УДК 32.019,5
DOI: 10.21209/2227-9245-2022-28-1-124-139

СИСТЕМА ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КНР

THE SYSTEM OF COUNTERING INFORMATION SECURITY THREATS OF THE PEOPLE'S REPUBLIC OF CHINA

П. В. Меньшиков,
Московский государственный институт международных отношений (Университет) МИД России, г. Москва
p.menshikov@odin.mgimo.ru

P. Menshikov,
Moscow State Institute of International Relations of the Ministry of Foreign Affairs of Russia, Moscow

Л. К. Михина,
Московский государственный институт международных отношений (Университет) МИД России, г. Москва
mik-laura888@yandex.ru

L. Mikhina,
Moscow State Institute of International Relations of the Ministry of Foreign Affairs of Russia, Moscow

Без информационного суверенитета не может быть государственного суверенитета. Китайское правительство хорошо это понимает и за время пандемии COVID-19, когда весь мир перешел в онлайн, приняло несколько законов, призванных регулировать информационную политику страны в информационном и медиапространствах. В настоящий момент в Китае действует новое законодательство в области информационной безопасности. Важнейшими среди законов в информационной и кибер-сфере являются Закон «О безопасности данных», «О защите персональных данных», Закон «О киберпространстве», первые два из которых призваны дополнить и усовершенствовать применение Закона «О кибербезопасности» 2017 г. Однако их принятие повлекло за собой целый ряд проблем для китайских компаний и вызвало волну международной критики. *Актуальность исследования:* Китай – динамично развивающееся государство с уникальной формой правления, правоприменительной практикой, активно отстаивающее национальные интересы. Китай занимает одну из лидирующих позиций в международных политических и экономических процессах. Страна является одним из ведущих разработчиков в сфере IT и информационно-коммуникационных технологий. Именно поэтому необходимо изучать, отслеживать новые тенденции и государственные задачи этой страны. Кроме того, согласно Концепции внешней политики Российской Федерации[1], Россия и Китай наращивают всеобъемлющее равноправное доверительное партнерство и стратегическое взаимодействие. Законодательные органы России и Китая обмениваются правовой практикой. Оба государства обозначили стимулирование роста высоких технологий и развитие киберпространства стратегически важной целью для защиты своего суверенитета. Страны активно принимают новые законодательные акты с целью защиты и регулирования интернета, облачных хранилищ и Big Data. Однако правовой опыт Китая и России в этой сфере различается, в связи с чем необходимо анализировать особенности китайской практики в области информационного регулирования. *Объект исследования* – система китайского законодательства в области информационной политики и работа Правительства Китая в данной области. *Предмет исследования* – новые китайские законы в области информационного регулирования, в том числе регулирования интернет-пространства и кибер-сферы. В статье рассмотрены правительственные стратегии Китая для достижения результатов нового пятилетнего плана с целью воспроизводства общей картины и выявления методов противостояния Китая угрозам информационной безопасности. *Цель исследования* – научно обосновать систему противодействия угрозам информационной безопасности Китая. *Задачи исследования*: рассмотреть особенности китайского законодательства в информационной сфере, интернете и кибер-сети; выявить общие тренды дальнейшей разработки китайского законодательства в информационной среде; обозначить основные векторы развития информационной политики Китая на ближайшее время. *Методы исследования.* В ра-

[1] Об утверждении Концепции внешней политики Российской Федерации: Указ Президента РФ [от 30 ноября 2016 г. № 640]/. – URL: https://www.garant.ru/products/ipo/prime/doc/71452062/ (дата обращения: 17.01.2022). – Текст: электронный.

боте задействованы формально-юридические методы анализа китайского законодательства в информационной и кибер сферах, используются частнонаучные и общенаучные методы познания специфики национального законодательства Китая в сфере обеспечения защиты национальной и информационной безопасности и государственного суверенитета. *Результаты исследования.* В новом информационном законодательстве Китая прослеживается одинаковый вектор государственной политики, направленный на защиту национального суверенитета посредством обеспечения регулируемой китайским Правительством системы безопасности данных и их локализации на территории страны. Китай рассматривает данные, накопленные частными компаниями, как национальный актив, использование которого должно осуществляться или ограничиваться в соответствии с китайскими законами. Однако большинство законов нуждаются в дополнении и расширении некоторых терминов в связи с угрозой юридической неопределенности и созданием правового вакуума для манипуляций

Ключевые слова: *Китай, законодательство, информационная безопасность Китая, киберпространство, кибербезопасность, Big Data, Закон «О защите персональных данных» КНР, Закон «О безопасности данных» КНР, Положение «О защите безопасности критической информационной инфраструктуры» КНР, Закон «О кибербезопасности» КНР*

There can be no state sovereignty without information sovereignty. The Chinese Government understands this well and during the COVID-19 pandemic, when the whole world "went online", adopted several laws designed to regulate the country's information policy in the media sphere. At the time of writing, China has a new legislation in the field of information security. The most crucial laws in information and cyber sphere are the Law "On Data Security", "On Personal Data Protection", and the Law "On Cyberspace", the first two of which are developed to supplement and improve the application of the Law "On Cybersecurity" adopted in 2017. However, the adoption of these laws entailed a number of problems for Chinese tech-goliaths and caused a wave of international criticism. This article examines the key provisions of the new set of China's legal framework in the field of information security and analyzes the prospects for its further development. *Materials and methods.* Formal legal methods of analyzing Chinese legislation in the in formation and cyber spheres are involved, scientific and general scientific methods of cognition of the specifics of China's national legislation in the field of ensuring the protection of national and information security and state sovereignty are usedin this paper. *Results of the study.* The new information legislation of China traces the same vector of state policy aimed at protecting national sovereignty by ensuring a data security system regulated by the Chinese Government and their localization on the territory of the country. China considers the data accumulated by private companies as a national asset, the use of which should be carried out or restricted in accordance with Chinese laws. However, most of the law needs to supplement and expand some terms due to the threat of legal uncertainty and the creation of a legal vacuum for manipulation

Key words: *China, legislation, information security of China, cyberspace, cybersecurity, Big Data, the Law "On the Protection of Personal Data" of the People's Republic of China, the Law "On Data Security" of the People's Republic of China, the Regulation "On the protection of the security of critical information infrastructure" of the People's Republic of China, the Law "On Cybersecurity" of the People's Republic of China*

Актуальность исследования. Китай – динамично развивающееся государство с уникальной формой правления, правоприменительной практикой, активно отстаивающее национальные интересы. Китай занимает одну из лидирующих позиций в международных политических и экономических процессах. Страна является одним из ведущих разработчиков в сфере IT и информационно-коммуникационных технологий. Именно поэтому необходимо изучать, отслеживать новые тенденции и государственные задачи этой страны. Кроме того, согласно Концепции внешней политики Российской Федерации[2], Россия и Китай наращивают всеобъемлющее равноправное доверительное партнерство и стратегическое взаимодействие. Законодательные органы России и Китая обмениваются правовой практикой. Оба государства обозначили стимулирование роста высоких технологий и развитие киберпространства стратегически важной целью для защиты своего суверенитета. Страны активно принимают новые законодательные акты с целью

[2] Об утверждении Концепции внешней политики Российской Федерации: Указ Президента РФ [от 30 ноября 2016 г. № 640]/. – URL: https://www.garant.ru/products/ipo/prime/doc/71452062/ (дата обращения: 17.01.2022). – Текст: электронный

защиты и регулирования интернета, облачных хранилищ и Big Data. Однако правовой опыт Китая и России в этой сфере различается, в связи с чем необходимо анализировать особенности китайской практики в области информационного регулирования.

Объект исследования – система китайского законодательства в области информационной политики и работа Правительства Китая в данной области.

Предмет исследования – новые китайские законы в области информационного регулирования, в том числе регулирования интернет-пространства и кибер-сферы.

В статье рассмотрены правительственные стратегии Китая для достижения результатов нового пятилетнего плана с целью воспроизводства общей картины и выявления методов противостояния Китая угрозам информационной безопасности.

Цель исследования – научно обосновать систему противодействия угрозам информационной безопасности Китая.

Задачи исследования: рассмотреть особенности китайского законодательства в информационной сфере, интернете и кибер-сети; выявить общие тренды дальнейшей разработки китайского законодательства в информационной среде; обозначить основные векторы развития информационной политики Китая на ближайшее время.

Методы исследования. В работе задействованы формально-юридические методы анализа китайского законодательства в информационной и кибер сферах, используются научные и общенаучные методы познания специфики национального законодательства Китая в сфере обеспечения защиты национальной и информационной безопасности и государственного суверенитета.

Информационная политика Китая как «управляемая открытость». В настоящее время информационную безопасность в контексте политики Китая и большинства стран мира можно разделить в соответствии с видами угроз на информационно-техническую безопасность страны, или кибербезопасность, направленную на предотвращение и противодействие угрозам инфраструктуры и баз данных, и информационно-социальную, главной целью которой является борьба с внешней пропагандой. КНР ведет борьбу с киберпреступностью, основным инструментом которой являются несанкционированные ИКТ и средства для получения несанкционированного доступа к информации и ее видоизменению; манипулированием китайского общественного сознания и дестабилизацией внутренней политики посредством национальных и транснациональных СМИ.

Особую роль как в противодействии киберугрозам, так и манипулировании общественным сознанием Китай отводит интернету. В КНР интернет запущен в 1987 г. в Пекинском институте физики и высоких энергий, а в октябре 1990 г. в стране зарегистрирована доменная зона *.cn*. Особенностью истории развития китайского интернета является то обстоятельство, что он сразу стал закрытым. Одной из причин этому послужило восстание на площади Тяньаньмэнь в 1989 г., важную роль в котором сыграла скоординированная работа национальных и зарубежных СМИ. В 1998 г. при Цзян Цзэмине в Китае началась разработка проекта «Золотой щит», система фильтрации информации, блокирующая доступ к запрещенным КПК ресурсам из внешнего пространства интернета. В Китае существует то, что принято называть «суверенным интернетом», где в свободном доступе функционируют именно китайские сайты, а знакомые всему миру поисковые серверы Google, сеть Facebook или газеты The New York Times, The Economist заблокированы. Управляемый интернет в Китае способствует противодействию кибератакам, более точному мониторингу и борьбе с антиправительственной пропагандой. Что касается последней, то это достигается с помощью жесткой интернет-цензуры с целью пресечения любого рода нежелательного контента, чтобы избежать восстаний, массовой паники или создания политического движения, в том числе и виртуального. Другим важным инструментом против манипуляции общественным сознанием стало развитие информационных агентств и диверсификация их работы. Постепенно начался рост зарубежных филиалов государственного информационного агентства «Синьхуа», CCTV и др. Это позволило создать видимость плюрализма мнений как в Китае, так и за рубежом, и обезопасить общество от возможных недовольств.

Со временем Китай перешел от оборонительной к наступательной стратегии применения ИКТ в отношении внешнеполитических сил. Так, в 2003 г. ЦВС и КПК ввели «концепцию трех войн», которая включает

психологическую, медийную и правовую войну. В концепции обозначена необходимость превентивных действий для предотвращения угроз по трем направлениям, в том числе в киберпространстве. Крайне важным элементом присутствия Китая в мировом информационном пространстве является его стремительно развивающаяся развлекательная индустрия и коммерческие интернет-площадки. Китай способствует популяризации китайской культуры и китайского языка. Например, на 2019 г. в мире зарегистрировано 550 институтов Конфуция, 1172 школ и классов [5].

После распространения в 2017 г. в США недовольства и принятия Администрацией Д. Трампа правительственных мер против экономической экспансии Китая и роста его культурного влияния руководство КНР начало активнее пропагандировать тезис об открытости страны для международного сотрудничества. Непосредственным выражением этого стали организация и проведение многочисленных пресс-конференций с участием государственных деятелей, иностранных журналистов, размещение большого объема статистических данных и официальной информации на сайтах профильных государственных структур. Правящие круги КПК осознают важность освещения значимых событий внутри страны в иностранных СМИ. Поэтому в Китае стимулируют развитие иноязычных китайских СМИ и приобретение иностранных активов. Примером финансируемой за счет Правительства КНР работы иностранного канала является русскоязычное интернет-издание «ЭКД!»[3], которое ежедневно освещает разного рода события, происходящие в Китае.

Особое внимание Китай уделяет защите своего информационного пространства, а расширение внешних каналов китайской политической пропаганды за рубежом приводит к усилению роли КНР не только в глобальном информационном пространстве, но и в международных политико-экономических процессах. Китай действует в рамках превентивного подхода к борьбе с киберпреступностью и манипуляцией обществом. Государственная информационная политика Китая может быть определена как «управляемая открытость», подразумевающая централизованный контроль властей медиапространства и, в то же время, создание альтернативной информации, что позволяет говорить о развитии и повышении качества информационной стратегии Китая, ее адаптации к современным реалиям и политическим вызовам [14].

Основы политики Китая в области информационной безопасности. Вектор Китая на борьбу с угрозами для национальной безопасности четко обозначен в 2015 г., когда в стране впервые принят закон «О государственной безопасности КНР». Этот закон стал не только зеркальным ответом на принятую в феврале того же года новую «Стратегию национальной безопасности США», но и привел законодательство в соответствие с международными реалиями. Закон привлек внимание всего мира. А в США документ был встречен высокой критикой и большими опасениями. Таким образом, закон «О государственной безопасности КНР», в первую очередь, направлен вовне и стал свидетельством трансформации Китая в глобального игрока, готового отвечать на различные вызовы и участвовать в мировой конкуренции. При этом, в законе прописаны абстрактные формулировки, оставляющие поле для их интерпретации, а соответственно, для манипуляций. В документе прописано много угроз, подрывающих национальную безопасность страны. Однако наибольший интерес вызывает ст. 25, где перечислены угрозы информационной безопасности Китая, а также задачи противодействия им. В документе сказано об обеспечении безопасности и подконтрольности основных сетевых и информационных технологий, а также главных объектов инфраструктуры, информационных систем и данных. Отмечено, что закон укрепляет регулирование перечисленных объектов, предупреждает, пресекает и наказывает за сетевые атаки, вторжение в сети, кражи в сетях, распространение незаконной и вредной информации и другие противоправные и преступные деяния в сетях, защищает суверенитет, безопасность, развитие государством сетевого пространства [15].

Все указанные формулировки общие, однако они обозначили курс Китая на необ-

[3] О проекте. – URL: https://ekd.me/about/ (дата обращения: 17.01.2022). Текст: электронный.

ходимость противодействия информационным угрозам и подчеркнули важность участия всего общества в борьбе с ними. Так, в документе прописано, что каждый гражданин и организация несет ответственность за нарушения норм и правил обеспечения национальной безопасности и за неоказание помощи компетентным органам. В дальнейшем это привело к расширению и ужесточению регулирования информационной политики КНР и повышению мер ответственности. Таким образом, со временем китайская информационная политика и система ее защиты приобрели особые черты.

Китай тщательно следит за общественными настроениями, пропагандирует обозначенные национальные цели и задачи в массы через ключевые государственные СМИ, а также через сериалы, мультфильмы и т. д. Принимая во внимание административно-территориальное устройство КНР и историко-политическое наследие отдельных регионов, можно убедиться, что не в каждом уголке Китая информационная политика работает отлаженно. Ярким примером здесь выступает специальный административный район Гонконг, бывшая британская колония, которая в 1997 г. прекратила свое существование и вошла в состав КНР как САР. В 1997 г. вступил в силу Основной Закон Гонконга (аналог конституции). Но Гонконг по своему идеолого-политическому содержанию не стал китайским. Там за время господства британцев сформировались западные диаспоры, которые до сих пор оказывают влияние на политическую жизнь в САР. Особенности политической жизни в Гонконге находят свое отражение в Основном законе. В ст. 5 говорится, что идеи социализма не должны практиковаться в Гонконге, а капиталистическая система должна оставаться неизменной в течение 50 лет. И это не единственная сложность в отношении этого района, которую на протяжении долгих лет решают китайские власти. В Основном законе, в ст. 23, сказано, что САР должна принимать законы, которые запрещают любые акты государственной измены, подстрекательства, подрывной деятельности против Центрального правительства или кражи информации, относящейся к государственной тайне. Все это необходимо, чтобы запретить иностранным политическим организациям и другим силам проводить политическую деятельность в Гонконге или устанавливать связи с иностранными политическими организациями и органами. Несмотря на это, по прошествии 23 лет после передачи суверенитета над Гонконгом Китаю, регион юридически не получил право самостоятельно принимать законы для обеспечения национальной безопасности в соответствии со ст. 23. В регионе фактически не определена конституционная и законодательная ответственность за обеспечение национальной безопасности.

Все изменилось в марте 2021 г., когда в Пекине завершился съезд Всекитайского собрания народных представителей (ВСНП), на котором законодатели обсудили реформу выборов в Гонконге. Официально проект назывался «О совершенствовании правовой системы и механизмов ее соблюдения в специальном административном районе Гонконг для обеспечения национальной безопасности»и принят 28 мая в ходе 3-й сессии 13-го ВСНП.

Глава Гонконга Кэрри Лам поддержала инициативу и призвала быстрее осуществить реформу, выразив обеспокоенность участием в выборах радикальных сил. По ее мнению, без реформы они могут дестабилизировать политическую систему Гонконга и нарушить принцип «Одна страна – две системы». Например, после серии переговоров и консультаций вице-президента США Майка Пенса с бывшим секретарем Гонконга Ансоном Чаном, спикера Палаты представителей США Нэнси Пелоси с представителем оппозиции Деннисом Квоком в ходе поездок, а также вслед за открытой поддержкой оппозиции американцами в 2019 г., в 2020 г. в Гонконге прошла череда общественных протестов, которые демонизировали Закон о ст. 23 и препятствовали его принятию. Позже Палата представителей США приняла закон «О защите прав человека и демократии в Гонконге» [3].

Существующая лазейка в национальной безопасности Гонконга ставила под угрозу действие принципа «Одна страна – две системы», национальный суверенитет, верховенство Закона. Неэффективно работала правоохранительная система. По отношению к участникам движения «Независимость Гонконга» применялись достаточно слабые наказания [20].

Закон о нацбезопасности вступил в силу в июне 2020 г. Согласно тексту, Закон пред-

усматривает создание в Гонконге Комитета национальной безопасности, находящегося в непосредственном подчинении у центральной власти КНР, а также вводит максимальное наказание в виде пожизненного заключения для тех, чьи действия направлены на подрыв власти либо отделение Гонконга или другой части страны от Китая, кто совершил теракт и вступил в сговор с иностранными силами с целью поставить под угрозу национальную безопасность [2].

Стратегические задачи Китая по развитию технологической сферы и киберпространства. В марте 2021 г. на очередном съезде ВСНП китайские законодатели одобрили план 14-й пятилетки на 2021–2025 гг., а также утвердили новые цели развития до 2035 г. В этот раз укрепление независимости страны в технологической сфере, искусственном интеллекте, квантовых компьютерах и развитие внутреннего рынка стали новыми «китами» КНР. В свою очередь, эти составляющие пятилетнего плана позволят сократить зависимость от иностранного рынка технологий, в частности от американского. Однако это лишь задача. Целью китайской политики в данном контексте является наращивание экономической, политической мощи и обеспечение суверенности принятия решений. Именно поэтому развитие технологий, внедрение инноваций и формирование устойчивой системы кибербезопасности в Китае следует рассматривать в качестве целостной государственной стратегии, призванной обеспечить достижение этой цели. Так, существует устойчивая взаимосвязь. Суверенитет в технологиях и, как следствие, киберпространстве – это суверенитет в информационном пространстве.

Принимая во внимание принятый на XIX съезде ВСНП очередной план пятилетнего развития, можем выявить следующие задачи государственной политики Китая по развитию технологической сферы и киберпространства. В первую очередь, это цифровизация логистики и промышленности. Для достижения этой цели Китаю необходимо нарастить потенциал в области информационно-коммуникационных и компьютерных технологий на основе искусственного интеллекта и 5G-технологий [9].

Следующая задача – регулирование национального киберпространства. Ее можно определить как стремление к балансу в сфере государственного регулирования информационного и киберпространства посредством создания системы эффективного применения законодательства в информационном пространстве и в сфере данных. В целом, еще в 2003 г. Правительство КНР стало последовательно разрабатывать законы в этой области и со временем приняло ряд важнейших документов, которые вместе дают исчерпывающее представление о государственной политике Китая в сфере управления информационным и киберпространством. Современная стратегия КНР в области кибербезопасности отражена в «Мнении Государственного совета о форсированном продвижении развития информатизации и о реальном обеспечении информационной безопасности», которая начала реализовываться 2012 г. В 2016 г. ЦК КПК опубликовал «План национальной стратегии инновационного развития», где указывалось, что для защиты экономического развития Китая, а также для модернизации и поддержания национальной сетевой безопасности необходимо стимулировать научные исследования и продвигать технологии сетевой безопасности [6]. Тренд защиты национальных интересов КНР в информационном пространстве с помощью новейших технологий экстраполирован практически на все китайские законы. Он также отслеживается в Законе «О государственной безопасности» Китая от 1 июля 2015 г. В ст. 24 Закона «О национальной обороне» прописано, что китайское государство укрепляет создание собственного инновационного потенциала и ускоряет развитие высоких технологий; ст. 73 гласит о поощрении технических инноваций в сфере национальной безопасности. В ст. 76 данного закона указано, что китайское государство призвано укреплять информирование населения, направлять общественное мнение в области национальной безопасности, ведет пропагандистскую и образовательную деятельность в сфере государственной безопасности. Однако основной импульс развития китайского законодательства по защите информации в сети получил в 2017 г.

Другой задачей государственной политики КНР по развитию и обеспечению безопасности киберпространства и технологической сферы является создание альтернативной стратегии регулирования глобального киберпространства. Китай стремится

сформировать правовые рамки поведения в киберпространстве, которые могли бы принять мировое или региональное сообщество. Среди подобных инициатив китайской стороны в 2020 г. можно назвать следующие. Во-первых, Глобальная инициатива по безопасности данных, направленная на обеспечение развития сферы ИКТ и противодействие их использования в преступных целях, включает восемь ключевых пунктов, получивших название «План Вана» (в честь министра иностранных дел КНР Ван И) [24]. Во-вторых, План «Совместное построение сообщества с общим будущим в киберпространстве», являющийся частью китайского плана «Построение человечества единой судьбы». Он носит декларативный характер и может быть рассмотрен как попытка создания альтернативной коалиции стран с «другими», в отличие от Запада, ценностями регулирования киберпространства. В Плане отсутствуют понятия прав человека и общих ценностей в киберпространстве, роли общественных организаций и т. п., что, в основном, характеризует западные ценности [25].

Еще одной важной задачей является обеспечение технологического лидерства государства в таких областях, как искусственный интеллект, 5G, суперкомпьютеры. Для развития каждой из этих сфер требуется задействовать колоссальные объемы данных. Каждая из сфер регулируется китайским информационным законодательством. В последнее время Китай особое внимание уделяет развитию космоса и гонке космических технологий. Только за 2021 г. Китай запустил в космос 50 ракет [12]. В КНР в 2016 г. запущен первый в мире спутник квантовой связи, позволяющий хранить больше информации, значительно экономя энергию [17].

Правовое регулирование BigData в Китае. Задача регулирования киберпространства в Китае реализуется посредством разработки соответствующих законов. С 2017 г. ПК ВСНП практически ежегодно принимал законы в рассматриваемой нами сфере. Среди них Закон «О защите персональных данных» 2021 г., «О безопасности данных» 2021 г., Положение «О защите безопасности критической информационной инфраструктуры» 2021 г., Гражданский кодекс КНР, вступивший в силу 1 января 2021 г., Закон «О криптографии» 2019 г., Меры по оценке безопасности облачных вычислений 2019 г., Закон «О шифровании данных» 2020 г., Закон «О кибербезопасности» и «О сетевой безопасности» 2017 г. Закон «О борьбе с терроризмом» 2015 г.

Закон «О защите персональных данных» составляет единую систему правового регулирования информационной среды и Big Data вместе с Законом «О безопасности данных», Законом «О кибербезопасности», Гражданским кодексом Китая, вступившим в силу 1 января 2021 г., и Регламентом «О защите безопасности критической информационной инфраструктуры», который начал действовать с 1 сентября 2021 г. Закон «О защите персональных данных»является рамочным, он устанавливает основные принципы, цели, полномочия и ответственность в области защиты персональных данных, однако не регулирует частные вопросы. Сейчас подобное ad hoc регулирование осуществляется государственными регуляторами, такими как Администрация по киберпространству. Действие закона не распространяется на «приватность» как таковую, поскольку она регулируется отдельным институтом китайского права. Закон «О защите персональных данных»направлен на защиту физических лиц, общества и национальной безопасности от вреда, который может быть причинен злоупотреблениями и нарушениями при обработке информации, относящейся к личности человека. Согласно ст. 3, Закон применяется к любой деятельности по обработке персональной информации в границах КНР. То есть, также относится информация о расе, этнической принадлежности, биометрии, религии, финансах и т. д. Кроме того, статья предусматривает *экстерриториальное применение,* для которого в Законе прописан ряд условий: 1) обработка персональной информации в целях предложения товаров или услуг физическим лицам, находящимся в Китае; 2) проведение анализа и оценки деятельности физических лиц на территории Китая; 3) иные обстоятельства, предусмотренные другими законами или административными подзаконными актами (бланкетная норма, допускающая ее трактовку на усмотрение властных органов). Из этого следует, что Закон регулирует деятельность как публичных институтов, так и частного сектора, применяется как на национальном, так и на внегосударственном уровне. Статья 4 устанавливает определение понятия «персональная информация», под

которой понимаются все виды информации, записанные с помощью электронных или иных средств, относящиеся к определенному или определяемому физическому лицу, за исключением информации после применения технологий анонимизации [19].

Закон «О безопасности данных» сфокусирован на защите национальной безопасности Китая и национальных данных. К сфере его действия относятся все операции обработки данных внутри страны. Идея закона заключается в создании всеобъемлющей системы защиты данных, управляемой государством. Целью Закона выступает обеспечение безопасности данных и стандартизация их обработки, содействие разработке и инновационному применению данных, защита прав и интересов физических и юридических лиц Китая, а также защита национального суверенитета. Государство, согласно тексту Закона, должно создать систему категоризации защиты данных в соответствии с их важностью для развития страны, а основу такой системы должны составить «каталоги важных данных». К обработке данных Закон относит сбор, хранение, использование, переработку, передачу, предоставление, раскрытие и осуществление других операций с данными. Закон содержит два ключевых термина: «национальные ключевые данные», которые влияют на национальную безопасность государства, экономику страны и интересы общества; «важные данные», которые как понятие в Законе не определены. Это может создать правовую неопределенность, как и в случае с Законом «О кибербезопасности» 2017 г., в отношении которого еще не были изданы правила его применения. Однако со временем должны быть созданы «каталоги важных данных». В Китае разработан ряд проектов подзаконных актов, в которых даны определения «важных данных» для различных экономических секторов. В мае 2021 г. Управление киберпространством Китая вынесло на общественное обсуждение «Проект Правил управления безопасностью автомобильных данных», в котором представлен список «важных данных» для автомобильной отрасли [23]. Термин «данные» подвергается широкой трактовке и подразумевает любую информацию, записанную в электронной или другой форме. За рамками Закона остаются два типа информации: государственная тайна, для которой существует Закон «Об охране государственных тайн», а также информация, которая входит в зону ответственности Центральной военной комиссии.

Действия этого Закона, по аналогии с Законом «О персональных данных», распространяется как на национальные и иностранные компании на материковой части Китая, так и на обработку данных за пределами страны, если ее обработка в иностранных государствах наносит ущерб национальной безопасности, правам и интересам граждан и организаций Китая или общественным интересам. Согласно ст. 36 Закона, передача данных, хранящихся на территории Китая, правоохранительным или судебным органам за пределы страны без предварительного согласия Правительства КНР, запрещена.

Так, на международном уровне самой важной составляющей Закона стали правила о трансграничных данных. Их регулирование уже частично попадало под действие Закона КНР «О кибербезопасности» 2017 г., который запретил организациям, предоставляющим онлайн услуги, собирать и продавать личные данные пользователей. В Законе «О персональных данных» сказано, что его юридическая сила выше международных договоров, ратифицированных китайским государством.

Согласно Закону, операторы данных обязаны проводить мониторинг угроз и, при выявлении дефектов, уязвимостей, и других угроз безопасности, предпринимать корректирующие меры. При возникновении происшествий, касающихся безопасности данных, операторы данных обязаны предпринимать меры для ликвидации последствий и своевременно информировать пользователей и соответствующие госорганы. Операторы данных, отнесенных к важным, обязаны регулярно представлять в соответствующие госорганы отчетность об оценке угроз, в которой должны содержаться виды и количество «важных данных» в распоряжении, сведения о деятельности, виды угроз безопасности и меры реагирования. Для компаний, нарушивших Закон, предусмотрено несколько видов юридической ответственности. Первый штраф может составлять сумму до 500 тыс. юаней, а для и для руководителей компаний или ответственных за безопасность данных – до 100 тыс. юаней. При повторном нарушении или утечке данных и других серьезных нарушениях компанию могут оштрафовать на сумму в объеме до 2 млн юаней.

Если же действия с данными будут констатировать угрозу национальной безопасности КНР, то организации предстоит выплатить сумму в размере до 10 млн юаней [8]. В соответствии со ст. 5 Закона, главным органом, являющимся ответственным за руководство работой по обеспечению безопасности данных в Китае, выступает Центральный комитет государственной безопасности (ЦКГБ) [7].

Закон «О кибербезопасности» вступил в силу 1 июня 2017 г. В нем изложены общие принципы и меры по поддержке и развитию сетевой безопасности, включая надзор, превентивные меры и реагирование на экстренные ситуации. В ст. 1 документа сказано, что Закон направлен на обеспечение сетевой безопасности, защиты суверенитета в киберпространстве и национальной безопасности, отстаивание интересов общества, защиту законных прав и интересов граждан, юридических лиц и других организаций.

Закон «О кибербезопасности» становится первым китайским документом, где вводится понятие «ключевая информационная инфраструктура». В соответствии с Законом, Китай осуществляет особую защиту КИИ в области общественных телекоммуникаций и информационных услуг. Сюда относится энергетика, транспорт, ирригационная система, оборона, экономика и финансы, промышленность и технологии, электронное правительство и другие важные отрасли и сферы деятельности, а также другая КИИ, если причинение вреда или раскрытие данных КИИ может представлять существенную угрозу национальной безопасности, экономике, благосостоянию или публичным интересам Китая.

По закону «О кибербезопасности» 2017 г., как и «О безопасности данных» 2021 г., организации, которые работают с КИИ, должны хранить все данные на территории Китая. Для отправки данных за пределы страны им необходимо получить официальное разрешение правительственных органов. Ответственность полностью возлагается на компании. Главное бремя за нарушение законодательства ложится на главу корпорации – от ежегодной переаттестации и найма специалистов до выполнения всех требований регулятора.

Несмотря на кажущуюся неполноту и местами расплывчатый характер, Закон является основой для государственного регулирования информационных технологий, встраивания их в общую конструкцию современного китайского общества.Документ подчеркивает важность стандартизации и контроля при доминирующей роли правительства. Основная ответственность за обеспечение безопасности возлагается на операторов КИИ [16]. Они должны, в соответствии с Законом, создавать специальные отделы для обеспечения безопасности и назначать ответственных лиц, проводить регулярное обучение и аттестацию своих сотрудников, вести мониторинг состояния сетей, осуществлять проверку безопасности при закупке основного оборудования и оценку угроз безопасности, принимать превентивные меры против кибератак, представлять соответствующую отчетность в контролирующие органы и хранить ее не менее шести месяцев со дня создания.Также в обязанности операторов связи входит первоначальная сортировка данных, шифрование и создание копий важной информации.При этом все операторы должны хранить «важные данные» и «персональные данные» на территории КНР. Регулятором по защите безопасности КИИ является Министерство общественной безопасности КНР, которое осуществляет свою деятельность под общим руководством Государственной канцелярии по делам интернет-информации (САС).

Провайдерам сетевых продуктов и услуг, согласно тексту Закона, запрещается устанавливать «вредоносные программы». При обнаружении в сетевых продуктах и услугах «слабых мест или других рисков» они должны незамедлительно принять меры по исправлению ситуации и своевременно уведомить пользователей и уполномоченные органы. Критическое сетевое оборудование и продукты сетевой безопасности перед стартом продаж должны проверяться на соответствие национальным стандартам, требованиям и быть сертифицированы институтами или пройти испытания на безопасность.

Вопросы приватности информации в интернете трактуются в Законе в общем виде; сбор персональной информации допускается в рамках «соответствующих законов и правил», то есть в рамках Закона «О безопасности данных», а также Законе «О защите персональных данных». Согласно Закону «О кибербезопасности», провайдеры, собирающие и хранящие данные пользователей, должны

получить их разрешение на сбор информации. При этом по Закону операторам запрещено разглашать, искажать, наносить ущерб, а также вести сбор личной информации; исключается анонимность пользователей при регистрации в интернете, социальной сети, подключении мобильной связи, предоставлении клиенту услуг, распространение информации или ее передача и при подписании соглашения об оказании услуг, когда клиент должен предоставить подлинное удостоверение личности.

В отдельной статье прописаны виды наказания за неисполнение или нарушение Закона, которые преимущественно составляют штрафы в размере до 100 тыс. юаней, в случаях, если их действия не влекут за собой уголовной ответственности [10].

Положение «О защите безопасности критической информационной инфраструктуры» опубликовано в 2017 г. после вступления в силу Закона «О кибербезопасности», а в августе 2021 г. проведена его качественная редакция. Положение расширило трактовку КИИ и внесло ясность относительно его имплементации. Положение к Закону КНР «О кибербезопасности» к КИИ также относит сетевую инфраструктуру и информационные системы перечисленных в Законе отраслей. В остальном перечень не изменился. Подробные правила признания инфраструктуры и информационных системы в качестве КИИ устанавливаются органами отраслевого регулирования и контроля для каждой отрасли отдельно. После определения правил и их регистрации в Министерстве общественной безопасности КНР органы отраслевого регулирования и контроля должны самостоятельно проводить оценку инфраструктуры и информационных систем и в соответствии с ней принимать решения об отнесении объектов к КИИ с учетом их значимости для соответствующей отрасли, возможного ущерба и другого взаимосвязанного влияния на эту отрасль или сферу деятельности. В случае отнесения к КИИ госорганы обязаны уведомить оператора инфраструктуры или информационной системы, а также проинформировать об этом Министерство общественной безопасности Китая.

Гражданский кодекс закрепляет право на неприкосновенность частной жизни и принципы защиты личной информации китайских граждан. Он определяет личную информацию как различного рода сведения (имя, фамилия, дата рождения, номер удостоверения личности, биометрические данные, сведения о здоровье и т. п.), которые зафиксированы в электронной или другой форме и позволяют по отдельности или в совокупности с другими сведениями идентифицировать конкретное физическое лицо. Кодекс устанавливает правовую основу для обработки персональной информации, обязанности для обработчиков личных данных, права отдельных лиц на их личную информацию и обязанности административных органов по сохранению, неразглашению и нераспространению информации, полученной ими при исполнении должностных обязанностей. Как определяет Верховный народный суд КНР, «спор о защите личной информации» может служить основанием для возбуждения гражданского иска в соответствии с кодексом.

Закон «О криптографии»,вступивший в силу 1 января 2020 г., призван регулировать применение шифрования, управлять развитием криптографии бизнеса, обеспечивать информационную и национальную безопасность, общественные интересы, защищать законные права граждан, юридических лиц и других организаций. Согласно Закону, криптографией являются технологии, продукты и услуги, которые определенным образом применяются к информации для обеспечения шифрования и аутентификации данных. Исполнение закона контролируется Государственным управлением криптографии и Национальным управлением по защите государственной тайны. В законе определены три категории шифрования: базовая, основная и коммерческая. Базовая и основная относятся к обеспечению национальной безопасности, коммерческая предполагает взаимодействие только между коммерческими структурами.

Вся принадлежащая государству конфиденциальная информация, передающаяся сетям транспортировки данных, и все информационные системы, хранящие такие данные, должны использовать алгоритмы базовой и общепринятой криптографии. При возникновении рисков или угрозы использования алгоритмов должны быть приняты незамедлительные меры. Закон предусматривает организацию строгого контроля за тем, как соблюдается режим криптозащиты данных. За нарушение конфиденциальности

данных наступает юридическая ответственность (какая именно, не уточняется) [4]. Так, с начала года за упущения наказано 383 тыс. чиновников [1].

Меры по оценке безопасности услуг облачных вычислений вступили в силу 1 сентября 2019 г. Документ представляет собой руководство по повышению уровня безопасности услуг облачных вычислений. Согласно содержанию документа, при оценке безопасности услуг облачных вычислений большое внимание уделяется кредитоспособности и состоянию хозяйственной деятельности операторов облачных платформ, биографии сотрудников компаний по предоставлению облачных услуг и состоянию безопасности цепочек поставок технологий, продукции и услуг облачных платформ. Поставщики облачных сервисов могут подавать заявки на оценку безопасности своих услуг [13].

В соответствии со ст. 19 Закона «О борьбе с терроризмом» 2015 г.правоохранительные органы Китая обладают широкими полномочиями удалять или блокировать контент, приказывать закрывать веб-сайты и прекращать другие услуги без судебного разбирательства. Статья 18 обязывает интернет-провайдеров и операторов связи предоставлять китайским властям коды дешифрования информации и другие технические интерфейсы. За нарушение положений законодательства операторов связи и провайдеров могут оштрафовать на сумму 200…500 тыс. юаней в соответствии со ст. 84 Закона. В Законе содержится определение терроризма, в связи с которым Закон подвергся резкой международной критике. Так, согласно ст. 3 Закона, под терроризмом понимаются «предложения и действия, создающие общественную панику, ставящие под угрозу общественную безопасность, посягающие на личность и собственность или принуждающие национальные органы или международные организации с помощью таких методов, как насилие, уничтожение, запугивание, для достижения своих политических, идеологических или других целей».

Последствия действий законов. Закон «О защите данных» от 1 сентября 2021 г. называют самым строгим в мире. Для достижения ключевой цели Китая, защиты государственного суверенитета в самом широком смысле, в Законе ввели ряд ограничений, что привело к проблемам для технологических корпораций. Еще в 2017 г., когда вступил в силу Закон «О кибербезопасности», запрещавший продавать данные китайских пользователей за пределы КНР, международные компании призывали правительство отсрочить начало действия Закона. Корпорации, которые локализовали сбор и обработку данных внутри страны, эти законы затрагивают не так сильно. В гораздо большей степени новые законы влияют на бизнес, оперирующий крупными данными и задействованный в отраслях КИИ или за границей. К ним относятся технологические гиганты Alibaba, Tencent, Huawei JD.com и другие. Первые правительственные санкции начались с остановки работы и расследования в отношение IPO Ant.Group, дочки Alibaba, которая должна была провести размещение. Однако оно не состоялось, и компания выплатила штраф 2,8 млрд долл. США. Компании вроде Tencent, Alibaba ищут лазейки для выхода на IPO, создавая подразделения в других странах и проводя листинг через них. Так, в 2019 г. Alibaba размещена в Гонконге, специальном административном районе Китая. Но едва успев оправиться от первого внутреннего финансового кризиса, компания Alibaba столкнулась с другими. Так, в 2020-2021 гг. компанию оштрафовали за несоблюдение кибер-законодательства. В декабре 2021 г. телекоммуникационный регулятор КНР приостановил сделку по кибербезопасности с дочерней компанией конгломерата – AlibabaCloud, которая не своевременно сообщила про уязвимость в системе ПО. Другой техногигант, Bytedance, после встречи с телекоммуникационным регулятором отложил выход на IPO, а по прошествии времени глава компании объявил о своей отставке во избежание конфликта с властями [11]. Печальный опыт прошел агрегатор такси и каршеринг Didi, который вышел на IPO в Америке. За этим последовало правительственное расследование, и через несколько дней акции компании упали, а на регистрацию новых пользователей введен запрет. В итоге, приложение Didi удалено и заблокировано для скачивания на территории Китая. А 27 декабря 2021 г. Министерство торговли КНР и Национальная комиссия по развитию и реформам опубликовали руководство и так называемый «негативный» список, который регулирует иностранные инвестиции. Список вступил в силу 1 января 2022 г. Согласно документу, компании, веду-

щие экономическую деятельность в отраслях, включенных в список, должны получить одобрение от китайских регуляторов, прежде чем они смогут провести первичное публичное размещение акций за границей [22].

В начале августа 2021 г. опубликован совместный документ Госсовета КНР и ЦК КПК, в котором говорилось о предстоящих планах государственного строительства до 2025 г. В него вошел пункт о регулировании бизнеса с основным упором на национальную безопасность, технологии и антимонопольное регулирование [21]. Это, в свою очередь, подтверждает тренд по дальнейшему ужесточению контроля технологического сектора, кибер- и информационного пространства Китая. Предположительно, в ближайшем будущем под столь же строгий контроль могут быть поставлены продуктовые сети и аптеки. В целом, 22 августа ЦБ Китая уже выписал на основе нового Закона штрафы на общую сумму 1,77 млн долл США. И, вероятно, еще множество компаний будут вынуждены заплатить, не успевая перестроиться под требования регуляторов. Кроме того, об усилении регулирования также свидетельствует покупка Пекином по 1 % акций компаний Bytedance и SinaWeibo. Символические доли имеют практическую направленность и предоставляют государственным представителям места в совете директоров ведущих китайских технологических компаний.

Заключение. В настоящий момент в Китае действует новое законодательство в области информационной безопасности. Важнейшими среди законов в информационной сфере являются Закон «О безопасности данных», «О защите персональных данных» и Закон «О киберпространстве», первые два призваны дополнить и усовершенствовать применение Закона «О кибербезопасности» 2017 г. В перспективе именно эти три закона образуют систему регулирования отношений по обработке данных в КНР. Каждый Закон и Положения к ним обязывают компании, сотрудников, операторов, провайдеров и других работников проводить регулярный мониторинг сети, баз данных, принимать превентивные, незамедлительные меры по предотвращению угроз кибербезопасности и безопасности информации и данных пользователей, предоставлять отчеты и вовремя информировать государственные органы о возможных или существующих угрозах. В каждом из них можно проследить одинаковый вектор политики, направленной на защиту государственного суверенитета посредством обеспечения регулируемой системы безопасности данных и их локализации на территории КНР. Таким образом, Китай рассматривает накопленные частными компаниями данные как национальный актив, использование которого должно осуществляться или ограничиваться в соответствии с китайскими законами.

Подводя итог, следует сказать, что все три закона нуждаются в дополнении. Существует неопределенность в отношении многих положений и ключевых понятий «законодательной триады» информационно-коммуникационной сферы и киберпространства КНР. В частности, это касается отсутствия в Законе «О защите данных» определения понятия «важные данные». В законах пока нет объяснений, каким образом следует транспортировать данные из Китая в рамках одной компании или группы. В Китае пока что не полностью созданы технологии удостоверения личности, не решен вопрос ответственности интернет-сайтов, а стандарты для различных отраслей только разрабатываются. В этот список можно добавить нехватку необходимых разъяснительных положений об интеллектуальной собственности при заключении пользовательских соглашений и другие проблемы. Одна из важнейших задач, которая стоит перед китайскими законодателями, это решение вопроса о взаимосвязи трех законов и их применение, наряду с другими, например, с Гражданским кодексом, или правилами входа на рынок аппаратного и программного обеспечения.

Все законы будут и дальше реформироваться под эгидой нового пятилетнего плана развития страны. Согласно ему, большинство законов будут постепенно адаптироваться под две ключевые линии развития: стимулирование разработки собственных технологий и достижение технологической и торговой независимости КНР. Такая работа уже идет. ПК ВСНП, постоянный орган при китайском однопалатном парламенте ВСНП, рассматривает ряд проектов поправок в действующие законы. Ведется обсуждение проектов к системе законов, призванных регулировать информационную и кибер-безопасность. Так, завершились консультации по второму проекту Закона «О персональных данных»,

который предположительно будет принят в 2022 г.[4]

Закон «О безопасности данных», наряду с Законом «О кибербезопасности», как и многие другие китайские законы, подвергается сильной зарубежной критике. Страны, на чью долю приходится наибольшее число размещенных на территории КНР технологических и финансовых предприятий, крайне обеспокоены, что действующие законы приведут к закрытию иностранных компаний из-за затрат и других трудностей, связанных с адаптацией под правовую базу. Многие из них не согласны с хранением данных на китайских серверах. Закон Китая «О безопасности данных» часто сравнивают с аналогичным законом Евросоюза, где под персональными данными понимается информация, которая в случае утечки или кражи способна нанести вред обладателю или поставить под угрозу его личную безопасность.

Пока не все компании способны соблюдать новые законы. Но крупный бизнес, особенно из технологической сферы, будет под жестким контролем китайских властей, а международным компаниям, планирующим продолжить работу в Китае, придется не только подстраиваться под новые правила, но и принять госрегулирование бизнеса через покупку акций и долей в компаниях как fait accompli.

Список литературы

1. 383 тысяч чиновников наказаны в Китае за первые три квартала 2019 года Russian.people.cn. 28.10.2019. Пекин. URL: http://russian.people.com.cn/n3/2019/1028/c31521-9626826.html (дата обращения: 17.01.2022). Текст: электронный.

2. В Гонконге вступил в силу принятый Китаем закон о нацбезопасности. Текст: электронный // РБК Новости. 2020. 30.06. URL: https://www.rbc.ru/politics/30/06/2020/5efb60369a79473f0d1de99d (дата обращения: 17.01.2022).

3. В Китае одобрили план технологического прорыва. Текст: электронный // РБК Новости. 11.03.2021. URL: https://www.rbc.ru/politics/11/03/2021/604a2c5e9a7947bc907a7920 (дата обращения: 17.01.2022).

4. В Китае приняли первый закон о шифровании данных. Текст: электронный // Коммерсантъ. 2019. 26.10. URL: https://www.kommersant.ru/doc/4140530 (дата обращения: 17.01.2022).

5. В мире работает 550 институтов Конфуция. Текст: электронный // РИА Новости. 2019. 10.12. URL: https://ria.ru/20191210/1562217842.html (дата обращения: 17.01.2022).

6. Задремайлова Вероника. Эволюция политики КНР в области информационной безопасности. URL: https://www.imemo.ru/files/File/magazines/puty_miru/2020/01/07_Romashkina.pdf (дата обращения: 17.01.2022). Текст: электронный.

7. Закон КНР «О безопасности данных»: краткий обзор. Текст: электронный // CNLegal, 22.09.2020. URL: https://cnlegal.ru/china_economic_law/china_data_security_law_2021/ (дата обращения: 17.01.2022).

8. Закон КНР о безопасности данных. Текст: электронный // Научно-технический центр «ГРЧЦ». 20.08.2021. URL: https://rdc.grfc.ru/2021/08/zakon_o_bezopacnocti_knr/ (дата обращения: 17.01.2022).

9. Как будет развиваться Китай в ближайшие 5 лет? Четырнадцатая пятилетка задает тренды. Текст: электронный // Агентство CNewsAnalytics. 29.10.2020. Пекин. URL: https://www.cna.com.tw/news/firstnews/202010290212.aspx (дата обращения: 17.01.2022).

10. Кибербезопасность по-китайски: в КНР вступает в силу новый закон об интернете Text: electronic // ТАСС Новости. 2017.29.05. URL: https://tass.ru/mezhdunarodnaya-panorama/4290068 (дата обращения: 17.01.2022).

11. Китай начал расследование в отношении одобривших IPO AntGroup регуляторов. Text: electronic // Forbes. 07.04.2021. URL: https://www.forbes.ru/newsroom/biznes/428037-kitay-nachal-rassledovanie-v-otnoshenii-odobrivshih-ipo-ant-group (дата обращения: 17.01.2022).

12. Китай провёл 50-й пуск космических ракет в 2021 году. 16.12.2021. URL: https://3dnews.ru/1056072/kitay-provyol-50y-pusk-kosmicheskih-raket-v-2021-godu (дата обращения: 17.01.2022). Текст: электронный.

[4] Translation: Personal Information Protection Law of the People's Republic of China (Draft) (Second Review Draft). – April 2021, – URL: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-draft-second-review-draft/ (дата обращения: 17.01.2022). – Текст электронный.

13. Китай усилит оценку безопасности услуг облачных вычислений. Текст: электронный // Рамблер. 23.07.2019. URL: https://finance.rambler.ru/other/42540367/?utm_content=finance_media&utm_medium=read_more&utm_source=copylink (дата обращения: 17.01.2022).

14. Кошурникова Н. А. Особенности информационной политики современного Китая. 2016. Екатеринбург. URL: https://elar.urfu.ru/bitstream/10995/40188/1/kiis_2016_035.pdf (дата обращения: 17.01.2022). Текст: электронный.

15. О государственной безопасности: Закон КНР [от 01.07.2015]. URL: https://chinalaw.center/constitutional_law/china_state_security_law_2015_russian/ (дата обращения: 17.01.2022). Текст: электронный.

16. О защите безопасности ключевой информационной инфраструктуры: положение; краткий обзор. Текст: электронный // CNLegal. 28.09.2020. URL:https://cnlegal.ru/china_economic_law/critical_information_infrastructure_security_2021/ (дата обращения: 17.01.2022).

17. О современной политике Китая в киберпространстве. Текст: электронный // D-Russia.ru, 02.07.2021. URL: https://d-russia.ru/o-sovremennoj-politike-kitaja-v-kiberprostranstve.html (дата обращения: 17.01.2022).

18. Об утверждении Концепции внешней политики Российской Федерации: Указ Президента РФ [от 30 ноября 2016 г. № 640]. URL: https://www.garant.ru/products/ipo/prime/doc/71452062/ (дата обращения: 17.01.2022). Текст: электронный.

19. Обзор Закона КНР «О защите персональной информации». Текст: электронный // Zakon.ru. 17.09.2021. URL: https://zakon.ru/blog/2021/09/17/obzor_zakona_knr_o_zaschite_personalnoj_informaciipersonal_information_protection_law_of_the_peoples#_ftn3 (дата обращения: 17.01.2022).

20. Объяснение телеканала CGTN: каковы основные положения законопроекта о национальной безопасности Гонконга? Текст: электронный. // Интерфакс. 08.06.2020. URL: https://www.interfax.ru/pressreleases/712249 (дата обращения: 17.01.2022).

21. Синьхуа, Центральный комитет Коммунистической партии Китая и Государственный Совет издали «План государственного строительства в условиях верховенства закона (2021–2025)». 11,08.2021. Пекин. URL: http://www.xinhuanet.com/2021-08/11/c_1127752490.htm (дата обращения: 17.01.2022). Текст: электронный.

22. Через несколько дней после одобрения структур VIE Пекин публикует «Негативный список», чтобы ужесточить контроль за зарубежными IPO стратегически важных компаний. Текст: электронный // ChinaStocks.Ne. 19.01.2022. Москва. URL: https://chinastocks.net/china-2/negativnyj-spisok-ipo/?lang=ru (дата обращения: 17.01.2022).

23. China Issued Draft Provisions on the Management of Automobile JDSupra. Data Security. 14.06.2021. URL: https://www.jdsupra.com/legalnews/china-issued-draft-provisions-on-the-6616687/ (дата обращения: 17.01.2022). Текст: электронный.

24. China's Bid to Write the Global Rules on Data Security. Текст: электронный // The Diplomat. 20.09.2020. URL: https://thediplomat.com/2020/09/chinas-bid-to-write-the-global-rules-on-data-security/ (дата обращения: 17.01.2022).

25. Highlights of 2020 World Internet Conference. 20.11.2020. URL:http://www.wuzhenwic.org/2020-11/20/c_565230.htm (дата обращения: 17.01.2022). Текст: электронный.

26. Personal Information Protection Law of the People's Republic of China (Draft) (Second Review Draft). April 2021. URL: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-draft-second-review-draft/ (дата обращения: 17.01.2022). Текст: электронный.

References

1. 383 tysyach chinovnikov nakazany v Kitaye za pervye tri kvartala 2019 goda Russian.people.cn. 28.10.2019. Pekin (383 thousand officials punished in China in the first three quarters of 2019 Russian.people.cn. 10/28/2019. Beijing). Available at: http://russian.people.com.cn/n3/2019/1028/c31521-9626826.html (date of access: 01/17/2022). Text: electronic.

2. *RBK Novosti. 2020. 30.06* (RBC News. 2020. 30.06). Available at:https://www.rbc.ru/politics/30/06/2020/5efb60369a79473f0d1de99d (date of access 01/17/2022). Text: electronic.

3. *RBK Novosti. 11.03.2021* (RBC News. 03/11/2021). Available at: https://www.rbc.ru/politics/11/03/2021/604a2c5e9a7947bc907a7920 (date of access: 01/17/2022). Text: electronic.

4. *Kommersant. 2019. 26.10* (Kommersant. 2019. 26.10). Available at:https://www.kommersant.ru/doc/4140530 (date of access: 01/17/2022). Text: electronic.

5. *RIA Novosti. 2019. 10.12* (RIA Novosti. 2019. 10.12). Available at: https://ria.ru/20191210/1562217842.html (date of access: 01/17/2022). Text: electronic.

6. Zadremaylova Veronika. *Evolyutsiya politiki KNR v oblasti informatsionnoĭ bezopasnosti* (The evolution of China's policy in the field of information security). Available at: https://www.imemo.ru/files/File/magazines/puty_miru/2020/01/07_Romashkina.pdf (date of access: 01/17/2022). Text: electronic.

7. CNLegal, 22.09.2020 (CNLegal, 09/22/2020). Available at: https://cnlegal.ru/china_economic_law/china_data_security_law_2021/ (date of access: 01/17/2022). Text: electronic.

8. *Nauchno-tehnicheskiy tsentr «GRCHTS». 20.08.2021*(Scientific and technical center "GRC". 08/20/2021). Available at: https://rdc.grfc.ru/2021/08/zakon_o_bezopacnocti_knr/ (date of access: 01/17/2022). Text: electronic.

9. *Agentstvo CNewsAnalytics. 29.10.2020. Pekin* (Agency CNewsAnalytics. 29.10.2020. Beijing). Available at: https://www.cna.com.tw/news/firstnews/202010290212.aspx (date of access 01/17/2022). Text: electronic.

10. *TASS Novosti. 2017.29.05* (TASS News. 2017.29.05). Available at: https://tass.ru/mezhdunarodnaya-panorama/4290068 (date of access: 01/17/2022). Text: electronic.

11. *Forbes. 07.04.2021* (Forbes. 04/07/2021). Available at: https://www.forbes.ru/newsroom/biznes/428037-kitay-nachal-rassledovanie-v-otnoshenii-odobrivshih-ipo-ant-group (date of access: 01/17/2022). Text: electronic.

12. *Kitay provel 50-y pusk kosmicheskikh raket v 2021 godu. 16.12.2021* (China conducted the 50th launch of space rockets in 2021. 12/16/2021). Available at: https://3dnews.ru/1056072/kitay-provyol-50y-pusk-kosmicheskih-raket-v-2021-godu (date of access: 01/17/2022). Text: electronic.

13. *Rambler. 23.07.2019* (Rambler. 07/23/2019). Available at: https://finance.rambler.ru/other/42540367/?utm_content=finance_media&utm_medium=read_more&utm_source=copylink (date of access 01/17/2022). Text: electronic.

14. Koshurnikova N. A. *Osobennosti informatsionnoy politiki sovremennogo Kitaya* (Features of the information policy of modern China. 2016. Yekaterinburg). Available at: https://elar.urfu.ru/bitstream/10995/40188/1/kiis_2016_035.pdf (date of access: 01/17/2022). Text: electronic.

15. *O gosudarstvennoy bezopasnosti: Zakon KNR* [ot 01.07.2015] (On State Security: Law of the People's Republic of China [dated July 1, 2015]. Available at: https://chinalaw.center/constitutional_law/china_state_security_law_2015_russian/ (date of access 01/17/2022). Text: electronic.

16. *CNLegal*. 28.09.2020 (CNLegal. 09/28/2020). Available at:https://cnlegal.ru/china_economic_law/critical_information_infrastructure_security_2021/ (date of access: 01/17/2022). Text: electronic.

17. *D-Russia.ru*, 02.07.2021 (D-Russia.ru, 07/02/2021). Available at: https://d-russia.ru/o-sovremennoj-politike-kitaja-v-kiberprostranstve.html (date of access: 01/17/2022). Text: electronic.

18. *Ob utverzhdenii Kontseptsii vneshney politiki Rossiyskoy Federatsii: Ukaz Prezidenta RF* [ot 30 noyabrya 2016 g. № 640] (On approval of the Foreign Policy Concept of the Russian Federation: Decree of the President of the Russian Federation [dated by November 30, 2016 No. 640]). Available at:https://www.garant.ru/products/ipo/prime/doc/71452062/ (date of access: 01/17/2022). Text: electronic.

19. *Zakon.ru.* 17.09.2021 (Zakon.ru. 09/17/2021). Available at: https://zakon.ru/blog/2021/09/17/obzor_zakona_knr_o_zaschite_personalnoj_informaciipersonal_information_protection_law_of_the_peoples#_ftn3 (date of access: 01/17/2022). Text: electronic.

20. *Interfaks. 08.06.2020*(Interfax. 06/08/2020. Available at: https://www.interfax.ru/pressreleases/712249 (date of access: 01/17/2022). Text: electronic.

21. *Sinkhua, Tsentralny komitet Kommunisticheskoy partii Kitaya i Gosudarstvenny Sovet izdali «Plan gosudarstvennogo stroitelstva v usloviyah verhovenstva zakona (2021–2025)»* (Xinhua, the Central Committee of the Communist Party of China and the State Council issued the "Plan of Nation Building Under the Rule of Law (2021-2025)". 11.08.2021. Beijing). Available at: http://www.xinhuanet.com/2021-08/11/c_1127752490.htm (date of access 01/17/2022). Text: electronic.

22. *ChinaStocks.Ne. 19.01.2022. Moskva* (ChinaStocks.Ne. 01/19/2022. Moscow). Available at: https://chinastocks.net/china-2/negativnyj-spisok-ipo/?lang=ru (date of access: 01/17/2022). Text: electronic.

23. *China Issued Draft Provisions on the Management of Automobile JDSupra. Data Security. 14.06.2021* (23. China Issued Draft Provisions on the Management of Automobile JDSupra. data security. 06/14/2021. Available at: https://www.jdsupra.com/legalnews/china-issued-draft-provisions-on-the-6616687/ (date of access 01/17/2022). Text: electronic.

24. *The Diplomat. 20.09.2020* (The Diplomat. 09/20/2020). Available at: https://thediplomat.com/2020/09/chinas-bid-to-write-the-global-rules-on-data-security/ (date of access 01/17/2022). Text: electronic.

25. *Highlights of 2020 World Internet Conference. 20.11.2020* (Highlights of 2020 World Internet Conference. 11/20/2020). Available at: http://www.wuzhenwic.org/2020-11/20/c_565230.htm (date of access: 01/17/2022). Text: electronic.

26. *Personal Information Protection Law of the People's Republic of China (Draft) (Second Review Draft)* (Personal Information Protection Law of the People's Republic of China (Draft) (Second Review Draft). April 2021). Available at: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-draft-second-review-draft/ (date of access: 01/17/2022). Text: electronic.

Информация об авторе

Меньшиков Петр Витальевич, канд. ист. наук, доцент, зав. кафедрой медийной политики и связей с общественностью, Московский государственный институт международных отношений (Университет) МИД России, г. Москва. Россия. Область научных интересов: реклама и связи с общественностью в международной деятельности, мировые политические процессы, региональная политика
p.menshikov@odin.mgimo.ru

Михина Лаурита Константиновна, ассистент кафедры медийной политики и связей с общественностью, Московский государственный институт международных отношений (Университет) МИД России, г. Москва. Россия. Область научных интересов: реклама и связи с общественностью в международной деятельности, мировые политические процессы, региональная политика
mik-laura888@yandex.ru

Information about the author

Petr Menshikov, candidate of historical sciences, associate professor, head of the Media Policy and Public Relations department, Moscow State Institute of International Relations of the Ministry of Foreign Affairs of Russia, Moscow, Russia. Scientific interests: advertising and public relations in international activities, global political processes, regional policy

Laurita Mikhina, assistant, Media Policy and Public Relations department, MGIMO, Ministry of Foreign Affairs of Russia, Moscow, Russia. Scientific interests: advertising and public relations in international activities, global political processes, regional policy

Для цитирования

Меньшиков П.В., Михина Л. К. Система противодействия угрозам информационной безопасности КНР// Вестник Забайкальского государственного университета. 2022. Т. 28, № 1. С. 124–139. DOI: 10.21209/2227-9245-2022-28-1-124-139.

Menshikov P., Mikhina L. The system of countering information security threats of the People's Republic of China // Transbaikal State University Journal, 2022, vol. 28, no. 1, pp. 124–139. DOI: 10.21209/2227-9245-2022-28-1-124-139.

Статья поступила в редакцию: 20.01.2022 г.
Статья принята к публикации: 25.01.2022 г.