Административное и муниципальное право
Правильная ссылка на статью:
Горян Э.В. — Критическая информационная инфраструктура Китайской Народной Республики: особенности правового регулирования в аспекте обеспечения информационной безопасности финансово-банковского сектора // Административное и муниципальное право. – 2020. – № 4. DOI: 10.7256/2454-0595.2020.4.32878 URL: https://nbpublish.com/library_read_article.php?id=32878

Критическая информационная инфраструктура Китайской Народной Республики: особенности правового регулирования в аспекте обеспечения информационной безопасности финансово-банковского сектора

Горян Элла Владимировна

кандидат юридических наук

доцент, Владивостокский государственный университет экономики и сервиса

690014, Россия, Приморский край, г. Владивосток, ул. Гоголя, 41, каб. 5502

ella-gorjan@yandex.ru

Статья из рубрики "АДМИНИСТРАТИВНОЕ И МУНИЦИПАЛЬНОЕ ПРАВО И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ"

DOI:

10.7256/2454-0595.2020.4.32878

Дата направления статьи в редакцию:

11-05-2020

Аннотация.

Объектом исследования являются правовые отношения, возникающие при регулировании критической информационной инфраструктуры в аспекте обеспечения информационной безопасности финансово-банковского сектора Китайской Народной Республики. Характеризуются Закон о кибербезопасности, действующие и разрабатываемые подзаконные нормативно-правовые акты Китайской Народной Республики в сфере безопасности критической информационной инфраструктуры. Исследуются особенности регламентирования отношений в сфере критической информационной инфраструктуры и их роль в обеспечении кибербезопасности финансово-банковской системы. Определяются факторы, влияющие на формирование национального механизма обеспечения безопасности критической информационной инфраструктуры С целью получения наиболее достоверных научных результатов использованы юридико-догматический подход, а также герменевтический и синергетический методы научного познания. Несмотря на многочисленность существующих и разрабатываемых источников правового регулирования критической информационной инфраструктуры, нормативный механизм обеспечения ее безопасности характеризуется взаимосвязанностью и отражает общий характер режима цифровой политики Китая. Закон о кибербезопасности КНР устанавливает общие нормы,

подзаконные акты - специальные нормы, а стандарты содержат высокотехнологические методические рекомендации, которые могут прояснить возможную неоднозначность общих и специальных норм. Однако даже в пределах этого механизма наблюдается частичное дублирование полномочий, в том числе в финансово-банковском секторе, что усложняет процесс идентификации объектов и определения субъектов критической информационной инфраструктуры. Становление механизма усложняется необходимостью одновременного достижения целей в сферах национальной безопасности и экономики, в частности при противостоянии на переговорах с США, продвигающих политику экономической экспансии на рынок Китая, используя в качестве рычагов давления тарифные и нетарифные меры.

Ключевые слова: правовой механизм, ИТ-продукты, оператор, Администрация киберпространства Китая, КИИ, Китай, критическая информационная инфраструктура, кибербезопасность, финансово-банковский сектор, сектор КИИ

Актуальность темы исследования. Последние три года правовой режим критической информационной структуры (далее КИИ) Китайской Народной Республики является предметом пристального внимания специалистов не только в сфере информационной безопасности, но и международной экономики [1]. Международный спор между США и КНР в сфере торговых отношений затрагивает не только вопросы таможенных тарифов и иных торговых барьеров: противостояние первых экономик мира касается, прежде всего, доступа к рынку в ключевых технологических секторах и снижения барьеров для трансграничной торговли [1]. Именно сфера цифровой экономики является основным вопросом повестки дня многолетних переговоров, исключить который из консультационного процесса пытается китайская сторона. Но США настаивает на неразрывности урегулирования торгового спора с согласованием нормативных предписаний в сфере информационной безопасности и защиты персональных данных, а также облачных технологий [2].

Действующий с 2017 года Закон о кибербезопасности Китайской Народной Республики (далее - Закон) [3] установил общие принципы и направления развития национального регулирования в сфере информационной безопасности государства, однако специальные нормы, касающиеся отдельных вопросов (КИИ, персональных данных) находятся в стадии разработки и согласования. Перед китайским законодателем стоит непростая задача построения сбалансированного нормативного механизма обеспечения безопасности КИИ, поскольку необходимо учесть интересы национальной безопасности и сохранить привлекательность китайского рынка для инвестиций. Подобная ситуация уже имела место в 2015 году, когда китайские власти пошли навстречу лоббистам США, ЕС и Японии и приостановили действие положения в сфере банковского сектора, требующее использование в финансово-банковских учреждениях ИТ-продуктов и сервисов исключительно китайского производства по причине их «безопасности и контролируемости». Но это требование в отношении ИТ-продуктов и услуг, тем не менее, было включено в ряд положений и стандартов в сфере кибербезопасности, как будет показано далее. Финансово-банковский сектор отнесен Законом к КИИ, поэтому для всех субъектов финансовой и банковской систем, как китайских, так и зарубежных, важно определить свою причастность к операторам КИИ и осуществлять свою деятельность в соответствии с нормативными предписаниями по кибербезопасности. Это выступает дополнительной гарантией прав инвесторов данного сектора, поскольку позволяет идентифицировать риски и осуществлять их управление. Все вышесказанное и

определяет актуальность исследования.

Постановка проблемы исследования. Вступивший в силу в 2017 году Закон о кибербезопасности КНР заложил фундамент нормативного механизма обеспечения информационной безопасности государства. Но процесс разработки и утверждения стандартов идентификации и функционирования КИИ еще не завершен, что создает неопределенность правового статуса потенциальных субъектов КИИ, в том числе и иностранных.

Цель и задачи исследования. Цель исследования – определить особенности правового регулирования КИИ в Китае в аспекте обеспечения информационной безопасности финансово-банковского сектора. Задачи исследования заключаются в характеристике процесса становления нормативного механизма регулирования КИИ; анализе основных положений как действующих нормативно-правовых актов, так и их проектов; определении особенностей регламентирования отношений в сфере КИИ и их влияния на обеспечение кибербезопасности финансово-банковской системы.

Методология. С целью получения наиболее достоверных научных результатов были использованы юридико-догматический подход, а также герменевтический и синергетический методы научного познания.

Предмет исследования, источниковая база исследования, противоречия в имеющихся исследованиях и авторская позиция. Предмет исследования составляет действующее законодательство КНР и проекты нормативно-правовых актов в сфере регулирования отношений по использованию критической информационной инфраструктуры.

Поиск в электронной библиотеке научных публикаций eLIBRARY.RU показал отсутствие проиндексированных в РИНЦ исследований по рассматриваемой теме. Косвенно она затрагивается в статье авторского коллектива Русаковой Е.П. [4] при характеристике недостатков закона о кибербезопасности в части обеспечения конфиденциальности персональных данных и сравнительно-правовом исследовании Е.П. Ермаковой и Е.Е. Фроловой о цифровом банкинге в Китае [5]. Основные положения Закона о кибербезопасности КНР в аспекте регулирования КИИ были рассмотрены нами в предыдущей статье [6]. Такой недостаток научных наработок доказывает необходимость исследования указанной темы.

Основная часть. Начиная с 2014 года вопросы определения и защиты КИИ поднимаются в каждом выступлении главы КНР на совещаниях правительства и национальных конференциях, посвященных кибербезопасности. В своей речи 2016 года о киберстратегии президент подчеркнул важность защиты таких секторов КИИ как финансы, энергетика, телекоммуникации и транспорт, а также призвал правительство ускорить работу над построением национального механизма обеспечения безопасности КИИ. В дальнейших выступлениях защита КИИ увязывалась с наращиванием потенциала отечественной кибериндустрии, консолидацией и централизацией платформ сбора информации о кибербезопасности; на регулирующие органы возлагалась функция по надзору за применением нормативных предписаний о защите КИИ, а на операторов КИИ – полная ответственность за обеспечение безопасности КИИ [7].

Следует отметить, что КИИ стала предметом регулирования еще в 2007 году, после принятия Министерством общественной безопасности КНР положения «Меры управления многоуровневой защитой информации» (Administrative Measures for Information Security

Multi-Level Protection Scheme, далее - MLPS) [8].

MLPS классифицирует все информационные системы на пять уровней в соответствии с потенциальным негативным воздействием информационных систем на национальную безопасность, общественный порядок, права и законные интересы граждан в случае угрозы информационной безопасности: (1) первый уровень – посягательство на информационные системы наносит ущерб законным интересам граждан, юридических лиц и других организаций не затрагивая национальную безопасность, общественный порядок и общественные интересы; (2) второй уровень - посягательство на информационные системы может нанести серьезный ущерб законным интересам граждан, юридических лиц и других организаций, общественному порядку и общественным интересам не затрагивая национальную безопасность; (3) третий уровень – посягательство на информационные системы может нанести серьезный ущерб общественному порядку и общественным интересам или национальной безопасности; (4) четвертый уровень - посягательство на информационные системы может нанести особенно серьезный ущерб общественному порядку и общественным интересам или серьезный ущерб национальной безопасности; (5) посягательство на информационные системы может нанести особенно серьезный ущерб национальной безопасности (ст. 7) [8].

Глава 3 MLPS регламентирует порядок определения уровней информационных систем и устанавливает режим их использования. В частности, все информационные системы третьего уровня и выше должны быть оснащены средствами защиты информационных систем, которые отвечают следующим критериям: а) для разработки и производства таких средств привлекаются инвесторы, являющиеся гражданами КНР или китайскими юридическими лицами; б) интеллектуальные права на основные технологии и ключевые компоненты средств защиты информационных систем зарегистрированы в КНР; в) отсутствие судимости у лиц, участвующих в разработке и производстве средств защиты информационных систем; г) наличие сертификата о государственной аккредитации у производителей средств защиты информационных систем (ст. 21). Подобные по жесткости требования установлены как для агентств по оценке уровня защиты (ст. 22), так и для учреждений, занимающихся оценкой степени безопасности информационных систем (ст. 23).

Отдельные главы MLPS посвящены управлению многоуровневой охраной информационных систем, составляющих государственную тайну (гл. 4), управлению системами криптографической защиты (гл. 5), ответственности за нарушение требований в отношении информационных систем выше третьего уровня (гл. 6). Эксперты отмечают, что закрепленный рассматриваемым положением подход к защите информационных систем основывается на уже недействующих критериях оценки компьютерной системы Министерства обороны США 80-х годов XX века, так называемой «Оранжевой книги» (Orange Book) [7].

В феврале 2014 года была создана Центральная ведущая группа по вопросам киберпространства, которую возглавил Генеральный секретарь ЦК КПК и президент Си Цзиньпин. Вопрос обеспечения кибербезопасности впервые был включен в отчет правительства во время Всекитайского собрания народных представителей и Народного политического консультативного совета Китая. В июне того же года состоялось первое обсуждение проекта Закона о кибербезопасности двенадцатым Всекитайским собранием народных представителей, а через два года – ноябре 2016 года на 24-й сессии Постоянного комитета 12-й сессии Всекитайского собрания народных представителей Китайской Народной Республики был принят Закон о кибербезопасности Китайской

Народной Республики.

Раздел 2 Закона устанавливает правовой режим защиты КИИ. Статья 31 содержит перечень секторов КИИ, к которым отнесены: информационно-коммуникационные услуги, энергетика, транспорт, водное хозяйство, финансы, государственные услуги и государственные сервисы электронной почты, а также указывает, что к КИИ могут быть отнесены те секторы, которые имеют значение для государственной безопасности, национальной экономики, жизнеобеспечению населения в случае их уничтожения, утраты функциональности или утери данных. На Государственный совет КНР были возложены обязанности определения объектов КИИ и мер безопасности для их защиты, а на операторов КИИ были возложены дополнительные обязанности (ст. 34), а в случае использования ими продуктов и услуг, могущих повлиять на государственную безопасность, такие продукты и услуги должны пройти специальную проверку (ст. 35).

Закон установил требование обязательного хранения всех персональных данных, используемых операторами КИИ, на территории Китая. В случае необходимости передачи этих данных за рубеж такие данные должны подвергаться проверке на предмет угрозы национальной безопасности (ст. 37). Предусмотрена обязанность операторов КИИ проводить как минимум ежегодные проверки состояния объектов КИИ и предоставлять информацию в уполномоченный орган. Статья 39 Закона содержит перечень полномочий государственного органа, ответственного за информационную безопасность (таковым является Администрация кибербезопасности Китая (Cyberspace Administration of China, далее - CAC), по планированию и координации осуществления мер по защите КИИ.

Параллельно с принятием Закона Координационным бюро кибербезопасности CAC было издано Руководство по проведению национальной инспекции кибербезопасности 2016 года, в котором был регламентирован процесс идентификации КИИ (раздел 3)[9], состоящий из 3 этапов:

1) идентификация критических операций в ключевых секторах, к которым отнесены энергетика, финансы, водное хозяйство, здравоохранение, защита окружающей среды, промышленное производство, муниципальное и государственное управление, телекоммуникации и интернет, вещание и телевидение;

2) идентификация информационных систем или систем промышленного контроля, поддерживающих критические операции;

3) идентификация КИИ, основанная на

а) зависимости критических операций от информационных систем или систем промышленного контроля и влияния на потенциальный ущерб от киберинцидентов (критичность);

б) специфичных критериях информационных систем, включающих количество посещений в сутки, количество активных пользователей, объема персональных данных и чувствительной информации; критериях для систем промышленного контроля, включающих количество серверов в дата-центрах, влияние киберинцидентов на жизнеобеспечение населения (водо-, энерго-, газо- и теплоснабжение, транспорт).

Эксперты отмечают, что представленная выше методология отражает ключевые элементы рекомендаций Европейского агентства сетевой и информационной безопасности (European Union Agency for Network and Information Security, ENISA)[7]. Основное различие между этими двумя методологиями заключается в том, что ENISA рекомендует

оценивать критичность и зависимость критически важных сервисов, прежде чем идентифицировать объекты КИИ, в то время как CAC делает акцент на критичности и зависимости конкретных объектов КИИ и дифференцирует вспомогательные роли информационных систем и промышленных систем управления для критических операций [7]. Другое заметное расхождение между этими двумя методологиями заключается в том, что исследование ENISA показало, что на втором этапе идентификация критически важных сервисов может осуществляться как с помощью централизованного подхода, когда государство идентифицирует объекты КИИ, так и с помощью децентрализованного подхода, когда идентификацию объектов КИИ осуществляют непосредственно операторы КИИ. Первый подход систематичен и более жесткий, в то время как второй – более прагматичен, поскольку операторы КИИ лучше понимают значимость и сложность объектов КИИ. По мнению экспертов, Китай использует централизованный подход к определению объема и последующей идентификации КИИ, и, вероятно, столкнулся с проблемой понимания технически сложных зависимостей объектов КИИ [7].

В 2017 году был разработан и представлен для обсуждения проект Регламента защиты критической информационной инфраструктуры (далее – Регламент защиты КИИ) [10].

В первой главе этого документа указаны общие положения защиты КИИ с распределением сфер ответственности задействованных субъектов. Во второй главе (Поддержка и защита) содержатся обязательства государственных органов по созданию действенных гарантий защиты КИИ, а также дан неисчерпывающий перечень действий, могущих нанести ущерб КИИ (ст. 16). Наибольший интерес представляет третья глава документа, в которой законодатель попытался определить пределы КИИ, оставляя перечень объектов КИИ открытым (ст. 18). По сравнению с Законом список объектов КИИ был расширен путем как включения дополнительных секторов (здравоохранение, образование, социальное обеспечение и защита окружающей среды, научные исследования и производство (оборонная промышленность, машиностроение, нефтехимическая и пищевая и фармацевтическая промышленность), средства массовой информации (радиостанции, телевизионные станции и службы новостей)), так и уточнения видов информационных сетей (радио и телевизионные сети и интернет, поставщики услуг, предоставляющие облачные вычисления, big data и другие крупные общедоступные информационные и сетевые услуги).

Критериев же для идентификации КИИ этот документ не содержит, вместо этого статья 19 содержит бланкетную норму, возлагающую на уполномоченные государственные органы обязанность по разработке руководящих принципов идентификации КИИ и организации процедуры самой идентификации. Ключевые обязанности операторов КИИ по обеспечению безопасности, установленные Законом, Регламент о защите КИИ дополняет следующими: требования к квалификации, образованию и подготовке персонала на ключевых позициях, определение ответственных сотрудников, оценка безопасности сетевых продуктов и сервисов, проверка безопасности сетевых систем, продуктов и сервисов, предоставляемых третьими лицами, техническое обслуживание только на территории Китая. Документ также устанавливает систему раннего предупреждения угроз, реагирования на чрезвычайные ситуации и оценки состояния (гл. 6), виды и формы ответственности операторов КИИ за нарушение положений регламента и индивидов за совершение правонарушений в сфере безопасности КИИ (гл. 7).

Очевидно, что применение положений этого документа должно осуществляться наряду с применением положений специального акта об идентификации КИИ, однако до сегодняшнего дня такой документ еще не разработан. Проблема заключается в том, что

идентификация КИИ – это сложная для разработки концепция, которая требует тщательного анализа и конструирования, а возможно и пересмотра, особенно в свете опыта других стран [11].

Тем временем Министерство общественной безопасности Китая с 2018 года разрабатывает проект нового положения о мерах управления многоуровневой системой защиты информации (MLPS 2.0) в аспекте защиты КИИ. В своем отчете руководитель Бюро кибербезопасности указанного Министерства, будучи одним из авторов проекта MLPS 2.0, привел примеры объектов КИИ третьего и четвертого уровней, однако методология их идентификации не была разъяснена [7]: к объектам КИИ третьего уровня он отнес центральную платформу авторизации Государственной электросетевой корпорация Китая, телекоммуникационную сеть China Unicom, группу вебсайтов Энергетической строительной корпорации Китая, а в качестве объектов КИИ четвертого уровня – систему управления питанием Государственной электросетевой корпорация Китая, оптоволоконные сети, международную сеть и сигнальный шлюз China Unicom.

В конце апреля 2020 года CAC издал ведомственное положение «Меры по проверке кибербезопасности» [12], разработанное во исполнение статьи 35 Закона, которая требует от операторов КИИ прохождения проверки безопасности, если приобретаемые и используемые ими сетевые продукты и сервисы могут затронуть национальную безопасность Китая. Первоначально для этих целей использовалось принятое в 2017 году положение «Меры по проверке безопасности сетевых продуктов и услуг (пробная версия)» [13], в соответствии с которыми CAC провела проверку кибербезопасности на ряде ключевых объектов КИИ. В 2019 году был опубликован первый проект положения «Мер по проверке кибербезопасности», а в январе 2020 года свет увидела вторая редакция проекта, после обсуждения которой был принят окончательный вариант документа.

К сетевым продуктам и услугам, подпадающим под действие этого положения, относятся базовое сетевое оборудование, компьютеры и серверы с высокой пропускной способностью, хранилища данных большой емкости, базы данных и приложения, оборудование для сетевой безопасности, службы облачных вычислений и другие сетевые продукты или услуги, которые оказывают важное влияние на КИИ (ст. 20) [12].

Одиннадцать агентств формируют межведомственный контрольный орган высокого уровня по кибербезопасности, возглавляемый CAC: Комиссия национального развития и реформ; Министерство промышленности и информационных технологий; Министерство общественной безопасности; Министерство национальной безопасности; Министерство торговли; Министерство финансов; Народный банк Китая; Государственная администрация по регулированию рынка; Национальная администрация радио и телевидения; Национальная администрация защиты государственной тайны; Государственная администрации криптографии. Эксперты предполагают, что каждый член будет осуществлять проверку кибербезопасности в своей сфере, например, Народный банк Китая будет проверять закупки операторов КИИ в финансово-банковском секторе [14]. Однако сложность может заключаться в том, что Народный банк Китая является не единственным регулятором финансово-банковской сферы, он является элементом взаимосвязанной системы финансового регулирования «один комитет, один банк и одна комиссия»: часть функций по регулированию осуществляют Комиссия по регулированию банковского страхования в Китае (China Banking and Insurance Regulatory Commission, CBIRC) и Комитет по финансовой стабильности и развитию

(Financial Stability and Development Committee, FSDC) при Государственном совете КНР. И оперативное регулирование финансово-банковской системы осуществляет как раз упомянутая комиссия: она уполномочена издавать обязательные для исполнения всеми банковскими и финансовыми учреждениями акты, определяющие меры безопасности и практики управления рисками. До принятия соответствующего отраслевого положения Народным банком Китая сложно судить о том, как эти учреждения, будучи признанными в качестве операторов КИИ, будут проходить проверку кибербезопасности. Возможно, такое отраслевое положение будет разработано Комиссией по регулированию банковского страхования в Китае.

Положение «Меры по проверке кибербезопасности» предусматривает следующие дополнительные обязанности операторов КИИ:

1) прогнозирование рисков для национальной безопасности и инициирование начала процедуры проверки кибербезопасности: при осуществлении закупки сетевых продуктов или сервисов операторы КИИ должны сначала оценить связанные с ними потенциальные риски национальной безопасности. Если таковые выявятся, то оператор КИИ должен подать заявку на проверку кибербезопасности в Бюро проверки кибербезопасности (ст. 5). Порядок самооценки таких рисков будет определяться ведомственными положениями отраслевых органов;

2) возложение на поставщиков сетевых товаров и услуг дополнительных контрактных обязательств: в соглашениях о закупках операторы КИИ должны указать, что поставщик сетевых продуктов или сервисов должен оказывать помощь в проверке кибербезопасности и обязуется не совершать такие действия, как а) незаконный сбор персональных данных пользователей; б) незаконный контроль или манипулирование пользовательским оборудованием; в) прекращение поставок сетевых продуктов или сервисов технической поддержки без объяснения причин (ст. 6).

В рассматриваемом положении приведен перечень оцениваемых рисков (ст. 9): (1) риск незаконного контроля, вмешательства или уничтожения КИИ после использования сетевых продуктов и сервисов, а также кражи, утечки и повреждения важных данных; (2) риск прекращения поставок сетевых продуктов и сервисов для обеспечения непрерывности функционирования КИИ; (3) безопасность, открытость, прозрачность сетевых продуктов и сервисов, разнообразие источников, надежность каналов поставок и риск перебоев в поставках из-за политических, дипломатических, торговых и других факторов; (4) соблюдение поставщиками сетевых продуктов и сервисов законодательства КНР; (5) другие факторы, которые могут поставить под угрозу национальную безопасность и безопасность КИИ. Эксперты отмечают, что в положение не были включены предполагавшиеся в проектах риск воздействия на национальную оборону Китая и связанные с ней технологии и собственность, а также риск приобретения сетевых продуктов и сервисов, финансированных либо подконтрольных зарубежным государствам [14].

Тем не менее, даже с принятием этого документа неопределенность все еще остается, в частности в отношении идентификации объектов и соответственно операторов КИИ. На пресс-конференции по поводу принятия положения представитель CAC на вопрос об идентификации объектов КИИ сослался на документ видимо для служебного пользования, поскольку он недоступен для ознакомления (Уведомление по вопросам, связанным с защитой безопасности критически важной информационной инфраструктуры,《关于关键信息基础设施安全保护工作有关事项的通知》) и привел примеры предположительно из этого документа: телекоммуникации, радио и телевидение,

энергетика, финансы, автомобильный и водный транспорт, железные дороги, гражданская авиация, почта, водное хозяйство, управление чрезвычайными ситуациями, здравоохранение, социальное обеспечение, имеющие к национальной обороне наука, технологии и промышленность [15].

В отношении оборудования, которое используется в объектах КИИ, предполагается принятие положения «Меры по проверке безопасности сетевого оборудования КИИ», проект которого был представлен для публичного обсуждения в 2019 году [16]. Это положение принимается во исполнение требований статьи 23 Закона о кибербезопасности Китая.

Отдельное положение будет принято в отношении информации об угрозах кибербезопасности (предусмотренное статьей 26 Закона, требующее от уполномоченных субъектов публиковать информацию о кибербезопасности, такую как уязвимости системы, компьютерные вирусы, сетевые атаки или сетевые вторжения), пока что представлен проект 2019 года – «Меры по публикации информации об угрозах кибербезопасности» [17]).

Ранее проект правил, опубликованный Министерством промышленности и информационных технологий в июне 2019 года, уже устанавливал обязательства по управлению уязвимостью, включая требования к субъектам, публикующим информацию об уязвимостях (ст. 6 Положения об управлении уязвимостями кибербезопасности (проект для комментариев) [18]). Однако в проекте этого положения требования уточняются и расширяются: запрещается публикация определенных деталей, например, исходного кода вредоносного программного обеспечения (ст. 4), устанавливается необходимость предварительного уведомления государственных органов перед публикацией отчетов об угрозах кибербезопасности (ст. 5).

Выводы. Правовое регулирование критической информационной инфраструктуры в Китая имеет свои особенности. Определение критической информационной инфраструктуры дается в Законе о кибербезопасности КНР как путем перечисления относящихся к ней секторов, так и путем указания признаков, по которым иные секторы могут быть отнесены к ней. Однако в подзаконных нормативных актах сфера критической информационной инфраструктуры расширяется за счет включения новых секторов, что свидетельствует о возрастающей роли стандартов, принимаемых ответственными органами, в частности, Администрацией киберпространства КНР, Министерством промышленности и информационных технологий КНР и Министерством общественной безопасности КНР, которые уполномочены разработать, помимо прочего, положение об идентификации объектов критической информационной инфраструктуры. Непосредственную разработку стандартов осуществляет Национальный комитет по стандартизации информационной безопасности (National Information Security Standardization Committee), известный как TC260, который подчиняется Администрации киберпространства КНР. До сих пор неясно, сколько стандартов, связанных с критической информационной инфраструктуры, будет разработано, но их насчитывают уже порядка десяти [19]. Одной из проблем законодателя является определение критериев, по которым определяется статус оператора критической информационной инфраструктуры, например, количество пользователей. Этот критерий очень важен для определения в качестве операторов КИИ субъектов электронной торговли, облачных сервисов и big data.

Несмотря на многочисленность существующих и разрабатываемых источников правового

регулирования критической информационной инфраструктуры, нормативный механизм обеспечения ее безопасности характеризуется взаимосвязанностью и отражает общий характер режима цифровой политики Китая. Закон о кибербезопасности КНР устанавливает общие нормы, подзаконные акты - специальные нормы, а стандарты содержат высокотехнологические методические рекомендации, которые могут прояснить возможную неоднозначность общих и специальных норм. Однако даже в пределах этого механизма наблюдается частичное дублирование полномочий Министерства общественной безопасности КНР как регулятора по мерам управления многоуровневой защитой информации и Администрации киберпространства КНР как регулятора критической информационной инфраструктуры, что, по мнению экспертов, может усложнить процесс идентификации объектов и определения субъектов [1]. В отношении финансово-банковского сектора наблюдается схожая ситуация: Народный банк Китая как финансовый регулятор уполномочен осуществлять проверку кибербезопасности сетевых продуктов и сервисов, используемых на объектах критической информационной инфраструктуры, но подобные функции должна осуществлять Комиссия по регулированию банковского страхования в Китае, которая в рамках системы финансового регулирования уполномочена издавать обязательные для исполнения всеми банковскими и финансовыми учреждениями акты, определяющие меры безопасности и практики управления рисками. До принятия соответствующего решения Народным банком Китая сложно судить о том, как эти учреждения, будучи признанными в качестве операторов критической информационной инфраструктуры, будут проходить проверку кибербезопасности. Возможно, будет иметь место делегирование Народным банком Китая полномочий Комиссии по регулированию банковского страхования в Китае.

Становление механизма обеспечения безопасности критической информационной инфраструктуры еще не завершено и усложняется необходимостью одновременного достижения целей в сферах национальной безопасности и экономики, в частности при противостоянии на переговорах с США, продвигающих политику экономической экспансии на рынок Китая, используя в качестве рычагов давления тарифные и нетарифные меры.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта 20-011-00454 «Обеспечение прав инвесторов в банковском и финансовом секторах в условиях цифровизации экономики в РФ и ведущих финансовых центрах Восточной Азии: сравнительно-правовой аспект».

Библиография

1. Webster G. Three Chinese Digital Economy Policies at Stake in the U.S.–China Talks [Electronic resource] / G. Webster, S. Sacks, P. Triolo // New America. – URL: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/three-chinese-digital-economy-policies-at-stake-in-the-uschina-talks/
2. Wei L. U.S. Trade Negotiators Take Aim at China’s Cybersecurity Law [Electronic resource] / L. Wei, B. Davis // The Wall Street Journal. – URL: https://www.wsj.com/articles/u-s-trade-negotiators-take-aim-at-chinas-cybersecurity-law-11553867916.
3. Cybersecurity Law of the People’s Republic of China [Electronic resource] // pkulaw.com. – URL: https://pkulaw.com/en_law/4dce14765f4265f1bdfb.html.
4. Русакова Е.П. Проблемы обеспечения конфиденциальности персональных данных в условиях реализации кампании по созданию «умных городов» в Китае: недостатки

закона о кибербезопасности / Е.П. Русакова, В.П. Барулина, А.И. Горбачева // Социально-политические науки. 2018. № 5. С. 201-206.

5. Ермакова Е.П. Правовое регулирование цифрового банкинга в России и зарубежных странах (Европейский Союз, США, КНР) / Е.П. Ермакова, Е.Е. Фролова // Вестник Пермского университета. Юридические науки. 2019. № 46. С. 606-625.
6. Горян Э.В. Закон о кибербезопасности Китайской Народной Республики как ключевой инструмент обеспечения информационной безопасности финансово-банковской системы / Э.В. Горян // Административное и муниципальное право. 2020. №3. С.47-55. DOI: 10.7256/2454-0595.2020.3.32677. URL: http://e-notabene.ru/pamp/article_32677.html
7. Lu X. Scoping Critical Information Infrastructure in China: CII is a major policy challenge in implementing Xi Jinping's cybersecurity strategy [Electronic resource] / X. Lu // The Diplomat. – URL: https://thediplomat.com/2018/05/scoping-critical-information-infrastructure-in-china/
8. Меры управления многоуровневой защитой информации 2007 года (信息安全等级保护管理办法) [Электронный ресурс] // Государственный Совет КНР: официальный сайт. – Режим доступа: http://www.gov.cn/gzdt/2007-07/24/content_694380.htm
9. Руководство по проведению национальной инспекции кибербезопасности 2016 года (国家网络安全检查操作指南) [Электронный ресурс] // Государственный Совет КНР: официальный сайт. – Режим доступа: https://wlzx.hebtu.edu.cn/resources/43/20161027101045853.doc
10. Critical Information Infrastructure Security Protection Regulations (opinion-seeking draft) [translation] // China Copyright and Media. – URL: https://chinacopyrightandmedia.wordpress.com/2017/07/10/critical-information-infrastructure-security-protection-regulations/
11. Yue C. China Cybersecurity Law update: Finally, draft regulations on "Critical Information Infrastructure" [Electronic resource] / C. Yue, M. Chan, S.-M. Werner, J.Shi // Bird&Bird. – URL: https://www.twobirds.com/en/news/articles/2017/china/draft-regulations-on-critical-information-infrastructure
12. Меры по проверке кибербезопасности 2020 года (网络安全审查办法) [Электронный ресурс] // Администрация кибербезопасности КНР: официальный сайт. – Режим доступа: http://www.cac.gov.cn/2020-04/27/c_1589535450769077.htm
13. Triolo P. Interim security review measures for network products and services [Electronic resource] / P. Triolo // China Copyright and Media. – URL: https://chinacopyrightandmedia.wordpress.com/2017/05/02/interim-security-review-measures-for-network-products-and-services/
14. Luo Y. China Issues New Measures on Cybersecurity Review of Network Products and Services [Electronic resource] / Y. Luo, Z. Yu // Inside Privacy. Covington & Burling LLP. – URL: https://www.insideprivacy.com/international/china/china-issues-new-measures-on-cybersecurity-review-of-network-products-and-services/
15. Dudley L. China's Cybersecurity Reviews Eye 'Supply Chain Security' in 'Critical' Industries [Translation] [Electronic resource] / L. Dudley, G. Webster, R. Creemers, E. Kania // New America. – URL: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cybersecurity-reviews-eye-supply-chain-security-critical-industries-translation/
16. Меры по проверке безопасности сетевого оборудования КИИ (проект для комментариев) (网络关键设备安全检测实施办法(征求意见稿)) [Электронный ресурс] // Министерство промышленности и информационных технологий КНР: официальный

сайт.-Режим доступа: http://www.miit.gov.cn/n1146285/n1146352/n3054355/n3057724/n3057728/c6991606/content.html
17. Creemers R. Translation: China's 'Cybersecurity Threat Information Publication Management Measures (Draft for Comment)' [Electronic resource] / R. Creemers, G. Webster // New America. – URL: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-cybersecurity-threat-information-publication-management-measures-draft-comment/
18. Peterson D. Translation: Chinese Rules for Managing Cybersecurity Vulnerabilities Published in Draft Form [Electronic resource] / D. Peterson, R. Zhong // New America. – URL: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinese-rules-managing-cybersecurity-vulnerabilities-published-draft-form/
19. Triolo P. China's Ambitious Rules to Secure 'Critical Information Infrastructure' [Electronic resource] / P. Triolo, R. Creemers, G. Webster // New America. – URL: https://www.newamerica.org/cybersecurity-initiative/blog/chinas-ambitious-rules-secure-critical-information-infrastructure/

Результаты процедуры рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов издательства можно ознакомиться здесь.

В представленной на рецензировании научной статье: "Критическая информационная инфраструктура Китайской Народной Республики: особенности правового регулирования в аспекте обеспечения информационной безопасности финансово-банковского сектора", автором исследуется опыт Китайской народной республики в вопросах обеспечения информационной безопасности финансово-банковского сектора. Автором при написании научной статьи использованы использованы юридико-догматический подход, а также герменевтический и синергетический методы научного познания. Актуальность темы статьи не вызывает сомнений, поскольку действующий с 2017 года Закон о кибербезопасности Китайской Народной Республики (установил общие принципы и направления развития национального регулирования в сфере информационной безопасности государства, однако специальные нормы, касающиеся отдельных вопросов (КИИ, персональных данных) находятся в стадии разработки и согласования. Именно данное обстоятельство и подтверждает актуальность темы исследования. Об актуальности темы исследования также говорит и тот факт, что исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта 20-011-00454 «Обеспечение прав инвесторов в банковском и финансовом секторах в условиях цифровизации экономики в РФ и ведущих финансовых центрах Восточной Азии: сравнительно-правовой аспект». Статья написана хорошим научным стилем,грамотно по структуре и содержанию - в статье проводится анализ особенностей правового регулирования КИИ в Китае в аспекте обеспечения информационной безопасности финансово-банковского сектора, дается характеристика процесса становления нормативного механизма регулирования КИИ; анализируются основные положения как действующих нормативно-правовых актов, так и их проектов; определяются особенности регламентирования отношений в сфере КИИ и их влияния на обеспечение кибербезопасности финансово-банковской системы. Научная новизна статьи также не вызывает сомнение. Данное исследование фактически первое исследование по данной тематике, что подтверждается данными системы РИНЦ. Именно поэтому данная статья вносит большой вклад в развитие указанной проблематике. Выводы в научной статье

абсолютно аргументированы, так мы полностью поддерживаем выводы автора, что Народный банк Китая как финансовый регулятор уполномочен осуществлять проверку кибербезопасности сетевых продуктов и сервисов, используемых на объектах критической информационной инфраструктуры, но подобные функции должна осуществлять Комиссия по регулированию банковского страхования в Китае, которая в рамках системы финансового регулирования уполномочена издавать обязательные для исполнения всеми банковскими и финансовыми учреждениями акты, определяющие меры безопасности и практики управления рисками. До принятия соответствующего решения Народным банком Китая сложно судить о том, как эти учреждения, будучи признанными в качестве операторов критической информационной инфраструктуры, будут проходить проверку кибербезопасности. И безусловно, абсолютно справедлив вывод автора о том, что будет иметь место делегирование Народным банком Китая полномочий Комиссии по регулированию банковского страхования в Китае. Библиография статьи хорошая, автором использовано большое количество научной литературы как на русском языке, так и на иностранном языке. Безусловно заслуживает отдельного внимания апелляция к оппонентам, автором рассмотрены работы авторов по указанной проблематике, проанализированы их плюсы и минусы и показана собственная точка автора на существо рассматриваемой проблемы. данная статья представляет безусловный интерес для читательской аудитории, так как выполнена на актуальную тему, с соблюдением всех необходимых требований. На основании вышеизложенного считаю, что статья "Критическая информационная инфраструктура Китайской Народной Республики: особенности правового регулирования в аспекте обеспечения информационной безопасности финансово-банковского сектора" рекомендуется к публикации