очередь, серьёзно «завязано» на государстве, или «территориальной организации власти в обществе, обладающей суверенитетом...». И здесь воз-

¹ Ольга Игоревна Мирошниченко, кандидат юридических наук, LLM, доцент кафедры теории и истории государства и права Юридической школы Дальневосточного федерального университета, г. Владивосток, Россия

² Дарья Сергеевна Проскурина, студентка Юридической школы Дальневосточного федерального университета, г. Владивосток, Россия.

Для цитирования: Мирошниченко О.И., Проскурина Д.С. Государственный суверенитет: дифференциация категории в условиях киберреалий // Азиатско-Тихоокеанский регион: экономика, политика и право. 2018. № 3. С. 9–20.

³ Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16129.

никает основной вопрос о разумности обозначенной формулировки. Подходит ли она под существующие реалии? Или сама по себе является препятствием для правовой актуализации? В рамках статьи анализируются различные подходы к правовому урегулированию отношений в рамках киберпространства, а также предлагаются два варианта наднационального регулирования указанных правоотношений – через разработку и создание внетерриториального международного органа, который будет обладать не только возможностью контроля общественных отношений в рамках киберпространства, но и специальными рычагами принуждения для воздействия на граждан любых государств, либо с помощью создания глобальной системы международных актов, которая бы регулировала большую часть существующих вопросов о взаимодействии лиц в киберпространстве и включала в себя четкий механизм быстрого реагирования на возникновение новых отношений в указанной сфере.

Авторы также полагают, что неспособность на теоретическом уровне концептуализировать соотношение указанных категорий может в будущем привести к дискредитации таких понятий, как «национальное государство» и «государственный суверенитет».

Ключевые слова: государственный суверенитет, киберпространство, государственная юрисдикция, киберсеть.

Olga I. Miroshnichenko¹

Far Eastern Federal University, Vladivostok, Russia

E-mail: olga-star.05@mail.ru

Darya S. Proscurina²

Far Eastern Federal University, Vladivostok, Russia

E-mail: sl.thsl@dvfu.ru

STATE SOVEREIGNTY: DIFFERENTIATION OF THE CATEGORY IN CYBER REALITIES³

Abstract. The key idea of this research is the correlation of two theoretical categories: national sovereignty and cyberspace. The authors think that neither theoretical legal science nor positivistic methods today can suggest any effective models for coexistence and cooperation of these phenomena. In the last 30 years lots of very significant changes have been made thus making the question of differentiation of legal reality very relevant. Today technical progress significantly outpaces the social, and in particular, the legal regulation which, in turn, is seriously based on the state, or on "the territorial organization of the power in society which has sovereignty ...". And here the main question of rationality of the designated formulation arises. Does this approach fit the existing reality? Or in itself it is an obstacle for legal updating? Different approaches to resolving and regulation of juridical relations are being analyzed. As a result two prospective ways of supranational regulation are suggested. The first one requires creating a unique authority, which won't be related to any state, but will have control over any cyber actors within any territory. The second variant is about a strict regulation of any acts within the cyber space through the system of independent legal documents. This system should also include a very quick mechanism of regulation of any rule violation. The authors also think that if no conceptualization of the above-mentioned categories is made in the nearest future, this may discredit the notions of "legal sovereignty" and "national state".

Keywords: national sovereignty, cyberspace, national jurisdiction, cyber net.

Технический прогресс в двадцать первом веке, очевидно, давно достиг того уровня, который обязывает к созданию эффективных и актуальных правовых ин-

¹ Olga I. Miroshnichenko, PhD in legal science, LLM in legal theory, associate professor, department of theory and history of state and law, Law School, Far Eastern Federal University, Russia.

² Darya S. Proscurina, student of Bachelor's degree course, Law school, Far Eastern Federal University, Russia.

For citing: Miroshnichenko O. I., Proscurina D. S. State sovereignty: differentiation of the category in cyber realities // Asia-Pacific RIM: Economic, Politics, Law. 2018. № 3. P. 9–20.

³ The reported study was funded by RFBR according to the research project № 18-29-16129.

струментов регулирования порождаемых им общественных отношений. Еще 20-30 лет назад субъект, сомневающийся в могуществе гоббсовского Левиафана (государства) или высказывавший мысль о «роботизации через глобализацию», казался чудачком и мечтателем. Сегодня идея «большой деревни» [1] не только не кажется утопией, но зачастую пугает своей реальностью. А на уровне современной теоретической правовой науки прочно оформляется мысль о кибер-правовой системе, не существующей в рамках никакой территориальности, но, тем не менее, обладающей всеми признаками указанной теоретической категории. Но самое интересное (или пугающее, в зависимости от субъекта и контекста рассмотрения), что самих акторов нового пространства, так называемого cyberspace, выкладки учёных и теоретиков мало волнуют. Такие гиганты, как Amazon, Facebook и т.д. фактически доказывают свою состоятельность, отдавая на откуп учёным лишь аналитику собственной деятельности.

Таким образом, отрицать произошедшие за последние 30 лет кардинальные изменения существующих реалий элементарно неразумно. Встаёт вопрос о дифференциации правового регулирования, которое всё ещё рассчитано в большей степени на существовавшие в XX столетии общественные отношения. Сегодня технический прогресс существенно опережает социальное, в частности, правовое регулирование, которое, в свою очередь, серьёзно «завязано» на государстве, или «территориальной организации власти в обществе, обладающей суверенитетом...». И здесь возникает основной вопрос, который мы хотим рассмотреть в рамках настоящего исследования: а так ли разумна указанная формулировка? Подходит ли она под существующие реалии? Или сама по себе является препятствием для правовой актуализации? Мы не можем изменить действительность: активное использование современных технологий в жизни граждан большинства стран мирового сообщества – данность, необходимость. Но что делать с основной обязанностью государства – защитой прав и интересов своих граждан, которая весьма осложнена в современных «киберусловиях»?

В частности, в попытках государств защищать интересы своих граждан в пространстве, не имеющем географических границ, возникает проблема соотношения таких категорий, как государственный суверенитет и киберпространство. Мы считаем, что основным в указанном контексте становится вопрос о модернизации самой классической концепции государственного суверенитета в современной теории права. Если сегодня не пересмотреть основные теоретические категории, мы рискуем прийти к реализации принципа, провозглашённого Декларацией независимости киберпространства: «...киберпространство – это так называемый terra nullius, к которому исторически созданные социальные регулятивы и законы не имеют никакого отношения и в рамках которого они будут воссозданы заново» [2].

Считаем разумным начать исследование с дифференциации указанных выше понятий.

Вспользуемся, например, классическим определением С.М. Кукушкиной, которая трактует суверенитет как формально-юридическую категорию, сформировавшуюся одновременно с государством; неотъемлемое, необходимое, качественное, конституционно-правовое свойство государства быть верховным внутри государственных границ и независимым на международной арене [3]. Иными словами, суверенным государством в международном праве считается такое государство, чья юрисдикция распространяется на всю его географическую территорию и не зависит от юрисдикции иного государства.

Таким образом, государственный суверенитет есть правовое поле, которое держит в сохранности правовую политику конкретного государства, организацию общественных отношений внутри этого государства и позволяет ограничить воздействие глобализации на отношения, в которые вступают его граждане. Его роль значительно снизилась с развитием информационных коммуникаций и технологий, которые создали отдельное пространство, не подвергаемое географическому разграничению.

Верховный суд США определяет киберпространство как уникальный носитель, известный его пользователям как киберпространство, не находящийся на определенной территории, но доступный каждому в любой точке мира через Интернет [4].

Международная организация по стандартизации даёт следующее определение киберпространства: сложная среда, которая возникает в результате взаимодействия людей, программного обеспечения и предоставления услуг в Интернете посредством технологических устройств и сетей, подключённых к нему, которая не существует ни в какой физической форме [5].

Таким образом, мы можем сделать вывод о том, что киберпространство представляет собой созданное на основании всеобщей сети Интернет информационное поле, в рамках которого возникают общественные отношения правового характера, не определяемые какими-либо территориальными границами.

В свете этого, вопрос о соотношении категорий киберпространства и государственного суверенитета в международном праве является актуальным, ведь сфера распространения второго феномена, а равно и юрисдикции конкретного государства, традиционно определялась его территорией. Киберпространство же нематериально и не подвержено географическим рамкам, вследствие чего возникает проблема определения сферы распространения государственной юрисдикции на конкретный объём киберпространства. Более того, возникает вопрос о самой возможности определения юрисдикционных границ государств в киберпространстве.

Бесспорно, киберпространство является средой, в которой, в том числе, возникают общественные отношения правового характера. Однако, в отличие от право-

отношений, реализуемых в рамках территориальной юрисдикции, их кибер-аналоги не подвержены регулированию конкретным государством, вследствие чего возникает проблема защиты прав и интересов граждан в случае, если они вступают в какое-либо общественное отношение через кибер-сеть.

Так, при рассмотрении дела *American Libraries Ass'n v. Pataki* суд США пришёл к выводу о том, что географические рамки не могут быть применимы к Интернету. Он провозгласил, что пользователи конкретного интернет-ресурса не знают и не интересуются его физическим нахождением. Суд заявил, что интернет-протоколы были разработаны скорее для того, чтобы игнорировать, а не подтверждать географическое местоположение. Фактически это судебное решение говорит о бесполезности географических границ в Интернете [6].

Тем не менее, существует и категорически иная точка зрения на «территориальность» и необходимый тип регулирования киберпространства, декларируемая и продвигаемая в частности такими государствами, как РФ и КНР. С точки зрения обозначенного подхода, в рамках каждого конкретного государства должны существовать так называемые *codes of conduct*, обозначающие устраивающие конкретную страну принципы регулирования киберпространства. Иными словами, в данном случае киберсреда – это отнюдь не сфера свободного обмена информацией между акторами вне зависимости от их национальности, гражданства и иных характеристик, а достаточно чётко урегулированная позитивным правом часть национальной правовой системы.

В любом случае, очевидно, что на настоящем этапе международное право, исходящее главным образом из принципа территориальности, не готово к чёткому урегулированию юридических конфликтов, в которых задействованы такие внетерриториальные образования, как Интернет [7].

Мировой опыт демонстрирует достаточное количество попыток установления границ киберпространства путём средств идентификации.

Наиболее предсказуемым методом проведения принципа суверенитета в киберпространство являются попытки идентифицировать информацию в сети и её отношение к конкретному государству. Например, сайты содержат URL индикаторы происхождения вроде “ru”, “nl”, однако это никак не способствует распространению суверенитета того или иного государства на отношения, которые возникают в связи с взаимодействием конкретного субъекта права с такой идентифицированной информацией [7]. В силу того, что доступ к конкретной информации в киберпространстве может получить любой человек, не зависимо от его места нахождения, политика распространения юрисдикции конкретного государства на ту или иную информацию в сети бессмысленна.

Так как информация в любом случае будет находиться в глобальном доступе, а отношения, которые возникнут по поводу этой информации, не смогут быть урегу-

лированы в рамках юрисдикции одного государства, как минимум из-за того, что в данном случае субъект такого отношения может не являться гражданином страны, чьей информацией он воспользовался.

Именно поэтому определение юрисдикции по местонахождению информации на сервере не является верным. Например, в деле *Steven Rambam v. JDO* американский суд установил недостаточность критерия нахождения сервера для установления юрисдикции [8].

Конструирование, а именно перевод контента одного сайта на адрес другого, которое проявляется в наличии перекрестных ссылок, делает политику идентификации интернет-ресурсов ещё более условной и является неотъемлемой частью глобальной сети. Такая особенность киберпространства обуславливается спецификой сети Интернет и также делает очевидной неэффективность применения понятия географической территориальности и юрисдикции в международном праве, поскольку в информационном пространстве почти теряется связь с физическим местоположением [9].

Итак, мы убедились в том, что существует потребность в разработке норм международного права, иным образом дифференцирующих правовой режим киберпространства и таким образом решающих проблему возможных государственно-кибернетических коллизий. Проблема реализации государственного суверенитета и юрисдикции в киберпространстве не может быть урегулирована самостоятельно ни в одном государстве, исходя только из существующих норм национального законодательства. Решение этой проблемы возможно лишь принятием соответствующей международной конвенции [10, с. 56].

Так, внедрение Интернета и информационно-коммуникационных технологий (ИКТ) в поле международно-правового регулирования необходимо, так как современные технологии вытесняют понятие географической территориальности. Однако такие нововведения могут поставить под угрозу основополагающие принципы традиционного международного права.

Мы считаем, международное право должно адаптировать свои догмы к внетерриториальным информационным образованиям, в частности, через адекватную интерпретацию категории «государственный суверенитет». Только в этом случае понятие государственного суверенитета будет актуально в условиях информационной глобализации.

Дэвид Пост и Дэвид Джонсон также придерживаются этой позиции, говоря о том, что многие из юрисдикционных и иных существенных проблем, возникающих в сфере всеобъемлющих коммуникационных технологий, могут быть разрешены с помощью одного простого принципа: представление о киберпространстве как об отдельном «месте» в целях осуществления юридического анализа путем признания юридически значимой границы между киберпространством и «реальным миром» [11].

Они считают, что киберпространство не может и не должно быть урегулировано теми институтами международного права, которые осуществляют правовое регулирование на материальной территории [11].

Таким образом очевидна невозможность приравнивания территориальных границ к виртуальным, как и, очевидно, невозможно применение традиционной концепции суверенитета в киберпространстве.

С теоретической точки зрения, идеальной моделью регулирования общественных отношений в рамках киберпространства являются проекты виртуальных государств, создаваемых в киберпространстве. Так, например, Й. Фергюсон и Р. Мэнсбач говорят о «Свободной бирманской коалиции» как об одном из таких государств. Территориально данное государство существует лишь в киберпространстве и «предлагает свою поддержку, которая трудно достижима географически [12]. То есть, модели таких государств в идеале могут защищать права своих «граждан» вне зависимости от их географического нахождения.

Очевидно, что к теоретизированным моделям виртуального государства невозможно применение понятия государственной суверенитет, так как речь не идёт ни о реальной территории, ни о юрисдикции конкретного традиционного государства.

Однако, исходя из всего вышеизложенного, следует также и вывод о том, что идея о «надправовом» регулировании отношений, возникающих в киберпространстве, в принципе может исключить классическое понимание суверенитета в международном праве.

Итак, мы считаем, что существует острая необходимость, во-первых, в концептуализации и признании киберпространства как сферы реализации общественных отношений, в том числе правового типа. Так, либо мы считаем киберпространство, по Барлоу, свободно функционирующей и не предполагающей вмешательства государства средой – это первый, по нашему мнению, крайне маловероятный вариант, либо, если мы делаем попытку включить киберпространство в существующий теоретический категориально-понятийный аппарат, совершенно очевидным становится острая необходимость изменения существующего правового инструментария, причём как фундаментального теоретического, так и позитивно-правового.

По нашему мнению, в рамках второго аспекта указанной проблемы наиболее перспективными являются два пути:

1. Попытка разработки и создания внетерриториального международного органа, который будет обладать не только возможностью контроля общественных отношений в рамках киберпространства, но и специальными рычагами принуждения для воздействия на граждан любых государств. Данный вариант является «идеальным решением» поставленной проблемы, так как при таком раскладе традиционное понятие государственного суверенитета в международном праве не утратит своего значения.

Мы полагаем, однако, что вероятность его реализации невелика, так как создание такой масштабной структуры, обладающей возможностью принуждения и не подпадающей под юрисдикцию того или иного государства, является крайне рискованным шагом для мирового сообщества. Попытка принятия такого шага была предусмотрена в Будапештской конвенции «О борьбе с киберпреступностью», подготовленной Советом Европы в 2001 г. [13]. Конвенция подписана представителями 30 стран в ноябре 2001 г. Она предусматривала создание транснационального органа, работающего в режиме реального времени и имеющего возможность удалять материалы вне зависимости от физического местонахождения интернет-ресурса. Однако положения данной конвенции так и не были реализованы [14, с. 40–44].

2. Создание глобальной системы международных актов, которая бы регулировала большую часть существующих вопросов о взаимодействии лиц в киберпространстве и включала в себя чёткий механизм быстрого реагирования на возникновение новых отношений в указанной сфере. Таким образом понятие суверенитета в международном праве стало бы включать в себя не только географическую территорию, но и объём потенциальных действий и возможностей, которые может совершать конкретное государство как актор киберпространства. Попытку создания такого соглашения предприняла Российская Федерация в 2011 г. Концепция Конвенции об обеспечении международной информационной безопасности явилась проектом глобального международного документа, охватывающего все ключевые вопросы противодействия угрозам из киберпространства в широком российском понимании.

Однако такой подход встретил резкое сопротивление со стороны США. Заместитель госсекретаря США М. Познер заявил о неприемлемости предложений, «превращающих Интернет из пространства, управляемого множеством людей и заинтересованных сторон, в подконтрольную центральным правительствам систему» [15, с. 126].

То есть данный вариант также является сложно реализуемым, так как, по мнению некоторых стран мирового сообщества, он может противоречить основным принципам демократии.

Бесспорным остаётся только одно: проблема соотношения категорий «государственный суверенитет» и «киберпространство» приобретает особое значение, так как неурегулированность этого вопроса может повлечь за собой серьёзные международные конфликты и международно-правовые коллизии. Мы полагаем также, что неспособность на теоретическом уровне концептуализировать указанное соотношение может в будущем привести к дискредитации таких понятий, как «национальное государство» и «государственный суверенитет».

СПИСОК ЛИТЕРАТУРЫ

1. Kaijuka, E. The world of innovations and Cyber Law. 2018 [Электронный ресурс]. – Режим доступа: https://www.academia.edu/37992759/the_world_of_innovations_and_cyberlaw.docx.
2. Barlow, J. P. Declaration of Independence of Cyberspace. 1996 [Электронный ресурс]. – Режим доступа: <https://www.eff.org/ru/cyberspace-independence>.
3. Кукушкина, С. М. Государственный суверенитет в современном мире : актуальные проблемы // Пробелы в российском законодательстве. – 2011. – № 3. – С. 84–86.
4. Menthe, D. Jurisdiction in cyberspace: a theory of international spaces // Michigan telecommunications and technology law review. – 1998. – Vol. 4, iss. 1. – P. 69–103.
5. Kristen, E. The Cyber-Law of nations // The Georgetown Law Journal. – 2015. – Vol. 103. – P. 317–380.
6. American Libraries Ass'n v. Pataki, 969 F. Supp. 160 (S.D.N.Y. 1997) [Электронный ресурс]. – Режим доступа: <https://law.justia.com/cases/federal/district-courts/FSupp/969/160/1808497/>.
7. Ансельмо, Э. Киберпространство в международном законодательстве: опровергает ли развитие Интернета принцип территориальности в международном праве? // Экономические стратегии. – 2006. – № 2. – С. 24–31.
8. Jewish Defense Organization, Inc. v. Superior Court (Rambam) (1999) [Электронный ресурс]. – Режим доступа: <https://law.justia.com/cases/california/court-of-appeal/4th/72/1045.html>.
9. Искевич, И. С. Актуальные проблемы определения юрисдикции при расследовании преступлений в информационном пространстве: международно-правовой аспект / И. С. Искевич, М. Н. Кочеткова, А. М. Попов // Проблемы правоохранительной деятельности. – 2016. – № 4. – С. 54–58.
10. Brown, K. The problems of International Finance Law and electronic commerce / K. Brown, S. Kaaya. – Sydney, 2000.
11. Johnson, D. R. Law and borders – the rise of law in Cyberspace / D. R. Johnson, D. G. Post // Stanford Law Review. – 1996. – Vol. 48, iss. 5. – P. 1367–1402.
12. Fergusson, Y. H. Technology and the transformation of global politics / Y. H. Fergusson, R. W. Mansbach // Geopolitics. – 1999. – Vol. 4, iss. 3. – P. 1–28.
13. Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 г.) [Электронный ресурс] // СПС «Гарант». – Режим доступа: <http://base.garant.ru/4089723/>.
14. Шарифов, М. Ш. Суверенная власть в киберпространстве и в сетевом пространстве // Современное право. – 2009. – № 6. – С. 40–44.

15. Бедрицкий, А. В. Международные договорённости по киберпространству: возможен ли консенсус? // Проблемы национальной стратегии. – 2012. – № 4 (13). – С. 119–136.

REFERENCES

1. Kaijuka E. *The world of Innovations and Cyber Law, 2018*. Available at: https://www.academia.edu/37992759/the_world_of_innovations_and_cyberlaw.docx (accessed 18 March 2018).

2. Barlow J. P. *Declaration of Independence of Cyberspace, 1996*. Available at: <https://www.eff.org/ru/cyberspace-independence> (accessed 10 March 2018).

3. Kukushkina S.M. Gosudarstvennyi suverenitet v sovremennom mire: aktual'nye problemy [State sovereignty in the modern world: Actual problems]. *Probely v rossiiskom zakonodatel'stve* [Gaps in the Russian legislation], 2011, no. 3, pp. 84–86.

4. Menthe D. Jurisdiction in Cyberspace: A Theory of International Spaces. *Michigan Telecommunications and Technology Law Review*, 1998, vol. 4, iss. 1, pp. 69–103.

5. Kristen E. *The Cyber-Law of Nations. California; Los Angeles (UCLA)*. Available at: <https://georgetownlawjournal.org/articles/63/cyber-law-of-nations/pdf> (accessed 10 March 2018).

6. *American Libraries Ass'n v. Pataki, 969 F. Supp. 160 (S.D.N.Y. 1997)*. Available at: <https://law.justia.com/cases/federal/district-courts/FSupp/969/160/1808497/> (accessed 22 March 2018).

7. Ansel'mo E. Kiberprostranstvo v mezhdunarodnom zakonodatel'stve: oprovergaet li razvitie Interneta printsip territorial'nosti v mezhdunarodnom prave? [Cyberspace in international law: does the development of the Internet negate the principle of territoriality in international law?]. *Ekonomicheskie strategii*, 2006, no. 2, pp. 24–31.

8. *Jewish Defense Organization, Inc. v. Superior Court (Rambam) 1999. Court of Appeal, Second District, Division 7, California*. Available at: <https://law.justia.com/cases/california/court-of-appeal/4th/72/1045.html> (accessed 10 March 2018).

9. Iskevich I. S., Kochetkova N. M., Popov A. M. Aktual'nye problemy opredeleniya yurisdiksii pri rassledovanii prestuplenii v informatsionnom prostranstve: mezhdunarodno-pravovoi aspekt [Actual problems of definition of jurisdiction in the investigation of crimes in the information space: the international legal aspect]. *Problemy pravookhranitel'noi deyatel'nosti*, 2016, no. 4, p. 54–58.

10. Brown K., Kaya S. *The problems of International Finance Law and Electronic Commerce*. Sydney, 2000.

11. Johnson D. R., Post D. G. Law and Borders – The Rise of Law in Cyberspace. *Stanford Law Review*, 1996, vol. 48, iss. 5, pp. 1367–1402.

12. Fergusson Y. H., Mansbach R. W. Technology and the Transformation of Global Politics. *Geopolitics*, 1999, vol. 4, iss. 3, pp. 1–28.

13. *Convention on crime in the sphere of computer information ETS No. 185 Budapest, November 23, 2001*. Available at: <http://base.garant.ru/4089723/>. (In Russian).

14. Sharifov M.S. Suverennaya vlast' v kiberprostranstve i v setevom prostranstve [Sovereign power in cyberspace and in the network space]. *Sovremennoe pravo*, 2009, no. 6, pp. 40–44.

15. Bedritskii A.B. Mezhdunarodnye dogovorennosti po kiberprostranstvu: vozmozhen li konsensus? [International agreements on cyberspace: can there be a consensus?]. *Problemy natsional'noi strategii*, 2012, no. 4 (13), pp. 119–136.