УДК 351.862.67:004.56(510)

DOI dx.doi.org/10.24866/1813-3274/2020-1/118-130

Д. В. Лобач¹

Владивостокский государственный университет экономики и сервиса,
г. Владивосток, Россия

E-mail: dimaved85@mail.ru

Е. А. Смирнова²

Дальневосточный федеральный университет, г. Владивосток, Россия

E-mail: smirnova.ea@dvfu.ru

ПОЛИТИКО-ПРАВОВЫЕ МЕРЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ В КИТАЙСКОЙ НАРОДНОЙ РЕСПУБЛИКЕ НА СОВРЕМЕННОМ ЭТАПЕ*

Аннотация. В статье анализируется китайский опыт обеспечения кибербезопасности за последние 20 лет. Отмечается, что за два прошедших десятилетия Китайская Народная Республика предприняла ряд последовательных шагов политико-правового характера в направлении обеспечения кибербезопасности в условиях новых и нарождающихся угроз. Особое внимание в контексте изучения правового механизма обеспечения кибербезопасности уделено изучению специальных нормативных положений Закона КНР о борьбе с терроризмом от 1 января 2016 г. и Закона о кибербезопасности КНР от 7 ноября 2016 г. Закон КНР о борьбе с терроризмом регламентирует ряд специальных мер, направленных на ограничение прав и свобод, связанных с получением и распространением информации определённого содержания. В частности, это проявляется в установлении запрета на распространение

¹ Дмитрий Владимирович Лобач, кандидат юридических наук, доцент кафедры теории и истории российского и зарубежного права Института права Владивостокского государственного университета экономики и сервиса, г. Владивосток, Россия.

² Евгения Александровна Смирнова, кандидат юридических наук, старший преподаватель кафедры трудового и экологического права Юридической школы Дальневосточного федерального университета, г. Владивосток, Россия.

Для цитирования: Лобач Д. В., Смирнова Е. А. Политико-правовые меры обеспечения кибербезопасности в Китайской Народной Республике на современном этапе // Азиатско-Тихоокеанский регион: экономика, политика, право. 2020. № 1. С. 118–130.

* Работа выполнена при финансовой поддержке Гранта Президента РФ № НШ-2668-2020.6 «Национально-культурные и цифровые тренды социально-экономического и политико-правового развития Российской Федерации в XXI веке».

взглядов и идей, которые противоречат официальной позиции властей во время чрезвычайной ситуации, и контроля над интернетом, радио и телекоммуникациями в условиях ликвидации последствий совершённого террористического акта. Закон о кибербезопасности КНР регламентирует общие обязательства для трёх категорий субъектов, к которым предъявляются особые требования по обеспечению информационной безопасности. К таковым субъектам относятся сетевые операторы (network operators), операторы критически важной информационной инфраструктуры (critical information infrastructure operators, CII Operators) и поставщики сетевых продуктов и услуг. В статье отмечается, что КНР проводит также политику в установлении и совершенствовании стандартов сетевой безопасности, которые представляют собой минимальные требования к качеству защищённости шифрования, персональных данных, важной информации, безопасных и контролируемых продуктов и услуг, многоуровневых схем безопасности, объектов критически важной информационной инфраструктуры и трансграничной передачи данных. Обосновывается вывод о том, что, хотя КНР и предприняла последовательные шаги в политико-правовом обеспечении кибербезопасности, однако в законе имеются положения, вызывающие нарекания с позиции несовершенства юридической техники и вероятного ущемления интересов третьих лиц.

Ключевые слова: терроризм, киберугроза, кибертерроризм, кибербезопасность, безопасность, Китайская Народная Республика, борьба с терроризмом, закон о кибербезопасности, Азиатско-Тихоокеанский регион, информационная безопасность, информационное общество.

D. V. Lobach¹

Vladivostok State University of Economics and Service, Vladivostok, Russia
E-mail: dimaved85@mail.ru

E. A. Smirnova²

Far Eastern Federal University, Vladivostok, Russia
E-mail: smirnova.ea@dvfu.ru

LEGAL POLICY MEASURES FOR CYBER SECURITY IN PEOPLE'S REPUBLIC OF CHINA AT THE PRESENT STAGE

Abstract. The article analyzed the Chinese experience in ensuring cybersecurity over the past 20 years. Over the past two decades, the People's Republic of China (PRC) has taken a number of successive political and legal steps towards ensuring cybersecurity in the face of new and emerging threats. Particular attention has been focused on the study of special regulations of the Suppression of Terrorism Law of the PRC of January 1, 2016 and the Cybersecurity Law of the PRC of November 7, 2016. The Suppression of Terrorism Law of the PRC regulates a number of special measures aimed at restriction of rights and freedoms associated with the receipt and dissemination of information of a certain content. In particular, this is manifested in the establishment of a ban on the dissemination of views and ideas that contradict the official position of the authorities during an emergency, and control over the Internet, radio and telecommunications in the context of eliminating the consequences of a terrorist act. The Cybersecurity Law of the PRC regulates general obligations for three categories of entities, which are required to meet special requirements for ensuring information security. These entities include network operators, critical information infrastructure operators (CII Operators), and network product and service providers. The article has noted that the PRC is also pursuing a policy of establishing and improving network security standards, which are the minimum requirements for the quality of encryption security, personal data, important information, safe and controlled products and services, multi-level security schemes, objects of critical information infrastructure and cross-border data transfer.

¹ Dmitry V. Lobach, Candidate of Sciences (Law), Associate Professor, Department of Theory and History of Russian and Foreign Law, Institute of Law, Vladivostok State University of Economics and Service, Vladivostok, Russia.

² Evgenia A. Smirnova, Candidate of Sciences (Law), Senior Lecturer, Department of Labor and Environmental Law, Law School, Far Eastern Federal University, Vladivostok, Russia.

For citing: Lobach D. V., Smirnova E. A. Legal policy measures for cyber security in People's Republic of China at the present stage // PACIFIC RIM: Economics, Politics, Law. 2020. No 4. P. 118–130.

The conclusion is substantiated that, although the PRC has taken successive steps in providing political and legal support for cybersecurity, the law contains provisions that cause criticism from the point of view of imperfection of legal technology and the possible infringement of the interests of third parties.

Keywords: terrorism, cyberthreat, cyberterrorism, cybersecurity, security, Republic of China, the fight against terrorism, the law on cybersecurity, Asia-Pacific region, information security, information society.

Кибербезопасность представляет собой широкий термин, охватывающий меры, принимаемые государственными и частными организациями, которые направлены на обеспечение безопасности онлайн-коммуникаций и информационных ресурсов. В контексте больших данных кибербезопасность охватывает аппаратные средства, технологии шифрования, программное обеспечение и индивидуальные навыки, используемые с целью снижения рисков, возникающих в результате онлайн-передачи и хранения данных [1]. Кибербезопасность, будучи необходимым условием развития информационного общества, также принято определять как совокупность стратегий и действий, которые должны быть предприняты для защиты соединённых сетей (включая аппаратные и программные средства, массивы информации) от несанкционированного доступа, изменения, кражи, уничтожения, блокирования и других противоправных действий при гарантии адекватного качества безопасности несмотря на изменяющийся характер киберугроз [2, с. 49]. В свою очередь, кибербезопасность как состояние защищённости информационно-коммуникационных отношений, связанных с онлайн-передачей, хранением, преобразованием и использованием данных, целесообразно рассматривать через актуальные угрозы, которые в своём проявлении наносят вред частным и публичным интересам в информационно-коммуникационной среде. В современных условиях информационно-технологического прогресса актуальные угрозы, посягающие на объекты телекоммуникационной инфраструктуры, компьютеры, каналы передачи данных, приложения, приводящие к определённым негативным последствиям (например, порча веб-сайтов, кража личных данных, нанесение вреда компьютерам и компьютерным системам, несанкционированное списание денежных средств, вымогательство под угрозой уничтожения приватной информации, компрометация конфиденциальных операционных данных), представлены большим разнообразием вредоносных программ (компьютерные вирусы, черви, троянские программы, фишинг, клавиатурный шпион, вредоносный код и др.), которые эволюционируют сообразно с релевантным развитием информационных технологий, знаний и навыков, которые используются в целях обеспечения кибербезопасности. При этом необходимо понимать, что в субъектном плане современные угрозы для кибербезопасности носят дифференцированный характер, поскольку акторами (за-

казчиками и исполнителями) кибератак могут быть инсайдеры и белые воротнички в организациях, хакеры, действующие на самостоятельной основе или в форме преступной кооперации, преступные синдикаты, террористы, а также агенты отдельных государств. Последние являются самой сложной категорией злоумышленников, которые при финансовой поддержке государств, имея достаточные технические ресурсы, выполняют сложные, продолжающиеся в течение длительного времени кибератаки в целях проникновения или установления контроля над целевыми системами [3, p. 350].

Учитывая тот факт, что кибербезопасность в современном мире становится имманентным условием для развития информационного общества, а также неотъемлемой частью в системе национальной безопасности многих государств, следует признать коррелирующую связь между состоянием кибербезопасности на национальном уровне и характером, масштабами и темпами развития властно-публичного управления и экономических отношений в обществе. В этом плане обращает на себя внимание опыт Китайской Народной Республики (далее по тексту – КНР) в части адекватного обеспечения национальной кибербезопасности относительно современных киберугроз, что обусловлено интенсивным развитием экономических, политических и социально-культурных отношений в этом государстве в современных условиях, которые связаны с революционными научно-технологическими процессами и новациями, предопределяющими трансформацию социальных структур.

За последние 20 лет КНР предприняла ряд последовательных шагов политико-правового характера в направлении обеспечения кибербезопасности в условиях новых и нарождающихся угроз, исходящих как от отдельных государств, так и от негосударственных акторов. Не претендуя на всеохватывающий анализ конкретных решений, предпринятых руководством КНР, остановимся на основных этапах в области обеспечения интересов национальной безопасности в киберпространстве.

Так, ещё в 2000 г. Всекитайским собранием народных представителей было принято постановление по защите интернет-пространства, где были обозначены те области, в которых могут осуществляться нарушения, что ознаменовало первую попытку со стороны государства классифицировать возможные информационные угрозы и впоследствии разработать меры по обеспечению безопасности в этой сфере. В 2003 г. Канцелярия Центрального комитета Коммунистической партии Китая опубликовала Постановление государственной информатизированной руководящей группы по работе в области укрепления информационной безопасности. Документ закреплял за ответственными лицами обязанность по совершенствованию защиты важной и стратегической инфраструктуры, проведению мониторинга интернет-пространства на наличие возможных угроз для государства, а также предусматривал разработку мер для привлечения квалифицированных специалистов в области информационной безопасности [4, p. 158].

В 2006 г. была принята Государственная стратегия по развитию информатизации на период с 2006 по 2020 гг. В данном документе особое внимание обращено на значение информационных технологий для китайского общества [5]. Отмечается, что проблемы информационной безопасности остаются довольно заметными: на глобальном уровне компьютерные вирусы, онлайн-атаки, нежелательная почта, утечки в системе, кражи секретов в Интернете, ложная и вредная информация, онлайн-преступления и другие подобные проблемы становятся всё более заметными с каждым днём, если они не будут должным образом решены, они могут оказать пагубное влияние на экономическое и социальное развитие страны, а также на национальную безопасность. Кроме того, в документе определены стратегические направления развития информатизации в стране (в частности, информатизация национальной экономики, электронное правительство, создание развитой сетевой культуры, содействие социальной информатизации, создание комплексной информационной инфраструктуры, повышение конкурентоспособности информационной индустрии, создание национальной системы защиты информационной безопасности, повышение способности граждан использовать информационные технологии), стратегические планы развития информатизации в стране (в частности, планы электронной коммерции, планы обучения и подготовки граждан в области информационных связей, планы развития электронного правительства, планы эксплуатации и использования сетевых информационных ресурсов и планы по сокращению цифрового разрыва), обеспечительные меры (в частности, научные исследования в области информатизации и политических систем, меры финансового обеспечения, разработка специальных норм и технических стандартов, оптимизация управления интернетом, кадровое обеспечение, международное сотрудничество в области информатизации и др.).

Среди стратегических направлений информатизации в КНР особое внимание уделяется созданию национальной системы защиты информационной безопасности. В рамках обозначенного направления было заявлено о необходимости усиления национального потенциала защиты информации. Постановка данной цели предполагает решение ряда задач, связанных с отслеживанием, исследованием и освоением передовых теорий, новаторских технологий и тенденций развития в области международной информационной безопасности, а также с внимательным изучением практики обнаружения информационных угроз (обнаружение и исследование утечек и бэкдоров в технологиях и продуктах информационной безопасности) и основных технологий безопасности. Кроме того, возникает необходимость повышать потенциал основных средств и оборудования, стимулировать местное развитие технологий информационной безопасности. В целом и общем декларируется и продвигается идея создания информационной площадки для социализма с китайской спецификой, при которой будут обеспечены национальная кибербезопасность от внешних и внутренних угроз и суверенный интернет.

Противодействие киберугрозам также охватывается специальным законом КНР о борьбе с терроризмом, принятым 1 января 2016 г. Указанный закон регламентирует ряд специальных мер, направленных на ограничение прав и свобод, связанных с получением и распространением информации определённого содержания. В частности, это проявляется в установлении запрета на распространение взглядов и идей, которые противоречат официальной информации властей, во время чрезвычайной ситуации и контроля над интернетом, радио и телекоммуникациями в условиях ликвидации последствий совершённого террористического акта. Закон также ввёл государственную цензуру в сети Интернет посредством возложения на операторов связи и поставщиков услуг обязанностей по реализации системы мониторинга информационного контента с последующим сообщением специальным органам власти о такой информации в случае её обнаружения. Кроме того, закон также закрепляет за специальными органами власти полномочия по принятию технических мер по недопущению трансграничного распространения информации террористического или экстремистского характера в сети Интернет. При этом в отношении операторов связи и интернет-провайдеров законодательно установлены требования постоянного обеспечения китайских правоохранительных органов бэкдорами (специально созданный разработчиком дефект алгоритма, который позволяет получить несанкционированный доступ к данным или удалённому управлению операционной системой и компьютером в целом), а также получение одобрения на принятие новых криптографических решений [6].

Особое значение для национальной кибербезопасности страны играет Закон о кибербезопасности КНР (известный также как китайский Закон об интернет-безопасности), принятый Постоянным комитетом Всекитайского собрания народных представителей 7 ноября 2016 г. и вступивший в силу 1 июня 2017 г. [7].

Рассматриваемый нормативно-правовой акт был принят для того, чтобы обеспечить сетевую безопасность, защитить суверенитет в киберпространстве, национальную безопасность и публичные интересы, права и интересы граждан, юридических лиц, а также содействовать здоровому развитию экономической и социальной информатизации. Предметная сфера закона охватывает создание, эксплуатацию, обслуживание и использование компьютерных сетей, а также надзор и управление безопасностью сетей на материковой территории КНР.

Правовой анализ рассматриваемого закона позволяет отметить основные новации, направленные на противодействие угрозам, которые могут подрывать национальный суверенитет в киберпространстве КНР.

Прежде всего в законе установлены общие обязательства для трёх категорий субъектов, к которым предъявляются особые требования по обеспечению информационной безопасности. К таковым субъектам относятся сетевые операторы (network operators), операторы критически важной информационной инфраструкту-

ры (critical information infrastructure operators, CII Operators) и поставщики сетевых продуктов и услуг. Сетевые операторы определяются как субъекты, которые владеют и управляют сетями или которые предоставляют сетевые услуги связи. Операторы критически важной информационной инфраструктуры (далее по тексту – операторы КИИ) являются разновидностью сетевых операторов, которые управляют объектами критически важной информационной инфраструктуры. К таковым операторам относят предприятия, которые осуществляют свою деятельность в сфере общественных коммуникаций, энергетики, транспорта, водоснабжения, финансов, государственной службы и электронного правительства. Другие компании также могут считаться операторами КИИ, если они имеют информационную инфраструктуру, составляющую основу национальной безопасности и экономики и обеспечивающую общественные интересы.

Общие обязанности в отношении вышеперечисленных субъектов закреплены в ст. ст. 21, 24, 25, 26, 28, 42 и 47 Закона о кибербезопасности КНР и охватывают требования по разработке внутренних правил управления безопасностью и операционных процедур; определению лиц, ответственных за кибербезопасность; внедрению технических мер для предотвращения кибератак; классификации собранных данных; резервному копированию и шифрованию всех важных данных; составлению специальных планов аварийного реагирования для инцидентов; принятию мер по сообщению об инцидентах в соответствующие отделы; своевременному устранению системных ошибок, компьютерных вирусов, сетевых атак, сетевых вторжений и других угроз безопасности; обеспечению технической поддержки и помощи органам общественной и национальной безопасности в целях обеспечения государственной безопасности и расследования преступлений; соблюдению соответствующих законов и правил при проведении аутентификации, тестировании и оценке рисков кибербезопасности; истребованию от пользователей предоставления достоверной идентификационной информации; уведомлению общественности об актуальных угрозах в сфере кибербезопасности (системные ошибки, компьютерные вирусы, сетевые атаки, сетевое вторжение); прекращению распространения информации, запрещённой законом или применяемыми правилами, а также принятию необходимых мер для обработки или удаления незаконной информации; принятию любых других мер, требуемых законом о кибербезопасности для защиты информации пользователей, и выполнению других обязанностей в соответствии с законом и административными регламентами.

Кроме того предъявляются и специальные требования как к операторам критически важной информационной инфраструктуры (операторы КИИ), так и к поставщикам сетевых продуктов и услуг.

В отношении операторов КИИ предъявлены дополнительные обязанности (ст. ст. 34–38 Закона кибербезопасности КНР), касающиеся: а) создания специаль-

ных органов управления безопасностью и проведения проверок в отношении лиц, занимающих ключевые должности, а равно отвечающих за управление безопасностью; б) обучения в области кибербезопасности, обеспечения технической поддержки и проведения на периодической основе оценки навыков сотрудников в обозначенной области; в) создания резервных копий для аварийного восстановления важных систем и базы данных; г) составления планов аварийного реагирования на инциденты и проведения учений на периодической основе; д) заключения соглашений о безопасности и конфиденциальности с сетевыми провайдерами для того, чтобы определить обязанности и ответственность при покупке сетевых продуктов или услуг; е) проведения постоянного мониторинга в целях определения рисков ухудшения состояния кибербезопасности с последующим представлением отчетов и предложений по улучшению работы отделов, отвечающих за охрану безопасности объектов критической информационной инфраструктуры.

В свою очередь, поставщики сетевых продуктов и услуг должны соблюдать обязательные нормативные требования. В частности, закон устанавливает запрет на установление вредоносных программ и возлагает на данных субъектов обязанности в принятии мер, направленных на информирование пользователей и уполномоченных структур об обнаружении в их продуктах и услугах недостатков и уязвимостей в сфере безопасности. Закон о кибербезопасности предусматривает обязательную сертификацию критического сетевого оборудования (маршрутизаторы, коммутаторы, PLC оборудование, телекоммуникационные стойки) и 11 специализированных продуктов кибербезопасности.

Нельзя не отметить и политику государства в установлении и совершенствовании стандартов сетевой безопасности. Так, в ст. 15 Закона о кибербезопасности КНР регламентирует, что административный департамент Государственного совета КНР по стандартизации и другие ведомства Государственного совета КНР исходя из своих предметных обязанностей принимают участие в организации разработки и своевременном пересмотре соответствующих национальных и отраслевых стандартов для управления сетевой безопасностью, а также для безопасности сетевых продуктов, услуг и операций. В самом общем виде стандарты охватывают минимальные требования к качеству защищенности шифрования, персональных данных, важной информации, безопасных и контролируемых продуктов и услуг, многоуровневых схем безопасности, объектов критически важной информационной инфраструктуры и трансграничной передаче данных [8].

Отдельно следует отметить меры административного реагирования в отношении специальных субъектов, ответственных за соблюдение требований Закона о кибербезопасности. Анализ ст. ст. 59–75 данного закона позволяет констатировать, что в зависимости от характера правонарушения предусмотрены дифференцированные меры административного реагирования: наложение обязанности на право-

нарушителя по принятию корректирующих мер, предупреждение, конфискация незаконных доходов, штрафы, приостановление операций, закрытие сайта, отзыв лицензии, арест. Кроме того, в соответствии со ст. 58 Закона о кибербезопасности за Государственным советом КНР и соответствующими органами власти провинций, автономных районов и муниципалитетов с одобрения Государственного совета закреплены полномочия по принятию временных мер в отношении сетевых коммуникаций в отдельных регионах. В сущности, закон закрепляет широкие полномочия за соответствующими надзирающими органами власти без должной их конкретизации. В специальной литературе отмечается, что в практическом аспекте такие полномочия могут быть связаны, например, с временным ограничением коммуникаций в сети Интернет, или же предполагается установление контроля над работой в сети определенных лиц [9].

Между тем следует отметить, что принятие Закона о кибербезопасности в целом является важной вехой в обеспечении состояния защищенности онлайн-коммуникаций и информационных ресурсов от современных и нарождающихся киберугроз, что является необходимым условием развития информационного общества и эффективного управления. Однако нельзя не признать и ряд аспектов, вызывающих нарекания с позиции вероятностей ущемления интересов третьих лиц. Прежде всего отдельные нормативные положения, регламентирующие возможность обращения с запросом о предоставлении исходного кода, алгоритма шифрования или другой важной информации для рассмотрения властями, создают риски потери этой информации, использования самими властями или передачи её конкурентам. Другое положение (ст. 28) требует, чтобы операторы сетей оказывали техническую поддержку органам государственной безопасности во время осуществления правомерных действий по обеспечению национальной безопасности и проведения уголовных расследований. Представляется, что такое требование предопределяет обеспокоенность в связи с тем, что иностранным технологическим компаниям, возможно, придется раскрыть интеллектуальную собственность или предоставить правительству доступ к бэкдору, чтобы продолжать вести бизнес в стране.

С критической стороны оценивается данный закон и в том плане, что для обеспечения локализации данных иностранные фирмы должны будут либо инвестировать средства в новые серверы данных в Китае, которые будут подвергаться государственным выборочным проверкам, либо нести новые расходы, чтобы нанять местного поставщика серверов (например, Huawei, Tencent или Alibaba), которые в последние годы затратили миллиарды на создание внутренних центров обработки данных. Значительные инвестиции этих китайских технологических компаний в последние годы являются одной из причин, по которой критики нового закона считают, что он частично призван укрепить внутреннюю китайскую индустрию управления данными и телекоммуникаций против глобальных конкурентов [10].

Многие нормы с позиции юридической техники носят абстрактный характер, что объясняется контекстной неопределённостью юридических предписаний и используемых терминов. Например, ст. 9 Закона о кибербезопасности регламентирует, что операторы сетей помимо соблюдения законов и административных правил должны следовать социальным нормам и соблюдать коммерческую этику, а также быть честными и заслуживающими доверие, выполнять обязательства по защите сетевой безопасности, принимать надзор со стороны правительства и общественности и нести социальную ответственность. Исходя из буквального прочтения данной нормы, становится совершенно не понятно, в чём собственно проявляется отличие законодательных и административных норм от социальных. В законе также отсутствует и какое-либо внятное определение социальной ответственности, при этом в главе 4 предусмотрены конкретные основания для привлечения субъектов к юридической ответственности. Сходным образом сформулирована правовая норма статьи 12 указанного закона, в которой, помимо прочего, закреплено, что любое лицо и организация, использующие сети, должны соблюдать законодательство, общественный порядок и уважать социальную мораль, а также они не должны ставить под угрозу безопасность сети и использовать сеть для осуществления деятельности, угрожающей национальной безопасности, национальной чести и интересам общества.

В заключение следует признать тот факт, что опыт Китая в обеспечении кибербезопасности охватывает последовательные шаги в направлении защиты национального суверенитета в киберпространстве, высшим проявлением чего стало принятие специального Закона о кибербезопасности в КНР. Среди положительных черт данного нормативного правового акта следует признать широкий характер регулятивного действия и наличие дифференцированного правового инструментария, используемого в целях обеспечения кибербезопасности. В то же время в законе также присутствуют нормы, вызывающие нарекания как в плане наличия дефектов юридической техники изложения нормативного материала, так и с позиции вероятного ущемления интересов третьих лиц. Подобные нормы в совокупности с расширенным пониманием общественного интереса и национальной безопасности предопределяют возможные риски вмешательства органов власти в информационно-коммуникационную инфраструктуру частных лиц и организаций, а равно проведение в их отношении расследования исходя из политических конъюнктурных соображений.

Список литературы

1. Encyclopedia of Big Data / ed. by L. A. Schintler, C. L. McNeely. – Springer International Publishing AG, 2018. – URL: https://link.springer.com/content/pdf/10.1007%2F978-3-319-32001-4_53-1.pdf (дата обращения: 20.02.2020).
2. Фалеев, М. И. Кибербезопасность – неотъемлемый элемент современной государственной политики в области национальной безопасности / М. И. Фалеев,

С. Ю. Сардановский // Стратегия гражданской защиты: проблемы и исследования. – 2016. – Т. 6, № 1 (10). – С. 48–54.

3. Borky, J. M. *Effective Model-Based Systems Engineering* / J. M. Borky, T. H. Bradley. – New York City : Springer International Publishing AG; part of Springer Nature, 2019. – 531 p.

4. Разумов, Е. А. Политика КНР по обеспечению кибербезопасности // Россия и АТР. – 2017. – № 4 (98). – С. 156–170.

5. 2006–2020 National informatization Development Strategy // China Copyright and Media. – URL: <https://chinacopyrightandmedia.wordpress.com/2006/03/19/2006-2020-national-informatization-development-strategy/> (дата обращения: 20.02.2020).

6. China's new counter-terrorism law: implications and dangers for Tibetans and Uyghurs: a join report by the international campaign for Tibet and find. November 2016. – URL: <https://www.refworld.org/docid/582b119b4.html> (дата обращения: 20.02.2020).

7. Cybersecurity Law of the People's Republic of China (Draft) (Second Draft) // The American Chamber of Commerce in the People's Republic of China (AmCham China). – URL: <https://www.amchamchina.org/uploads/media/default/0001/05/b78e2db2b147c09b8430b6bd55f81bc8299ea50f.pdf> (дата обращения: 20.02.2020).

8. How Chinese cybersecurity standards impact doing business in China // The Center for Strategic and International Studies (CSIS). – URL: <https://www.csis.org/analysis/how-chinese-cybersecurity-standards-impact-doing-business-china> (дата обращения: 20.02.2020).

9. Implementing China's Cybersecurity Law. August 2017. – URL: <https://www.jonesday.com/files/upload/Implementing%20Chinas%20Cybersecurity%20Law.pdf> (дата обращения: 20.02.2020).

10. Wagner, J. China's Cybersecurity Law: what you need to know. The law, which comes into effect June 1, raises data protection concerns for foreign firms. // The Diplomat. – URL: <https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/> (дата обращения: 20.02.2020).

References

1. Schintler L. A., McNeely C. L., eds. *Encyclopedia of Big Data*. Springer International Publishing AG. 2018. Available at: https://link.springer.com/content/pdf/10.1007%2F978-3-319-32001-4_53-1.pdf (accessed 20 February 2020).

2. Faleev M. I., Sardanovsky S. U. Kiberbezopasnost' – neot'emlemyi element sovremennoi gosudarstvennoi politiki v oblasti natsional'noi bezopasnosti [Cybersecurity – an integral element of modern state policy in the field of national security]. *Strategiya grazhdanskoi zashchity: problemy i issledovaniya*, 2016, vol. 6, no. 1 (10), pp. 48–54.

3. Borky J. M., Bradley T. H. *Effective Model-Based Systems Engineering*. New York City: Springer International Publishing AG, part of Springer Nature, 2019. 531 p.
4. Razumov E. A. Politika KNR po obespecheniyu kiberbezopasnosti [China's cyber security policy]. *Rossiya i ATR*, 2017, no. 4 (98), pp. 156–170.
5. *2006–2020 National Informatization Development Strategy*. China Copyright and Media. Available at: <https://chinacopyrightandmedia.wordpress.com/2006/03/19/2006-2020-national-informatization-development-strategy/> (accessed 20 February 2020).
6. *China's new counter-terrorism law: implications and dangers for Tibetans and Uyghurs: a join report by the international campaign for Tibet and find*. November 2016. Available at: <https://www.refworld.org/docid/582b119b4.html> (accessed 20 February 2020).
7. *Cybersecurity Law of the People's Republic of China (Draft) (Second Draft)*. The American Chamber of Commerce in the People's Republic of China (AmCham China). Available at: <https://www.amchamchina.org/uploads/media/default/0001/05/b78e2db2b147c09b8430b6bd55f81bc8299ea50f.pdf> (accessed 20 February 2020).
8. *How Chinese Cybersecurity Standards Impact Doing Business In China*. The Center for Strategic and International Studies (CSIS). Available at: <https://www.csis.org/analysis/how-chinese-cybersecurity-standards-impact-doing-business-china> (accessed 20 February 2020).
9. *Implementing China's Cybersecurity Law*. August 2017. Available at: <https://www.jonesday.com/files/upload/Implementing%20Chinas%20Cybersecurity%20Law.pdf> (accessed 20 February 2020).
10. Wagner J. *China's Cybersecurity Law: What You Need to Know. The law, which comes into effect June 1, raises data protection concerns for foreign firms*. The Diplomat. Available at: <https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/> (accessed 20 February 2020).