Эволюция права в эпоху постпандемии: мировой опыт технологической интеграции и кибербезопасности

Карцхия А. А., Ибрагимов Дж. Ю.[1]

Ключевые слова: *защита данных, киберзащита, киберугрозы, персональные данные, обработка данных, защита информации, страны БРИКС.*

Аннотация. *Статья посвящена анализу совершенствования законодательства в сфере защиты данных и кибербезопасности на примере стран БРИКС в условиях постпандемии COVID-19 и ее влияния на перспективы развития правовых институтов на основе сравнительно-правового анализа российского и зарубежного законодательства и практики правоприменения. Новое законодательство, по мнению авторов, построенное на принципах всеобъемлющей защиты прав и законных интересов личности, эффективной киберзащиты данных, должно способствовать достижению оптимальной защиты личных интересов граждан и национальных интересов государства и общества.*

DOI: 10.21681/2226-0692-2021-2-36-41

Общемировой кризис, вызванный последствиями пандемии COVID-19, стал фактором, оказавшим сильное стимулирующее воздействие на научно-технологическое развитие, и во многом способствовал переформатированию социального и экономического уклада современного общества.

Характер изменений в технологической среде, как отмечалось на Всемирном экономическом форуме [1], определяется растущими системными рисками, которые потребуют обеспечения кибербезопасности операций и эффективного управления кибер-рисками в сфере бизнеса и критических национальных инфраструктур, а также стройной системы действий со стороны государств на национальном и международном уровне для принятия решений в области безопасности и способствующих повышению доверия и прозрачности между различными компонентами экосистемы информационной и кибербезопасности, включая системность мер ответственности, оптимизации существующих моделей регулирования бизнеса и госуслуг, содействие международному бизнесу и торговле данными и цифровыми услугами. Необходимо принять меры в целях получения выгоды от новых технологий с учетом потребностей развивающихся стран и необходимости коллективных усилий по сокращению трансграничной киберпреступности. Киберпространство стремительно растет по мере появления новых подключенных устройств, сетей, сервисов и данных, что приводит к расширению масштаба не только сетей, но и объемов данных, емкости хранилищ, систем обработки и пространства знаний. Современные исследования выявляют четыре репрезентативные трансформационные технологии, которые в ближайшей перспективе будут способствовать изменению динамики киберпространства: повсеместная связность (англ. ubiquitous connectivity), искусственный интеллект (англ. artificial intelligence (AI)), квантовые вычисления (англ. quantum computing) и, наконец, подходы следующего поколения технологий к управлению идентификацией и доступом к данным в киберпространстве для создания новых сервисов, приложений и операционных моделей.

Современные исследователи отмечают, что основа геополитического доминирования перешла от промышленного производства к информационному контролю. Это изменение уже более десяти лет определяет смещение глобального баланса сил от США в пользу Китая, который вкладывает существенные ресурсы в новые технологии: беспроводную связь 5G, квантовые вычисления и искусственный интеллект с целью усиления своего контроля над глобальным потоком информации. Эта стратегическая оценка основана как на динамике современной конкуренции великих держав, так и на стратегических оценках, подготовленных Институтом национальных стратегических исследований (США) в последние 40 лет. Великая держава демонстрирует, как отмечается в аналитическом отчете [2], три очевидных атрибута: всеобъемлющие возможности, независимое поведение и признание другими государствами лидирующего статуса державы в международной системе. Это приводит к обладанию нестандартными чертами в сравнении с другими государствами. Великая держава использует эти характеристики для реализации широ-

[1] ***Карцхия Александр Амиранович,*** доктор юридических наук, профессор кафедры гражданско-правовых дисциплин РГУ нефти и газа (НИУ) имени И. М. Губкина, г. Москва, Российская Федерация.
E-mail: arhz50@mail.ru
Ибрагимов Джавид Юсифович, аспирант кафедры гражданско-правовых дисциплин РГУ нефти и газа (НИУ) имени И. М. Губкина, г. Москва, Российская Федерация.
E-mail: javid-ibrahimov@yandex.ru

ких внешнеполитических интересов за пределами своего непосредственного территориального окружения и воспринимается другими государствами как могущественная и влиятельная держава. На заре новой эры Соединенные Штаты, Китай и Россия подходят под такое описание великой державы.

Статус государства (державы) в последние годы ассоциируется в том числе с возможностями и развитостью системы национальной безопасности и структурированности этого современного феномена, во многом характеризующего суверенитет, политический и экономический потенциал государства [3].

Концепция суверенитета предполагает, что государства являются основными действующими лицами в международном праве, утверждая юрисдикцию на основе принципов территориальности и доктрины влияния. Территориальный принцип означает, что государства имеют полномочия регулировать передачу информации через свои границы и использование такой информации людьми, находящимися на их территории. Это отразилось, например, в попытках Китая сохранить свой информационный суверенитет, изолировав свой Интернет от западных веб-сайтов и фильтрацией потенциально вредной информации. Государства часто ссылаются на территориальный принцип для мониторинга аппаратного и программного обеспечения, используемого в интернет-коммуникациях на территории государства [4].

Развитие современной экосистемы национальной безопасности связано также с формированием новых структурных элементов национальной безопасности, таких как биобезопасность, кибербезопасность, криптобезопасность и инвестиционная безопасность, что находит свое выражение в законах и правоприменительной практике России и многих зарубежных стран, включая страны БРИКС. В целом система национальной безопасности с правовой точки зрения представляет собой систему законодательных и иных правовых актов, обеспечивающих государственный суверенитет страны, права и законные интересы ее граждан в соответствии с конституционно-правовыми положениями Конституции РФ, защиту критически важной структуры страны и их антитеррористическую защищенность. В зависимости от появления новых угроз национальным интересам, новых вызовов внутреннего и внешнего характера могут появляться новые направления деятельности (элементы), защиты которых требуют национальные интересы [5, 6].

Нынешний пандемический кризис COVID-19, по экспертной оценке [7], является яркой иллюстрацией глобализации дебатов о конфиденциальности данных. К примеру, законодательная база ЕС по защите данных и конфиденциальности (Общий регламент ЕС по защите данных, англ. General Data Protection Regulation (GDPR), 2018) оказалась достаточно гибким инструментом, позволяющим разрабатывать практические решения (например, приложения для отслеживания), обеспечивая при этом высокий уровень защиты персональных данных. Другим аспектом информационной безопасности является коммерческое использование персональных данных, часто помимо воли их обладателей. Характерным примером такой коммерциализации может служить публичное закрепление в правилах WhatsApp изменения схемы передачи персональных данных пользователей: мессенджер будет передавать данные о пользователях материнской компании Facebook, а она дальше может использовать эти данные для анализа, подбора контекстной рекламы и перепродажи другим компаниям[2].

Регулирование правовой защиты данных стало ключевой точкой во время пандемии в отношении решения множества проблем, включая сбор, отслеживание и защиту медицинских, биометрических и иных данных, а также обеспечение кибербезопасности удаленной работы, поскольку работники всё чаще работают дома. Пандемия ускорила отход от ручных, бумажных рабочих процессов и повысила риски кибербезопасности для бизнеса. В потребительской сфере торговые предприятия и владельцы брендов стали расширять свои каналы электронной коммерции, чтобы иметь больше возможностей для дистанционных продаж, что также имеет важные последствия для защиты данных и кибербезопасности.

В этой связи интересен опыт стран БРИКС в сфере кибербезопасности и правового регулирования оборота персональных данных. В странах группы БРИКС (Бразилия, Россия, Индия, Китай и ЮАР) в совокупности проживает 3,2 млрд человек, или 40% населения мира. Эти страны являются основными производителями таких данных, защита которых становится ключевым приоритетом для формирования современной среды человека, цифровой экосистемы. Растущая экономическая и стратегическая ценность персональных данных становится важным фактором утверждения «цифрового суверенитета» государств. Страны БРИКС в последние годы предприняли серьезные изменения в области регулирования защиты данных, разработав новое законодательство, обновив существующие или учредив новые регулирующие органы [8, 3].

Новый импульс в развитии российского права связан с новеллами Основного закона Российской Федерации, которые, в частности, выделили сферу обеспечения безопасности личности, общества и государства при применении информационных технологий, обороте цифровых данных среди предметов ве́дения Российской Федерации (пп. «м» ст. 71 Конституции Российской Федерации).

В связи с этим приобретает особую актуальность вопрос баланса прав и законных интересов, правового положения участников правоотношений, связанных с поиском, получением, передачей, производством и распространением персональных данных, с учетом современного уровня развития средств и способов обращения такого специфического нематериального объекта, какой является информация [9, с. 30—31].

В Российской Федерации в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (ст. 3) персональными данными является любая информация, прямо или косвенно относящаяся к субъекту персональных данных — определенному или определяемому физическому лицу. Обработка персональных данных — т. е. любое действие (операция) или совокупность действий (операций), совершаемых

[2] URL: http://www.whatsapp.com/legal/updates/privacy-policy?eea=0#privacy-policy-updates-how-we-work-with-other-facebook-companies .

с использованием средств автоматизации или без использования таких средств с персональными данными и включающих сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных — допускается только с согласия субъекта персональных данных, который дает согласие на обработку таких данных свободно, своей волей и в своем интересе. Такое согласие должно быть конкретным, информированным и сознательным и может быть отозвано субъектом персональных данных. Допускается обработка персональных данных без согласия их обладателя только в определенных законом случаях. Закон требует обеспечения конфиденциальности персональных данных, возлагая обязанность на операторов и иных лиц, получивших доступ к персональным данным, не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Запрещена обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни. Исключения допускаются, в частности, в случаях необходимой обработки персональных данных для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно, а также обработки персональных данных в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну.

К особой категории персональных данных относятся биометрические данные, т. е. сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных.

Биометрические персональные данные гражданина РФ могут проходить обработку в единой информационной системе персональных данных, обеспечивающей их обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации (ст. 14.1 Федерального закона от 27.07.2006 № 149-ФЗ (ред. от 08.06.2020) «Об информации, информационных технологиях и о защите информации»)[3].

КНР активно совершенствует законодательство в сфере всеобъемлющего регулирования кибербезопасности и защиты данных. Краеугольным камнем регулирования защиты данных и кибербезопасности в Китае является Закон о кибербезопасности, который вступил в силу в июне 2017 г. Закон сформулирован в общих чертах, и многие детали оставлены для уточнения в подзаконных актах. В КНР также принят «Стандарт технологии информационной безопасности — Спецификация безопасности персональных данных (ПД)», применяемый с 1 октября 2020 г. и содержащий набор правил, частично напоминающих положения Европейского регламента по защите персональных данных (GDPR). Кроме того, в октябре 2020 года опубликованы для обсуждения проекты Закона о защите личной информации и Закона о безопасности данных [10]. Эти законодательные новации во многом следуют принципам европейской модели защиты данных.

В то же время усилия Китая по обеспечению «киберсуверенитета» [11] являются отличительным фактором, поскольку Китай, как и многие другие страны, рассматривает политику защиты данных и кибербезопасности как инструмент международной торговли и политики национальной безопасности. Кроме того, опираясь на международный опыт, Китай уделяет повышенное внимание регулированию мощных цифровых платформ, которые являются основой электронной коммерции, цифровых коммуникаций и контента в КНР. Более строгие меры защиты данных — ключевая особенность этих нормативных инициатив, ориентированных на внутренний рынок, а политика «Защита данных 2.0» направлена на постоянное продвижение стандартов защиты данных в административных регионах страны.

С 1 января 2021 года в КНР вступил в силу Гражданский кодекс КНР[4], в котором предусмотрена глава «Право на неприкосновенность частной жизни» и «Защита личных данных», где дается определение персональной информации как различных типов информации, записываемой в электронном виде или иным образом, которые могут идентифицировать конкретное физическое лицо отдельно или в сочетании с другой информацией, включая имя физического лица, дату рождения, номер документа, удостоверяющего личность, биометрическую информацию, адрес проживания, номер телефона, адрес электронной почты, информация о здоровье, информация о местонахождении и др. Персональные данные — это любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу (субъект данных); идентифицируемое физическое лицо — это лицо, которое может быть идентифицировано прямо или косвенно, в частности, посредством ссылки на идентификатор, такой как имя, идентификационный номер, данные о местоположении, сетевой идентификатор либо один или несколько факторов, специфичных для физической, физиологической, генетической, умственной, экономической, культурной или социальной идентичности этого физического лица.

В 2020 году представлены к рассмотрению проекты Закона о безопасности данных и Закона о защите личной информации. Законопроект о защите личной информации устанавливает, в частности, порядок оценки безопасности экспорта данных для лиц, передающих данные, которые (i) являются операторами критически важной информационной инфраструктуры или (ii) вы-

[3] Собрание законодательства РФ, 31.07.2006, № 31 (1 ч.), ст. 3448.

[4] URL: http://chinalaw.center/civil_law/china_civil_code_2020_russian .

полняют обработку определенных объемов данных, соответствующих пороговым значениям существенности, устанавливаемым Администрацией киберпространства Китая. Кроме того, законопроекты предусматривают меры противодействия дискриминационному обращению — уполномочивают китайские регулирующие органы принимать контрмеры, если иностранные правительства дискриминируют или иным образом ограничивают китайские предприятия в отношении инвестиций или ведения торговой деятельности в секторах, связанных с данными. Прямое включение мер торговой политики в китайский Закон о защите данных окажет существенное влияние на деятельность многонациональных компаний, ведущих бизнес в Китае. В последние годы в Китае наблюдаются стремительные изменения в регулировании защиты данных, хотя по-прежнему отсутствует всеобъемлющий межотраслевой закон о защите данных. В настоящее время имеется сочетание отраслевых законов, законов о защите прав потребителей и законов о кибербезопасности для регулирования обработки данных, дополненных рядом необязательных национальных стандартов. Нарушения конфиденциальности остаются широко распространенным явлением в массивной и все более развивающейся экономике Китая. Новые законопроекты представляют собой попытку унификации и систематизации законодательства КНР по вопросам защиты данных и кибербезопасности.

В Индии нет специального закона о кибербезопасности. Однако Закон об информационных технологиях 2000 года (Information Technology Act, 2000)[5] вместе с правилами и положениями, сформулированными в нем, касается кибербезопасности и связанных с ней киберпреступлений. Закон не только обеспечивает юридическое признание и защиту транзакций, осуществляемых посредством электронного обмена данными и других средств электронной связи, но также содержит положения, направленные на защиту электронных данных, информации или записей, а также предотвращение несанкционированного или незаконного использования компьютерных систем. Этот закон принят в целях обеспечения юридического признания транзакций, осуществляемых посредством электронного обмена данными и других средств электронной связи, обычно называемых электронными методами связи и хранения информации, для облегчения электронной подачи документов в государственные органы, а также для внесения поправок в Уголовный кодекс Индии, Закон о свидетельских показаниях Индии 1872 г., Закон о доказательствах банковских книг 1891 г. и Закон о Резервном банке Индии 1934 г. Некоторые из преступлений в области кибербезопасности предусмотрены Законом об информационных технологиях, включая взлом сети, атаки типа «отказ в обслуживании», фишинг, атаки вредоносного ПО, мошенничество с идентификационными данными и кража электронных средств.

Закон об информационных технологиях 2000 г. направлен прежде всего на создание правовой основы, обеспечивающей юридическую неприкосновенность всех электронных записей и других видов деятельности, осуществляемых с помощью электронных средств. В этом Законе также говорится, что, если не согласовано иное, заключение контракта может быть выполнено с помощью электронных средств связи, имеет юридическую силу и возможность судебной защиты. Указанный закон направлен на облегчение электронного взаимодействия в торговле и коммерции, устранение барьеров и препятствий на пути электронной торговли, возникающих в результате большой неопределенности, связанной с требованиями к тексту и электронной подписи в Интернете. Закон также направлен на выполнение своих задач по продвижению и развитию правовой и деловой инфраструктуры, необходимой для осуществления электронной торговли, использовании электронных подписей.

Другие законы, содержащие положения, связанные с кибербезопасностью, включают Уголовный кодекс Индии (1860 г.), который предусматривает наказание за правонарушения, в том числе совершенные в киберпространстве (такие как клевета, обман, криминальное преследование и непристойность). В соответствии с Законом о компаниях 2013 г. предусмотрена обязанность компаний обеспечить безопасность электронных записей и систем безопасности от несанкционированного доступа и взлома корпоративных электронных сетей. В Индии существуют также отраслевые нормативные акты, изданные национальными регулирующими органами — Резервным банком Индии, Департаментом телекоммуникаций и Департаментом ценных бумаг. В соответствии с Законом о регулировании и развитии страхования Индии 1999 г. Биржевой совет Индии устанавливает требования о соблюдении стандартов кибербезопасности регулируемыми организациями (банки, страховые компании, поставщики телекоммуникационных услуг и зарегистрированные на бирже организации).

В 2019 году в Парламент Индии внесен законопроект о защите личных данных (*Personal Data Protection Bill,* PDP)[6], чтобы полностью пересмотреть текущий режим защиты данных в Индии, который в настоящее время регулируется Законом об информационных технологиях 2000 г. Текущий проект закона PDP предусматривает единые требования соответствия для всех форм персональных данных, расширяет права, предоставляемые отдельным лицам, создает центральный регулятор защиты данных, а также устанавливает требования к локализации данных для определенных форм конфиденциальных данных. Законопроект PDP применяется экстратерриториально к неиндийским организациям в случае выполнения определенных требований взаимосвязи, а также налагает серьезные финансовые санкции в случае нарушений норм закона.

В ЮАР с 1 июля 2021 года вступает в силу всеобъемлющий закон Южной Африки — Закон о защите личной информации (Protection of Personal Information Act 2013 г., POPIA)[7] для реализации конституционных прав граждан Южной Африки на неприкосновенность частной жизни. POPIA предусматривает общий механизм защиты информации, применимый к организациям как

[5] URL: http://www.indiacode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf .

[6] URL: http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf .

[7] URL: http://popia.co.za/ .

в государственном, так и в частном секторе. Подобно Директиве ЕС о защите данных 95/46/EC, POPIA устанавливает восемь условий для законной обработки данных. Этими условиями являются:
(1) подотчетность,
(2) ограничение обработки,
(3) спецификация цели,
(4) дальнейшее ограничение обработки,
(5) качество информации,
(6) открытость,
(7) гарантии безопасности,
(8) участие субъекта данных.

POPIA применяется к обработке личной информации, внесенной в запись, ответственной стороной, которая обрабатывает информацию в Южной Африке и имеет домицилий в Южной Африке или находится в другом месте, но использует автоматизированные или неавтоматические средства в Южной Африке для обработки персональных данных. POPIA обычно применяется к «ответственным сторонам» (т. е. к основным обработчикам персональных данных, которые определяют цель и средства обработки), а ограниченные обязательства также распространяются на «операторов» (обработчиков данных).

POPIA содержит открытое определение «персональной информации», которое обычно означает информацию, относящуюся к идентифицируемому живому физическому лицу и, где это применимо, идентифицируемой компании или другому аналогичному юридическому лицу. Определение включает информацию, относящуюся к партнерствам и некорпоративным лицам, и предоставляет подробный перечень примеров персональной информации, включая информацию о частной переписке и о возрасте, поле и расе, идентификаторов, таких как идентификационные номера, номера телефонов, информация о местоположении, онлайн-идентификаторы, а также личные мнения и предпочтения.

В соответствии с POPIA ответственная сторона, обрабатывающая личную информацию, должна соблюдать все восемь условий и принимать меры, необходимые для выполнения этих условий. Соответствие должно быть достигнуто не только при фактической обработке информации, но также при определении цели и средств обработки личной информации.

В Бразилии общим Законом о защите данных (*Lei Geral de Proteção de Dados Pessoais*, LGPD)[8], который вступил в силу в августе 2020 года, устанавливается порядок сбора, обработки, использования, защиты и уничтожения персональных данных. LGPD также предусматривает девять основных прав, которые дают субъектам данных бóльший контроль над своими данными и способами их использования, а также штрафы за нарушение закона. Ранее в Бразилии действовало более 40 различных законов о персональных данных, которые теперь упразднены и объединены в единую правовую базу LGPD.

Формирование нового законодательства стран БРИКС во многом происходит под влиянием европейского законодательства (Общий регламент защиты данных (GDPR) и др.) и правоприменительной практики. В частности, значительным событием в области глобального законодательства о защите данных стало решение Суда Европейского Союза (Court of Justice of the EU, CJEU) в деле, широко известном как «Schrems II» (CJEU judgement of 16 July 2020, *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems,* case C-311/18)[9], в котором Суд ЕС признал недействительным ранее принятую Европейской комиссией Рамочную программу защиты конфиденциальности между ЕС и США (EU-US Privacy Shield Framework), которая заменила предыдущее соглашение (Safe Habor) и которая разрешала бесплатную передачу персональной информации любым государствам — членам Европейского Союза или Европейской экономической зоны в соответствии с GDPR из ЕС в США, на том основании, что Privacy Shield Framework не защищает права граждан ЕС в соответствии с законами ЕС. Тем не менее это не отменяет использование утвержденных ЕС договорных положений, которые устанавливают стандарты защиты для передачи личной информации, известные как стандартные договорные положения (SCC). Новая судебная практика ЕС должна быть учтена при применении законов о защите персональных данных странами БРИКС и передаче персональных данных.

Вместе с тем непрерывный доступ к любой информации существует практически по всем вопросам в постоянно взаимосвязанном мире, а личная и корпоративная информация легко доступна в Интернете с использованием технологических платформ. Информация является важнейшим элементом власти, обладание ей позволяет получить преимущества в принятии решений, обеспечении кибербезопасности и отражении киберугроз. Как отмечают эксперты [12], киберпространство включает сложные и динамичные технологические инновации, для которых существующая правовая система не всегда подходит. Проблемой является отсутствие всеобъемлющих договоров, способствующих международному сотрудничеству в области киберзащиты. В результате многие страны не будут должным образом подготовлены или адекватно защищены законодательством в случае кибератаки на национальном уровне.

Пандемия COVID-19 сформировала новые вызовы, которым должно соответствовать национальное законодательство в области защиты персональных данных и кибербезопасности, а также международно-правовые акты в этой сфере. Перспективы развития законодательства и всей системы права должны основываться на принципах всеобъемлющей защиты прав и законных интересов личности, создания эффективной киберзащиты персональных данных и значимой информации в национальных интересах суверенных стран. ■

[8] URL: https://gdpr.eu/gdpr-vs-lgpd/?cn-reloaded=1 .

[9] URL: https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation .

Литература

1. Future Series: Cybersecurity, emerging technology and systemic risk. Insight report, November 2020. World Economic Forum. URL: http://www.weforum.org .
2. Strategic Assessment 2020. Into a New Era of Great Power Competition / Edited by Thomas F. Lynch III. Institute for National Strategic Studies, National Defense University, Washington, D.C., 2020, p. xvi, 139-140 et al.
3. Pallavi Khanna. State Sovereignty and Self-Defence in Cyberspace. BRICS Law Journal, Volume V (2018), Issue 4, p. 140-157. DOI: 10.21684/2412-2343-2018-5-4-139-154 .
4. Cyberspace Regulation and the Discourse of State Sovereignty, 112 Harvard Law Review 1680, 1685 (1999), Nov. 10, 2018. URL: http://cyber.law.harvard.edu/property00/jurisdiction/hlr.html .
5. Карцхия А.А. Новые элементы национальной безопасности: национальный и международный аспект // Вопросы кибербезопасности. 2020. № 6 (40). С. 72—82.
6. Карцхия А.А. Тенденции развития правовых институтов под влиянием пандемии: российский и зарубежный опыт // Мониторинг правоприменения. 2021. № 2. С. 10—15.
7. Communication from the Commission to the European Parliament and the Council "Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition—two years of application of the General Data Protection Regulation", 24/06/2020. URL: http://ec.europa.eu/info/law/law-topic/data-protection/communication-two-years-application-general-data-protection-regulation_en .
8. Luca Belli. A Multidimensional Approach to Cybersecurity for the BRICS // CyberBRICS: Cybersecurity Regulations in the BRICS Countries, p.15-17, URL: http://www.cyberbrics.info .
9. Защита данных: научно-практический комментарий к судебной практике / Э.В. Алимов, Д.Р. Алимова, Х.И. Гаджиев и др.; отв. ред. В.В. Лазарев, Х.И. Гаджиев. М. : ИЗиСП, КОНТРАКТ, 2020.
10. URL: http://russian.people.com.cn/n3/2021/0309/c31521-9826811.html.
11. CyberBRICS: Cybersecurity Regulations in the BRICS Countries, URL: http://www.cyberbrics.info .
12. Marthie Grobler, Joey Jansen van Vuuren (2012). Collaboration as proactive measure against cyber warfare in South Africa, African Security Review, 21:2, p. 61-73. DOI: 10.1080/10246029.2012.654803

***Рецензент: Захарцев Сергей Иванович**, доктор юридических наук, академик РАЕН, заведующий кафедрой адвокатуры и правоохранительной деятельности Российского государственного социального университета, г. Москва, Российская Федерация.*

E-mail: sergeyivz@yandex.ru