Административное и муниципальное право
Правильная ссылка на статью:
Горян Э.В. — Закон о кибербезопасности Китайской Народной Республики как ключевой инструмент обеспечения информационной безопасности финансово-банковской системы // Административное и муниципальное право. – 2020. – № 3. DOI: 10.7256/2454-0595.2020.3.32677 URL: https://nbpublish.com/library_read_article.php?id=32677

Закон о кибербезопасности Китайской Народной Республики как ключевой инструмент обеспечения информационной безопасности финансово-банковской системы

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:

10.7256/2454-0595.2020.3.32677

Дата направления статьи в редакцию:

20-04-2020

Аннотация.

Объектом исследования являются правовые отношения, возникающие при обеспечении информационной безопасности финансово-банковской системы Китайской Народной Республики. Характеризуется Закон о кибербезопасности Китайской Народной Республики, который вступил в силу в 2017 году. Исследуются предметная и субъектная сфера действия этого закона. Определяются основные положения этого нормативно-правового акта, устанавливающие фундамент национального институционального и нормативно-правового механизмов обеспечения информационной безопасности финансового и банковского секторов как объектов критической информационной инфраструктуры. С целью получения наиболее достоверных научных результатов был использован ряд общенаучных (системно-структурный, формально-логический и герменевтический методы) и специального юридического метода познания (формально-юридический). Закон о кибербезопасности Китая является основополагающим нормативно-правовым актом, определяющим принципы, механизмы и порядок обеспечения информационной безопасности. В нем дано определение КИИ через перечисление секторов и указание критериев, по которым можно определить тот или иной сектора в качестве критической информационной инфраструктуры. Финансово-банковский сектор соответствует предъявляемым критериям, поэтому обеспечение его

информационной безопасности основывается на общих положениях этого закона. Закон определяет режим охраны и защиты персональных данных, а также обязанности операторов сети, которые включены в институциональный механизм обеспечения кибербезопасности. Все вышеперечисленное делает Закон о кибербезопасности Китая ключевым нормативно-правовым инструментом механизма обеспечении информационной безопасности финансово-банковской системы.

Ключевые слова: кибербезопасность, критическая информационная инфраструктура, правовой механизм, Китай, персональные данные, оператор сети, финансовая система, банковский система, киберинцидент, Администрация кибербезопасности Китая

Актуальность темы исследования. Финансово-банковская система является основной мишенью кибератак, использующих уязвимости информационно-коммуникационных систем, что определяет финансово-банковскую систему в качестве одного из секторов критической информационной инфраструктуры (далее – КИИ), в отношении которой государство выступает главным гарантом, обязанным обеспечить комплекс условий для нормального функционирования и определить круг субъектов, уполномоченных принимать меры по ее охране и защите.

Последние годы большинство государств активизировали свои действия по обеспечению информационной безопасности КИИ, не ограничиваясь просто в определении секторов КИИ, а продолжая усовершенствовать механизм, определяя порядок идентификации объектов и субъектов КИИ с последующим наделением их полномочиями, связывая все элементы в один сбалансированный и взаимосвязанный механизм. За последние несколько лет Китайская Народная Республика (далее – Китай) значительно продвинулась в совершенствовании национального механизма обеспечения безопасности КИИ, что позволило ей гарантировать стабильность функционирования финансово-банковской системы, обслуживающей одну из первых экономик мира. Особенностью Китая является особый режим автономности информационно-телекоммуникационной сети «Интернет», что определяет и особую, отличную от других государств, структуру и методику функционирования механизма безопасности. Это делает опыт Китая интересным для российских исследователей и законодателя, поскольку позволяет определить эффективность тех или иных элементов механизма обеспечения кибербезопасности. Как мы указывали ранее [1, С. 6], две основные задачи кибербезопасности заключаются в защите непосредственно информационных систем (прежде всего, КИИ) и данных, находящихся в них. Следовательно, государство должно обеспечить безопасность двух этих объектов. Для решения первой задачи государство или ограничивает свою ответственность в пределах КИИ (так называемая «классическая» модель), или берет на себя ответственность за безопасность всех информационных систем, используя специальные организационно-правовые и технические меры (так называемая «китайская» модель). Вторая задача решаема или путем возложения ответственности за сохранность данных на самих пользователей и операторов информационных систем - «либеральная» модель, или путем введения специальных требований о локализации всех данных в пределах юрисдикции государства - модель «цифрового национализма» (data nationalism). Китай взял на себя ответственность за безопасность всех информационных систем и персональных данных. Результаты использования таких моделей Китаем [2] свидетельствуют об оправданности спорных для западной правовой идеологии подходов, что в результате гарантирует стабильность финансово-банковской системы. Все вышесказанное и определяет актуальность исследования.

Постановка проблемы исследования. Китайская Народная Республика, будучи одной из первых экономик мира, постоянно совершенствует механизм кибербезопасности, реформируя не только институциональную его часть, но и нормативно-правовую. Закон о кибербезопасности определяет основные аспекты обеспечения кибербезопасности в государстве, поэтому необходимо исследовать его на предмет выявления правовых предписаний, устанавливающих вектор прилагаемых усилий по гарантированию информационной безопасности финансово-банковский системы Китая.

Цель и задачи исследования. Цель исследования – определить особенности Закона о кибербезопасности Китая как правовой основы обеспечения кибербезопасности финансово-банковской системы. Задачи исследования заключаются в характеристике основных положений этого нормативно-правового акта и определении правовых предписаний, заложенных в основу правового механизма обеспечения информационной безопасности финансово-банковской системы.

Методология. С целью получения наиболее достоверных научных результатов был использован ряд общенаучных (системно-структурный, формально-логический и герменевтический методы) и специального юридического метода познания (формально-юридический).

Предмет исследования, источниковая база исследования, противоречия в имеющихся исследованиях и авторская позиция. Предмет исследования составляет Закон о кибербезопасности Китайской Народной Республики 2017 года - основной нормативно-правовой акт в сфере регулирования деятельности субъектов обеспечения информационной безопасности в Китае.

Поиск в электронной библиотеке научных публикаций eLIBRARY.RU показал, что проиндексированные в РИНЦ исследования по теме представлены двумя научными статьями: недостатки закона о кибербезопасности в части обеспечения конфиденциальности персональных данных были рассмотрены авторским коллективом Русаковой Е.П.[3], а Е.П. Ермакова и Е.Е. Фролова провели сравнительно-правовое исследование в сфере цифрового банкинга в Китае[4]. Такая скудность научных разработок доказывает необходимость исследования указанной темы.

Основная часть. Закон о кибербезопасности Китайской Народной Республики (Cybersecurity Law of the People's Republic of China, далее - Закон) [5] был принят на 24-й сессии Постоянного комитета 12-й сессии Всекитайского собрания народных представителей Китайской Народной Республики 7 ноября 2016 года и вступил в силу 1 июня 2017 года. Его разработка длилась два года – с 2014 года до 2016 года. До его вступления в силу в Китае действовало несколько нормативно-правовых актов, сфера действия которых охватывала основном безопасность информационно-компьютерных систем и инфраструктуры: принятое Государственным советом Китая «Положение о защите компьютерных информационных систем, об административных мерах для информационных служб Интернета» (Regulations on Security Protection of Computer Information Systems, Administrative Measures for Internet Information Services), утвержденные Министерством общественной безопасности «Административные меры по предотвращению заражения и лечению компьютерных вирусов» (Administrative Measures for Prevention and Treatment of Computer Viruses) и «Административные меры по многоуровневой защите информационной безопасности» (Administrative Measures for Hierarchical Protection of Information Security), а также принятый Постоянным комитетом Всекитайского собрания народных представителей Китая Закон об охране

государственной тайны (Law on Guarding State Secrets).

Закон состоит из семи глав: (1) общие положения; (2) обеспечение и продвижение кибербезопасности; (3) безопасность работы сети, включающей два раздела: общие положения и безопасность операций на объектах критической информационной инфраструктуры; (4) безопасность информации в сети; (5) мониторинг, профилактика и реагирование на кибератаки; (6) юридическая ответственность; (7) дополнительные положения.

Определение понятий, используемых в Законе, дается в главе VII «Заключительные положения» (ст. 76). Сеть означает систему, которая состоит из компьютеров или других информационных терминалов и соответствующего оборудования для сбора, хранения, передачи, обмена и обработки информации в соответствии с определенными правилами и процедурами (ст. 76(1)). В качестве «оператора сети» Закон рассматривает владельцев и администраторов сети, а также поставщиков сетевых услуг (ст. 76(3)). Сетевые данные означают все виды электронных данных, которые собираются, хранятся, передаются, обрабатываются и генерируются через сеть (ст. 76(4)). К персональным данным относят все виды информации, записанные в электронной или другой форме, которые могут использоваться независимо или в сочетании с другой информацией для идентификации личности физического лица, включая, помимо прочего, имя физического лица, дату рождения, номер удостоверения личности, биометрические данные, адрес и номер телефона (ст. 76(5)).

В главе I «Общие положения» указаны цели, на достижение которых направлен Закон (ст. 1), сфера применения – создание, эксплуатация, обслуживание и использование сетей, а также надзор и управлению информационной безопасностью на территории Китайской Народной Республики (ст. 2). Статья 3 устанавливает принципы обеспечения кибербезопасности: паритет информационной безопасности и информационного развития, принцип научного развития, правового управления и обеспечения безопасности, содействие созданию сетевой инфраструктуры, поощрение инноваций и применения сетевых технологий, поддержка развития человеческого капитала в сфере кибербезопасности, создание и совершенствование систему гарантий кибербезопасности и расширение возможностей информационной безопасности. На государство возложены следующие обязанности:

а) разработка и совершенствование стратегии кибербезопасности с определением основных требований и целей, разработкой политик, дорожных карт и мер в ключевых сферах (ст. 4);

б) принятие эффективных мер мониторинга и защиты от угроз как внутри, так и за пределами государства, защита КИИ от атак, преследование за незаконную деятельность в сети в соответствии с законом, поддерживать безопасность и порядок в киберпространстве (ст. 5);

в) поощрение законопослушного поведения в сети, способствование распространению основных социалистических ценностей и принятие мер для повышения осведомленности и уровня кибербезопасности всего общества с его вовлечением в механизм информационной безопасности (ст. 6);

г) международное сотрудничество в сфере управления киберпространством, осуществления исследований и разработок сетевых технологий и стандартов, пресечения преступлений и создания многосторонней, демократической и прозрачной системы киберуправления (ст. 7);

д) защита прав граждан, юридических лиц и других организаций, обеспечение доступа к сети, предоставление качественных, безопасных и удобных услуг связи, обеспечение упорядоченного и свободного потока информации в соответствии с законом (ст. 12);

е) защита несовершеннолетних от информации, способной навредить их физическому и психическому здоровью (ст. 13);

ж) разработка национальных стандартов для обеспечения безопасности и стабильной работы сети, эффективного реагирования на киберинциденты, предотвращения преступных действий и поддержания целостности, конфиденциальности и доступности сетевых данных (ст. 10).

Для реализации этих обязанностей предусмотрено создание специального государственного органа, ответственного за общее планирование, координацию и надзор в сфере кибербезопасности, наряду с созданием компетентных подразделений, наделенных соответствующими функциями, во всех органах власти (ст. 8).

На частный сектор (сетевых операторов) возложены обязанности соблюдения законодательства и деловой этики, уважения общественной морали и добросовестного исполнения обязательств по обеспечению информационной безопасности, разработки кодексов поведения в области кибербезопасности, принятия на себя социальных обязанностей и подчинения распоряжениям правительства (ст.ст. 9, 11). Они, как и все остальные представители частного сектора и индивиды, обязаны выполнять требования законодательства, соблюдать общественный порядок и уважать общественную мораль, не подвергать угрозе безопасность информационных сетей и не использовать их для осуществления какой-либо деятельности, 1) направленной против национальной безопасности, чести и интересов государства, государственной власти или социалистического строя, территориальной целостности и национального единства; 2) пропагандирующей терроризм или экстремизм, этническую ненависть или дискриминацию; 3) распространяющей насилие или порнографическую информацию, дезинформацию с целью нарушения экономического и общественного порядка; 4) нарушающей репутацию, конфиденциальность, права интеллектуальной собственности или другие законные права и интересы любого другого лица (ст. 12). Представители частного сектора имеют право сообщать о поведении, которое угрожает кибербезопасности, в уполномоченные органы, при этом конфиденциальность информации об информаторе и его законные права и интересы защищаются (ст. 14).

В главе II «Поддержка и продвижение кибербезопасности» содержится перечень государственных гарантий обеспечения информационной безопасности: (1) система национальных и отраслевых стандартов администрирования кибербезопасности и безопасности сетевых продуктов, услуг и операций (ст. 15); (2) государственная поддержка ключевых отраслей и проектов в сфере технологий кибербезопасности и вовлечение частного сектора в национальные инновационные технологические проекты (ст. 16); (3) государственная поддержка системы аутентификации, обнаружения и оценки кибербезопасности (ст. 17); (4) государственная поддержка разработки технологий защиты и использования сетевых данных, доступности общедоступных ресурсов и технологических инноваций (ст. 18); (5) особая ответственность местных органов власти и средств массовой информации за цифровое просвещение пользователей (ст. 19); (6) государственная поддержка системы образования в сфере подготовки специалистов (ст. 20).

Глава III «Безопасность сетевых операций» включает два раздела, содержащих общие

положения об установленном в государстве режиме безопасности (ст.ст. 21-30) и положения о специальном режиме безопасности КИИ (ст.ст. 31-39). Общие положения предусматривают комплекс обязанностей операторов сети (ст. 21), требования к продуктам и услугам сети (ст. 22), обязательную сертификацию сетевого оборудования и специализированных продуктов кибербезопасности (ст. 23), обязательная идентификация пользователей (ст. 24), наличие планов реагирования на киберинциденты (ст. 25), открытость и доступность информации, относящейся к кибербезопасности (ст. 26), запрет осуществления незаконной деятельности (как прямо, так и непосредственно через предоставление другим лицам специального оборудования или программ) (ст. 27), обязанность операторов сети оказывать техническую поддержку и помощь уполномоченным органам в обеспечении безопасности и борьбы с преступностью (ст. 28), наличие системы взаимодействия операторов сети (ст. 29), запрет уполномоченным органам использовать информацию иначе как для обеспечения кибербезопасности (ст. 30).

Особое внимание для нашего исследования представляет раздел 2, посвященный специальному режиму защиты КИИ. Закон дает перечень секторов КИИ (ст. 31): это информационно-коммуникационные услуги, энергетика, транспорт, водное хозяйство, финансы, государственные услуги и государственные сервисы электронной почты, а также 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 возложены обязанности определения объектов КИИ и мер безопасности для их защиты, а операторы сети поощряются к добровольному участию в механизме защиты КИИ. В отношении КИИ на операторов сети 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 устанавливает 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 (Cybersecurity Administration of China, CAC), по планированию и координации осуществления мер по защите КИИ (ст. 39).

Глава IV Закона определяет режим защиты информации в киберпространстве, прежде всего - персональных данных. В соответствии с положениями этой главы на операторов сети возложены такие обязанности как (1) обеспечение конфиденциальности информации (ст. 40); (2) обеспечение критерия необходимости и достаточности персональных данных (ст. 41); (3) обезличивание информации (ст. 42); (4) удаление информации, полученной в нарушение закона или содержащей неверные сведения (ст. 43); (5) принятие немедленных мер по защите информации в случае неправомерности ее использования (ст. 47); (6) создание системы взаимодействия с клиентами, сотрудничество с уполномоченными органами (ст. 49); (7) прекращение передачи, обработки и других операций с информацией, применение необходимых технических мер по требованию уполномоченных органов (ст. 50).

Закон также устанавливает запрет на незаконное получение и распространение информации (ст. 44) и обязанность уполномоченных органов власти соблюдать

требования конфиденциальности (ст. 45). Отдельно законом определен запрет на создание интернет страниц или средств связи для осуществления противозаконной деятельности, в том числе распространения информации о способах такой деятельности и торговли запрещенными или ограниченными в обороте средствами (ст. 46). Запрещено также распространение вредоносных программ и запрещенной (ограниченной в пользовании) информацией (ст. 48).

Меры мониторинга, профилактики и реагирования на кибератаки предусмотрены главой V рассматриваемого Закона. Полномочия по принятию таких мер возложены на уже упоминавшуюся Администрацию кибербезопасности Китая (ст.ст. 51-53). В случае возрастания угрозы киберинцидентов уполномоченные органы (подразделения народных правительств на уровне провинций или вышестоящие органы) обязаны принимать такие меры как (а) издание распоряжений соответствующим департаментам, учреждениям и персоналу своевременно собирать и представлять соответствующую информацию и усиливать мониторинг рисков кибербезопасности; (б) организация работы соответствующих подразделений, учреждений и специалистов для анализа и оценки информации о рисках кибербезопасности и прогнозирования вероятности возникновения, масштабов влияния и степени ущерба от инцидентов; (в) издание заблаговременных предупреждений о киберугрозах для общественности и объявление мер по предотвращению и уменьшению вреда от них (ст. 54).

В случае киберинцидента оператор сети должен немедленно приступить к реализации плана реагирования на него с целью расследования и оценки, а также предпринять технические и другие необходимые меры для устранения потенциальных угроз безопасности и предотвращения распространения вреда, а кроме того необходимо своевременно опубликовать информацию о случившемся (ст. 55).

Если же при осуществлении надзора и администрирования уполномоченные органы определят высокий риск возникновения или выявят киберинцидент, то они сообщают о случившемся оператору сети, который обязан принять меры для недопущения/устранения последствий (ст. 56).

Особое место в Законе занимают положения об ответственности за нарушение требований и предписаний (глава VI). Предусмотрены административный, уголовный и гражданско-правовой виды ответственности, а формы ответственности включают предупреждения, штрафы, приостановление деятельности, запрет на занятие определенных должностей, конфискация незаконных доходов, административный арест, наложение ареста на имущество и возмещение причиненного ущерба.

Выводы. Исходя из вышеизложенного, можно сделать следующие выводы. Закон о кибербезопасности Китая является основополагающим нормативно-правовым актом, определяющим принципы, механизмы и порядок обеспечения информационной безопасности. В нем дано определение КИИ через перечисление секторов и указание признаков, по которым можно определить тот или иной сектора в качестве критической информационной инфраструктуры. Финансово-банковский сектор является таковым, поэтому обеспечение его информационной безопасности начинается с общих положений этого закона. Следует отметить также отдельную главу, определяющую режим охраны и защиты персональных данных, а также обязанности операторов сети, которые включены в институциональный механизм обеспечения кибербезопасности. Поэтому Закон о кибербезопасности Китая является ключевым нормативно-правовым инструментом такого механизма.

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. Горян Э.В. Развитие российского правового механизма кибербезопасности: «особый путь» или следование в русле международных тенденций? / Э.В. Горян // Административное и муниципальное право. – 2019. – № 5. – С. 1-15.
2. Ip K. China Cybersecurity and Data Protection: a major overhaul of the proposed data localisation regime [Electronic resource] / K. Ip, M. Robinson, N. Lau, J. Gong // Lexology. – URL: https://www.lexology.com/library/detail.aspx?g=b67f553e-f736-496a-8be8-fd6ca6e5e0e7.
3. 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.
4. 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.
5. Cybersecurity Law of the People's Republic of China [Electronic resource] // pkulaw.com. – URL: https://pkulaw.com/en_law/4dce14765f4265f1bdfb.html

Результаты процедуры рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается

В представленной на рецензировании научной статье: "Закон о кибербезопасности Китайской Народной Республики как ключевой инструмент обеспечения информационной безопасности финансово-банковской системы ", автором исследуются опыт Китайской народной республики в вопросах обеспечения информационной безопасности. Автором при написании научной статьи использованы основные методы исследования: системно-структурный, формально-логический и герменевтический, а также формально-юридический. Актуальность темы статьи не вызывает сомнений, поскольку Китайская Народная Республика, будучи одной из первых экономик мира, постоянно совершенствует механизм кибербезопасности, реформируя не только институциональную его часть, но и нормативно-правовую. Закон о кибербезопасности необходимо исследовать на предмет выявления правовых предписаний, устанавливающих вектор прилагаемых усилий по гарантированию информационной безопасности финансово-банковский системы Китая. Об актуальности темы статьи также свидетельствует 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». Обращает на себя внимание правильная постановка проблемы исследования. Содержание статьи полностью соответствует названию. Статья написана хорошим научным стилем,грамотно по структуре и содержанию, в статье обозначены и раскрыты: актуальность, постановка проблемы исследования, цели и задачи исследования, методология исследования, предмет исследования, источниковая база исследования, противоречия в имеющихся

исследованиях и авторская позиция, а также авторские выводы по исследованиям. Отдельным плюсом рецензируемой научной статьи, является тот факт, что автором проанализировано полностью детально все содержание каждой главы закона,и выделены его положительные стороны. Научная новизна статьи также не вызывает сомнений: по тематике данной статьи существует всего 2 публикации и вопросы поднятые в статье ранее не обсуждались, в научной литературе. Выводы, полученные автором в ходе написания статьи, могут быть полезны также и при совершенствовании Российского законодательства по данной проблеме. Выводы в научной статье соответствуют всем требованиям, предьявляемым к научным статьям: показано, что Закон о кибербезопасности Китая является основополагающим нормативно-правовым актом, определяющим принципы, механизмы и порядок обеспечения информационной безопасности, также показаны все положительные моменты данного закона. При написании научной статьи автором достигнуты цели и задачи исследования: полностью раскрыты особенности Закона о кибербезопасности, а также даны основные характеристики основные положений данного закона. Библиография статьи хорошая, соответствует всем требованиям,предьявляемым к библиографии научных статей.Автором проанализированы все статьи, которые опубликованы по тематике исследования, а также актуальная литература по теме исследования. Статья написана на актуальную тему, с соблюдением всех требований и безусловно будет представлять интерес для читательской аудитории. На основании вышеизложенного считаю, что статья "Закон о кибербезопасности Китайской Народной Республики как ключевой инструмент обеспечения информационной безопасности финансово-банковской системы" нуждается в доработке