DOI dx.doi.org/10.24866/VVSU/2073-3984/2020-2/088-102

УДК 341.171

Э.В. Горян

Владивостокский государственный университет экономики и сервиса
Владивосток. Россия

Роль финансового регулятора в обеспечении информационной безопасности России и Китая: сравнительно-правовой аспект*

Объектом исследования являются отношения, возникающие при обеспечении информационной безопасности в финансово-банковском секторе. Характеризуется деятельность государственных финансовых регуляторов Российской Федерации и Китайской Народной Республики в сфере информационной безопасности. Выделяются и сравниваются особенности правового статуса финансовых регуляторов, определяющие координационную роль в институционально-правовом механизме обеспечения кибербезопасности. Исследуются ключевые документы, формирующие нормативно-правовые механизмы обеспечения информационной безопасности в банковско-финансовом секторе России и Китая.

С целью получения наиболее достоверных научных результатов был использован ряд общенаучных (системно-структурный, формально-логический и герменевтический методы) и специальных юридических методов познания (сравнительно-правовой и формально-юридический методы).

В России ответственность за обеспечение стабильности финансово-банковской системы несет Центральный банк Российской Федерации (Банк России), который уполномочен издавать подзаконные нормативные акты, обязательные для исполнения всеми субъектами публичного и частного секторов. В Китае финансовый регулятор представлен системой «один комитет, один банк и одна комиссия» и включает Комитет по финансовой стабильности и развитию при Государственном совете КНР,

Горян Элла Владимировна – канд. юрид. наук, доцент, доцент кафедры гражданско-правовых дисциплин; e-mail: ella.goryan@vvsu.ru

* *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».*

Народный банк Китая и Комиссию по регулированию банковского страхования. Комитет принимает ключевые макроэкономические решения, банк разрабатывает и реализует валютно-финансовую политику, а комиссия осуществляет регулирование отношений в рамках политик и принципов, разработанных первыми двумя. Сходство в статусе финансовых регуляторов заключается в наделении их широкими нормотворческими полномочиями, в том числе в сфере информационной безопасности, а также в охвате разработанными ими инструментами ключевых вопросов: безопасность информационных систем, персональные данные, система управления рисками, аутсорсинг, аудит и мониторинг. Преимуществом российского финансового регулятора является наличие в его структуре специального подразделения, оперативно реагирующего на компьютерные атаки в кредитно-финансовой сфере. Но в Китае этот вопрос относится к компетенции Администрации киберпространства Китая, центрального государственного органа, курирующего все вопросы информационной безопасности государства. Финансовые регуляторы играют важную роль в обеспечении информационной безопасности, что определяется их особым правовым статусом и видно по результатам реализации их полномочий – массиву нормативных актов, охватывающих все аспекты деятельности финансовых институтов.

Ключевые слова и словосочетания: финансовый регулятор, финансовая система, кибербезопасность, критическая информационная инфраструктура, Российская Федерация, Китай.

E.V. Gorian

Vladivostok State University of Economics and Service
Vladivostok. Russia

The role of the financial regulatory authority in information security of Russia and China: a comparative legal aspect

The object of the study is information security ensuring in the banking and financial sector. The activities of state financial regulators of the Russian Federation and the People's Republic of China in the information security are being characterized. The features of the legal status of financial regulators that determine the coordinating role in the institutional and legal mechanism for ensuring cybersecurity are highlighted and compared. The key documents that formulate the regulatory mechanisms for ensuring information security in the banking and financial sector of Russia and China are studied.

In order to obtain the most reliable scientific results, a number of general scientific (system-structural, formal-logical and hermeneutic methods) and special legal methods of cognition (comparative legal and formal-legal methods) will be used.

In Russia, the Central Bank of the Russian Federation (Bank of Russia) is responsible for ensuring the stability of the financial and banking system, and it is authorized to issue binding regulations. In China, the financial regulator is represented by the “one committee, one bank and one commission” system and includes the Financial Stability and Development Committee, the People’s Bank of China and China Banking and Insurance Regulatory Commission. The committee envisages macroprudential decisions, the bank develops and implements monetary and financial policies, and the commission regulates relations within the framework of

the policies and principles developed by the first two entities. The similarity in the status of financial regulators lies in the fact that they are vested with broad legislative powers, including in the field of information security, as well as in the coverage of the key issues regulated: information system security, personal data, risk management system, outsourcing, audit and monitoring. An advantage of the Russian financial regulator is the presence in its structure of a special unit that promptly responds to computer attacks in the credit and financial sector. But in China, this issue falls within the competence of the Cyberspace Administration of China, the central government agency that oversees all issues of state information security. Financial regulators play an important role in ensuring of information security, which is determined by their special legal status and is evident from the results of the exercise of their powers – an array of regulations covering all aspects of the activities of financial institutions..

Keywords: financial regulatory authority, financial system, cybersecurity, critical information infrastructure, Russian Federation, China.

Актуальность темы исследования. Финансово-банковский сектор является неотъемлемым элементом всех экономических отношений: от его бесперебойного функционирования зависит вся цепочка поставок и само существование субъектов экономики. Это определяет его особую важность и наделяет статусом объекта критической информационной инфраструктуры (КИИ). Проблемы в функционировании могут возникнуть как в обычной обстановке (перебои в функционировании различного происхождения: человеческий, технический, организационный факторы), так и в случае кибератак, так как именно финансово-банковский сектор становится первоочередной мишенью злоумышленников. Ответственность за безопасность объектов КИИ разделяют как специализированные государственные институты, выполняющие функции по обеспечению национальной безопасности [3, с. 55–57], так и институты, непосредственно эти объекты использующие. Как правило, первые обеспечивают общую неприкосновенность и бесперебойное функционирование компьютерных систем, а вторые – конфиденциальность и безопасность информации. В финансово-банковском секторе координирующую роль и ответственность несет финансовый регулятор, которому предоставлены специальные нормотворческие полномочия. Китайская Народная Республика (далее – Китай) является лидирующей национальной экономикой, влияющей на все международные экономические отношения. Как показала ситуация с COVID-19, замедление темпов китайской экономики привело к серьезным последствиям для всей мировой экономики. Поэтому даже вероятные риски в финансово-банковском секторе способны привести к негативным последствиям для всего мира. Осознание этой ответственности является одним из факторов, которые объясняют решительность и полномасштабность китайских властей в обеспечении информационной безопасности финансово-банковского сектора. Несмотря на то, что российский механизм обеспечения информационной безопасности в финансово-банковском секторе не уступает ведущим мировым стандартам [4], изучение опыта Китая необходимо для дальнейшего совершенствования этого механизма, а также для гармонизации финансово-банковских систем и обеспечения информационной безопасно-

сти на транснациональном уровне. Все вышесказанное свидетельствует об актуальности темы исследования.

Постановка проблемы исследования. Обеспечение информационной безопасности объектов КИИ осуществляется непрерывно и совместно как публичным, так и частным секторами. На публичный сектор возложена ответственность за надлежащую координацию субъектов в рамках конкретной сферы. В финансово-банковской сфере такими полномочиями наделен финансовый регулятор, поэтому определение его роли в обеспечении информационной безопасности указанных сегментов КИИ является научно и практически обоснованным [4]. Отток инвестиций из России в течение последних лет повлек необходимость корректировки экономической политики государства. Одним из вариантов решения имеющихся проблем стало выявление положительного опыта зарубежных государств, в данном случае – Китая. Сравнение деятельности финансовых регуляторов России и Китая по обеспечению информационной безопасности и изучение положительного опыта последнего необходимо для совершенствования российского финансово-банковского сектора.

Цели и задачи исследования. Цель нашего исследования – определить преимущества и недостатки правового регулирования деятельности финансовых регуляторов России и Китая и сформулировать предложения по совершенствованию российского механизма. Задачи исследования заключаются в сравнении правового статуса субъектов, выделении отличающихся полномочий в рассматриваемой сфере и определении возможности применения положительного опыта Китая.

Методология. С целью получения наиболее достоверных научных результатов будет использован ряд общенаучных (системно-структурный, формально-логический и герменевтический методы) и специальных юридических методов познания (сравнительно-правовой и формально-юридический методы).

Предмет исследования, источниковая база исследования, противоречия в имеющихся исследованиях и авторская позиция. Предмет исследования составляют основные нормативно-правовые акты в сфере деятельности финансовых регуляторов России и Китая по обеспечению информационной безопасности, а также ряд научных исследований по теме.

Выбранная тема исследования мало представлена в российской научной литературе. Особенности применения стандарта российского финансового регулятора по обеспечению информационной безопасности организаций банковской системы анализировали В.В. Александров и Ю.В. Малий [1]. Несколько сравнительно-правовых исследований посвящены банковским системам России и Китая [2; 7], Е.П. Ермакова и Е.Е. Фролова рассматривали вопросы сравнительно-правового регулирования цифрового банкинга [5]. Однако сравнительно-правовые исследования в сфере обеспечения информационной безопасности в банковско-финансовом секторе отсутствуют.

Основная часть. Исторически система финансового регулирования Китая представляла собой объективное выражение формулы «один банк и три комиссии» и включала Народный банк Китая (People’s Bank of China, PBoC, далее –

НБК), действующий в качестве центрального банка, Комиссию по регулированию банковской деятельности (China Banking Regulatory Commission, CBRC, далее – Комиссия), Комиссию по регулированию страховой деятельности (China Insurance Regulatory Commission, CIRC) и Комиссию по регулированию ценных бумаг (China Securities Regulatory Commission, CSRC). Каждый из элементов этой системы выполнял функции регуляторов соответствующих отраслей. Однако с 2008 года в Китае начался рост так называемого «теневого» банковского сектора, представленного учреждениями, которые занимались одновременно банковской деятельностью, страхованием и ценными бумагами, поэтому государству стало трудно регулировать деятельность этих «гибридных» учреждений. На тот момент полномочия НБК в качестве центрального банка не позволяли координировать деятельность трех комиссий по регулированию и управлению постоянно меняющимся финансово-банковским сектором. Также было трудно использовать системный подход к регулированию, который обычно требует учета различных особенностей элементов финансовой системы и их взаимосвязи.

Поэтому в 2017 году был создан Комитет по финансовой стабильности и развитию (Financial Stability and Development Committee, FSDC, далее – Комитет), который является суперфинансовым регулятором непосредственно при Государственном совете КНР и возглавляется вице-премьером, имеющим более высокий статус, чем главы других регулирующих комиссий и НБК. Роль Комитета заключается в том, чтобы координировать общую стратегию управления финансовым сектором и формулировать политику на высоком государственном уровне, включая надзор за валютно-финансовой политикой и финансовым регулированием, разработку политики по управлению системными финансовыми рисками и поддержание финансовой безопасности Китая, а также предоставление рекомендаций местным органам власти в отношении финансового развития провинций [22].

Другим ключевым шагом китайского правительства стало слияние банковских и страховых регуляторов Китая, Комиссии по регулированию банковской деятельности (China Banking Regulatory Commission, CBRC) и Комиссии по регулированию страховой деятельности (China Insurance Regulatory Commission, CIRC), в один регулятор – Комиссию по регулированию банковского страхования в Китае (China Banking and Insurance Regulatory Commission, CBIRC, далее – Комиссия) в 2018 году. Однако новосозданная Комиссия утратила некоторые полномочия, присущие своим предшественницам, а именно: функцию по определению общей политики регулирования, которая была передана НБК. В результате финансовый регулятор Китая представлен взаимосвязанной системой «один комитет, один банк и одна комиссия»: Комитет является «суперрегулятором», занимает руководящую роль в координации финансовых регуляторов и реализует «макроблагоразумную» (macroprudential) политику через НБК. Он, в свою очередь, являясь центральным банком, ответствен за разработку и реализацию валютно-финансовой политики (валютный курс, межбанковское кредитование, ценные бумаги и проч.). Комиссия реализует политику, сформулированную

Комитетом и НБК, а также осуществляет мониторинг соответствия, уделяя особое внимание уменьшению доли заемных средств и смягчению систематических рисков, которые накопились на китайском финансовом рынке за последнее десятилетие. Следует отметить, что НБК не несет прямой ответственности за разработку и внедрение правил, относящихся к управлению рисками для финансовых организаций. Однако он уполномочен создавать системы внутреннего аудита и инспекции центральной банковской системы, а в годовом отчете за 2016 год было указано, что он регулярно проводит внутренние аудиты и оценки рисков для информационных систем в своем головном офисе и дочерних учреждениях [16].

В России Центральный банк Российской Федерации (Банк России) является единственным финансовым регулятором, имеющим особый конституционно-правовой статус (ст. 75 Конституции РФ). Федеральный закон от 10.07.2002 №86-ФЗ «О Центральном банке Российской Федерации (Банке России)» (далее – ФЗ-86) определяет такие функции в сфере обеспечения информационной безопасности как установление правил проведения банковских операций и осуществления расчетов; осуществление валютного контроля и банковского надзора, а также валютного регулирования (ст. 4 ФЗ-86) [13].

Остановимся на основных инструментах обеспечения информационной безопасности, разработанных финансовыми регуляторами России и Китая.

Нормативно-правовая база регулирования финансово-банковской сферы Китая является трехуровневой. В ее основе лежат три закона, принятые Всекитайским собранием народных представителей (National People’s Congress), высшим законодательным органом Китая: 1) Закон КНР о Народном банке Китая 1995 года в редакции 2003 года (Law of the People’s Republic of China on the People’s Bank of China) [27]; 2) Закон КНР о коммерческих банках 1995 года в редакции 2015 года (Law of the People’s Republic of China on Commercial Banks); 3) Закон КНР о регулировании и надзоре за банковской деятельностью 2003 года в редакции 2006 года (Law of the People's Republic of China on Regulation of and Supervision over the Banking Industry). Второй уровень состоит из административных норм и правил, принятых Государственным советом, высшим административным органом Китая. Они уполномочивают Комиссию на регулирование определенного аспекта финансово-банковской системы, а она издает соответствующие руководства и стандарты, которые финансовые учреждения обязаны исполнять. Такие документы Комиссии и документы Народного банка Китая составляют третий уровень наиболее многочисленных нормативных актов: руководства (guidance), предписания (notice) и правила (rule). Поскольку особенностью китайской правовой системы является предпочтение конкретных правовых предписаний общим, то именно подзаконные нормативные акты выступают в качестве основных источников права. Поэтому именно третий уровень нормативных актов служит основой для финансово-банковского регулирования в Китае [22].

Комиссия уполномочена издавать обязательные для исполнения всеми банковскими и финансовыми учреждениями акты, определяющие меры безопасности и практики управления рисками.

Первым инструментом, разработанным финансовым регулятором в сфере кибербезопасности, считается изданное Комиссией по регулированию банковской деятельности в 2009 году Руководство по управлению рисками в сфере информационных технологий коммерческого банка (Commercial Bank Information Technology Risk Management Guidelines 2009) [20]. В нем подробно изложены политики, стратегии и средства контроля в сфере информационной безопасности: от разработки и тестирования информационных систем до планирования непрерывности бизнеса и управления рисками в случае ИТ-аутсорсинга. Это руководство в значительной степени было основано на международных стандартах и передовых практиках: стандартах ISO27000 для средств управления информационной безопасностью, передовой практике COBIT и ITIL, а также Базельских основных принципах управления непрерывностью бизнеса (Basel Core Principles for business continuity management) [30].

Требования в отношении внутреннего контроля были уточнены в трех последующих документах. В 2010 году в Руководстве по осуществлению внутреннего контроля информационных систем предприятия (Enterprise Internal Control Application Guide for Information Systems) были изложены требования в отношении процессов обеспечения информационной безопасности банков, включая установку программного обеспечения для обеспечения безопасности; создание системы управления пользователями и правами доступа; использование брандмауэров, сканирование уязвимостей и обнаружение вторжений для защиты от атак [24]. В Руководстве по осуществлению динамического мониторинга показателей ИТ-рисков коммерческих банков 2015 года (Guidance on Dynamic Monitoring Indicators for IT Risk of Commercial Banks 2015) были определены восемь показателей, ориентируясь на которые банкам рекомендуется осуществлять мониторинг, чтобы улучшить свое состояние информационной безопасности, включая доступность системы, частоту успешных обновлений системы, частоту блокирования фишинговых веб-сайтов и количество событий безопасности [23]. Третьим документом стало Руководство по проведению экспертизы по управлению рисками в сфере информационных технологий (On-site Examination Manualon IT Risk Management), которое содержит описание 300 ключевых факторов риска для информационных систем, а также методов и процедур обеспечения соответствия правилам регулятора [29]. Разработаны также конкретные рекомендации относительно обеспечения безопасности центров обработки данных (Commercial Bank Data Center Supervision Guidelines 2010) [19].

В дополнение к вышеуказанным мерам контроля банки должны разрабатывать и реализовывать стратегии и политики управления рисками на системном уровне с целью повышения способности выявлять, управлять и снижать институциональные риски, такие, как угрозы информационной безопасности. Эти обязанности изложены в Руководстве по комплексному управлению рисками для банковских финансовых учреждений 2016 года (Comprehensive Risk Management Guidelines for Banking Financial Institutions 2016) [21], Руководстве по консолидированному управлению и надзору в коммерческих банках 2014 года (Guidelines for Consolidated Management and Supervision of Commercial Banks

2014) [25], Руководстве по внутреннему контролю коммерческих банков 2014 года (Guidelines on Internal Control of Commercial Banks 2014) [28] и Руководстве по управлению операционными рисками коммерческих банков 2007 года (Guidelines for Operational Risk Management of Commercial Banks 2007) [26].

Эти руководства обязывают все финансовые организации создавать механизмы мониторинга ИТ-рисков для защиты информационных систем и данных клиентов, разрабатывать планы аварийного восстановления в случае сбоя системы и проводить ежегодные внутренние аудиты систем управления рисками. Такие требования в значительной степени основаны на Основных принципах Базельского банковского комитета для эффективного банковского надзора (Basel Banking Committee's Core Principles for Effective Banking Supervision), что было подтверждено Международным валютным фондом [17].

Следующим ключевым фактором кибербезопасности выступает управление непрерывностью операций. Общие требования изложены в Руководстве по управлению операционными рисками 2007 года (Operational Risk Management Guidelines 2007) и Руководстве по надзору за непрерывностью бизнеса 2011 года (Business Continuity Supervision Guidelines 2011): банки обязаны составлять планы реагирования и восстановления в случае нарушения работы критических систем [18]. Непосредственно в отношении информационной безопасности Стандарты управления по реагированию на чрезвычайные ситуации важных информационных систем банков (Management Standards on Emergency Response of Banks' Important IT Systems) и Предписание об усилении безопасности важных информационных систем (Notice on Strengthening the Safety of Significant Information Systems) обязывают банки усилить защиту ключевых информационных систем от таких рисков, как средства связи и поддержка электропитания [17]. В соответствии с Руководством по надзору за непрерывностью бизнеса банки обязаны представлять ежегодные отчеты аудитов и отчеты оценивания системы управления непрерывностью операций, а Комиссия должна включить критерий оценки рисков непрерывности операций в стандарт проверки финансовых организаций.

Для осуществления своих полномочий и регулирования отношений в своей сфере Банк России издает нормативные акты, обязательные для федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, всех юридических и физических лиц (ст. 7 ФЗ-86). Эти акты имеют форму инструкций, положений и указаний.

Первым положением в сфере информационной безопасности является положение Банка России от 04.08.2005 №274-П «Об электронной информационной системе Банка России» [14], определяющее порядок обмена электронными сообщениями между финансовым регулятором и другими субъектами в целях осуществления банковских операций и других видов деятельности, предусмотренных законодательством. Указанная система включает в себя вычислительные и технические центры Банка России, которые оперируют всевозможной информацией (административной, экономической, учетной, отчетной, операционной,

о расчетных операциях и др.). Обеспечение информационной безопасности этой системы наряду со всей банковской системой России осуществляется в соответствии со Стандартом Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» [9], который охватывает такие аспекты информационной безопасности, как модели угроз и нарушителей информационной безопасности; система информационной безопасности; система менеджмента информационной безопасности и проверка/оценка информационной безопасности.

Еще одним важным инструментом обеспечения информационной безопасности является дополненное в 2018 году положение о требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств от 09.06.2012 №382-П [12]. Этот документ устанавливает обязанность финансовых операторов информировать о хакерских атаках, раскрывать размер финансового ущерба от кибератак, сертифицировать технические меры защиты информации.

В начале 2019 года финансовый регулятор утвердил положение о требованиях к защите информации в платежной системе Банка России №672-П [11], которое распространяется на объекты информационной инфраструктуры, применяемые для обработки защищаемой информации.

Российский финансовый регулятор определил операции, которые можно передавать на аутсорсинг, в частности, те, которые связаны с применением информационных технологий, обслуживанием и администрированием средств вычислительной техники, серверного и телекоммуникационного оборудования, устройств самообслуживания, с разработкой программного обеспечения; операции по хранению и обработке информации, в том числе на внешних центрах обработки данных и облачных сервисах (облачных службах); операции по обеспечению информационной безопасности организации банковской системы России и др. [10]. Соответствующим стандартом установлены допустимые виды международной сертификации по информационной безопасности: ISACA и ISC.

Непосредственное оперативное управление информационной безопасностью осуществляется через Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ) – одно из структурных подразделений Департамента информационной безопасности [15]. ФинЦЕРТ осуществляет информационное взаимодействие не только между субъектами финансовой системы, но и разработчиками антивирусного программного обеспечения, провайдерами и операторами связи, а также правоохранительными и иными государственными органами, курирующими информационную безопасность отрасли. Кроме того, ФинЦЕРТ готовит аналитические материалы о фактах кибератак и устанавливает рекомендации в области обеспечения защиты информации при осуществлении переводов денежных средств [15] на основании положений специального стандарта об управлении инцидентами информационной безопасности [8].

Перед тем как подвести итоги, остановимся на особенностях участия финансовых регуляторов в общегосударственном механизме обеспечения кибербезопасности.

В Китае обеспечение кибербезопасности в финансово-банковском секторе Комиссия осуществляет в тесном взаимодействии с Администрацией киберпространства Китая (Cybersecurity Administration of China, CAC), на которую возложены широкие полномочия по реализации Закона о кибербезопасности 2016 года (Cybersecurity Law 2016, CSL). Администрация киберпространства Китая и Министерство общественной безопасности (Ministry of Public Security, MPS) определяют порядок реализации режима информационной безопасности, установленного Законом о кибербезопасности, путем проведения проверок безопасности продуктов и услуг, предоставляемых субъектами КИИ.

Несмотря на то, что Банк России обеспечивает стойкость финансовой системы России в сфере информационной безопасности, он не был определен в качестве центра компетенций федерального проекта Программы «Цифровая экономика» по информационной безопасности (сейчас таким центром выступает ПАО «Сбербанк России», а руководителем рабочей группы по направлению «Информационная безопасность» – президент группы компаний InfoWatch Н. Касперская) [6]. Тем не менее, финансовый регулятор тесно сотрудничает через свое структурное подразделение – ФинЦЕРТ, осуществляет информационное взаимодействие не только между субъектами финансовой системы, но и разработчиками антивирусного программного обеспечения, провайдерами и операторами связи, а также правоохранительными и иными государственными органами, курирующими информационную безопасность отрасли: Федеральной службой безопасности, Национальным координационным центром по компьютерным инцидентам и Федеральной службой по техническому и экспортному контролю.

Выводы. В отличие от российского, китайский финансовый регулятор представлен тремя государственными органами. В России ответственность за обеспечение стабильности финансово-банковской системы несет Центральный банк Российской Федерации (Банк России), который уполномочен издавать подзаконные нормативные акты, обязательные для исполнения всеми субъектами публичного и частного секторов. В Китае финансовый регулятор представлен системой «один комитет, один банк и одна комиссия» и включает Комитет по финансовой стабильности и развитию при Государственном совете КНР, Народный банк Китая и Комиссию по регулированию банковского страхования. Комитет принимает ключевые макроэкономические решения, банк разрабатывает и реализует валютно-финансовую политику, а комиссия осуществляет регулирование отношений в рамках политик и принципов, разработанных первыми двумя. Сходство в статусе финансовых регуляторов заключается в наделении их широкими нормотворческими полномочиями, в том числе в сфере информационной безопасности, а также в охвате разработанными ими инструментами ключевых вопросов: безопасность информационных систем, персональные данные, система управления рисками, аутсорсинг, аудит и мониторинг. Преимуществом российского финансового регулятора является наличие в его структуре специ-

ального подразделения, оперативно реагирующего на компьютерные атаки в кредитно-финансовой сфере. Но в Китае этот вопрос относится к компетенции Администрации киберпространства Китая, центрального государственного органа, курирующего все вопросы информационной безопасности государства. Насколько удачна эта модель институционального механизма, сложно судить в рамках данной работы, поскольку мы ограничены объектом и предметом исследования. Тем не менее, и в Китае, и в России финансовые регуляторы играют важную роль в обеспечении информационной безопасности, что определяется их особым правовым статусом и видно по результатам реализации их полномочий – массиву нормативных актов, охватывающих все аспекты деятельности финансовых институтов.

1. Александров В.В., Малий Ю.В. Применение стандарта Банка России по обеспечению информационной безопасности организаций банковской системы Российской Федерации // Вестник Белгородского университета кооперации, экономики и права. – 2015. – № 2 (54). – С. 289‒292.
2. Верников А.В. Сравнительный анализ российской и китайской моделей банковских систем: пять лет спустя // Проблемы прогнозирования. – 2015. – № 2 (149). – С. 108–120.
3. Горян Э.В. Институциональные механизмы обеспечения безопасности критической информационной инфраструктуры Российской Федерации и Сингапура: сравнительно-правовой аспект // Административное и муниципальное право. – 2018. – №9. – С.49–60.
4. Горян Э.В. Роль финансового регулятора в обеспечении кибербезопасности в России и Сингапуре: сравнительно-правовой аспект // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. – 2019. – Т. 11. № 2. – С.83–101.
5. Ермакова Е.П., Фролова Е.Е. Правовое регулирование цифрового банкинга в России и зарубежных странах (Европейский Союз, США, КНР) // Вестник Пермского университета. Юридические науки. – 2019. – № 46. – С. 606–625.
6. Информационная безопасность. – Текст: электронный // Цифровая экономика России 2024: [сайт]. – URL: https://data-economy.ru/security (дата обращения: 12.04.2020).
7. Нугаев Ф.Ш. Формирование конкурентных преимуществ банковских систем России, Китая и США в концепции национальных интересов // Современные исследования основных направлений гуманитарных и естественных наук: материалы междунар. науч.-практ. конф. / под ред. И.Т. Насретдинова, 2017. – С. 722–726.
8. О вводе в действие стандарта Банка России «Безопасность финансовых (банковских) операций. Управление инцидентами информационной безопасности. О формах и сроках взаимодействия Банка России с участниками информационного обмена при выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации. СТО БР БФБО-1.5-2018»: приказ Банка России от 14.09.2018 №ОД-2403. – Текст: электронный // СПС «КонсультантПлюс»: [сайт]. – URL: http://www.consultant.ru/document/cons_doc_LAW_310165/ (дата обращения: 12.04.2020).
9. О вводе в действие стандарта Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения. СТО БР ИББС-1.0-2014»: распоряжение Банка России от 17.05.2014 №Р-399. – Текст: электронный // СПС «КонсультантПлюс»: [сайт]. – URL:

http://www.consultant.ru/document/cons_doc_LAW_163762/ (дата обращения: 12.04.2020).

10. О вводе в действие стандарта Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Управление риском нарушения информационной безопасности при аутсорсинге. СТО БР ИББС-1.4-2018»: приказ Банка России от 06.03.2018 №ОД-568. – Текст: электронный // СПС «КонсультантПлюс»: [сайт]. – URL: http://www.consultant.ru/document/cons_doc_LAW_294526/ (дата обращения: 12.04.2020).
11. О требованиях к защите информации в платежной системе Банка России (вместе с «Правилами материально-технического обеспечения формирования электронных сообщений и контроля реквизитов электронных сообщений в информационной инфраструктуре участника ССНП, а также правила материально-технического обеспечения обработки электронных сообщений и контроля реквизитов электронных сообщений в информационной инфраструктуре ОПКЦ»): положение Банка России от 09.01.2019 №672-П. – Текст: электронный // СПС «КонсультантПлюс»: [сайт]. – URL: http://www.consultant.ru/document/cons_doc_LAW_320979/ (дата обращения: 12.04.2020).
12. О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств: положение Банка России от 09.06.2012 №382-П (ред. от 07.05.2018). – Текст: электронный // СПС «КонсультантПлюс»: [сайт]. – URL: http://www.consultant.ru/document/cons_doc_LAW_131473/ (дата обращения: 12.04.2020).
13. О Центральном банке Российской Федерации (Банке России): федер. закон от 10.07.2002 №86-ФЗ (ред. от 03.04.2020). – Текст: электронный // СПС «КонсультантПлюс»: [сайт]. – URL: http://www.consultant.ru/document/cons_doc_LAW_37570/ (дата обращения: 12.04.2020).
14. Об электронной информационной системе Банка России: положение Банка России от 04.08.2005 №274-П. – Текст: электронный // СПС «КонсультантПлюс»: [сайт]. – URL: http://www.consultant.ru/document/cons_doc_LAW_55289/ (дата обращения: 12.04.2020).
15. Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ). – Текст: электронный // Банк России: [сайт]. – URL: https://www.cbr.ru/fincert/ (дата обращения: 12.04.2020).
16. Annual Report 2016 //The People's Bank of China. – URL:http://www.pbc.gov.cn/english/130739/3398661/3398676/index.html (дата обращения: 12.04.2020).
17. Assessment of Observance of Basel Core Principles for Effective Banking Supervision: People's Republic of China // International Monetary Fund. – URL: https://www.imf.org/en/Publications/CR/Issues/2017/12/26/Peoples-Republic-of-China-Financial-Sector-Assessment-Program-Detailed-Assessment-of-45516 (дата обращения: 12.04.2020).
18. Business Continuity Supervision Guidelines2011 // China Banking Regulatory Commission. – URL: http://www.chinastor.com/dp/bcm/0124361012017.html (дата обращения: 12.04.2020).
19. Commercial Bank Data Center Supervision Guidelines 2010 // China Banking Regulatory Commission. – URL: https://baike.baidu.com/item/ 商业银行数据中心监管指引/2192141 (дата обращения: 12.04.2020).

20. Commercial Bank Information Technology Risk Management Guidelines 2009 // China Banking Regulatory Commission. – URL: http://www.cbrc.gov.cn/chinese/home/docDOC_ReadView/20090601FC296F80D3957B65FFFA9EDA836D7300.html (дата обращения: 12.04.2020).
21. Comprehensive Risk Management Guidelines for Banking Financial Institutions2016// China Banking Regulatory Commission. – URL: http://www.cbrc.gov.cn/chinese/home/docDOC_ReadView/A0D2DC141DDF4781AF9EB218A883F3AC.html (дата обращения: 12.04.2020).
22. Dongyue C., Yixin H. Banking Regulation 2020: China// Global Legal Insights. – URL: https://www.globallegalinsights.com/practice-areas/banking-and-finance-laws-and-regulations/china (дата обращения: 12.04.2020).
23. Dynamic Monitoring Indicators for IT Risk of Commercial Banks// China Banking Regulatory Commission. – URL: http://www.cbrc.gov.cn/govView_810A47B1E9F04531A1DB90EEBCC93D55.html (дата обращения: 12.04.2020).
24. Enterprise Internal Control Application Guide for Information Systems // Ministry of Finance of the People's Republic of China. – URL: http://www.law-lib.com/law/law_view.asp?id=315992 (дата обращения: 12.04.2020).
25. Guidelines for Consolidated Management and Supervision of Commercial Banks 2014// China Banking Regulatory Commission. – URL: http://www.cbrc.gov.cn/chinese/home/docDOC_ReadView/27E97E0235134CBDBD5AD4F5AD0A4D42.html (дата обращения: 12.04.2020).
26. Guidelines for Operational Risk Management of Commercial Banks2007// China Banking Regulatory Commission. – URL: http://www.cbrc.gov.cn/govView_6C-25993381CA4293A804FC5DBB4B76B1.html (дата обращения: 12.04.2020).
27. Law of the People's Republic of China on The People's Bank of China // National People's Congress. – URL: http://www.npc.gov.cn/englishnpc/Law/2007-12/12/content_1383712.htm (дата обращения: 12.04.2020).
28. Notice on Issuing the Guidelines on Internal Control of Commercial Banks 2014 // China Banking Regulatory Commission. – URL: http://www.cbrc.gov.cn/EngdocView.do?docID=231AD998D90B4AE585383BF38089E194 (дата обращения: 12.04.2020).
29. On-site Examination Manual on IT Risk Management// The People's Bank of China. – URL: https://www.banklaw.com/laws/bffa-2f4699ee11e89b644ccc6a5a6fc1.html (дата обращения: 12.04.2020).
30. Comparison Map Between ISO 27001 and Bank Information Technology Risk Management Guidelines //Shanghai Anyan Information Technology Company. – URL: http://www.aryasec.com/0e2d3e35-afec-6a3d-f1eda9e9a8ade7ff/e3d03b79-1fa5-1144-c809-793c23bdf4df.shtml (дата обращения: 12.04.2020).

Транслитерация

1. Aleksandrov V.V., Malij YU.V. Primenenie standarta Banka Rossii po obespecheniyu informacionnoj bezopasnosti organizacij bankovskoj sistemy Rossijskoj Federa-cii // Vestnik Belgorodskogo universiteta kooperacii, ekonomiki i prava. – 2015. – № 2 (54). – S. 289–292.
2. Vernikov A.V. Sravnitel'nyj analiz rossijskoj i kitajskoj modelej bankovskih sistem: pyat' let spustya // Problemy prognozirovaniya. – 2015. – № 2 (149). – S. 108–120.

3. Goryan E.V. Institucional'nye mekhanizmy obespecheniya bezopasnosti kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii i Singapura: sravnitel'-no-pravovoj aspekt // Administrativnoe i municipal'noe pravo. – 2018. – №9. – S. 49–60.
4. Goryan E.V. Rol' finansovogo regulyatora v obespechenii kiberbezopasnosti v Rossii i Singapure: sravnitel'no-pravovoj aspekt // Territoriya novyh vozmozhnostej. Vest-nik Vladivostokskogo gosudarstvennogo universiteta ekonomiki i servisa. – 2019. – T. 11. № 2. – S. 83–101.
5. Ermakova E.P., Frolova E.E. Pravovoe regulirovanie cifrovogo bankinga v Rossii i zarubezhnyh stranah (Evropejskij Soyuz, SSHA, KNR) // Vestnik Permskogo univer-siteta. Yuridicheskie nauki. – 2019. – № 46. – S. 606–625.
6. Informacionnaya bezopasnost'. – Tekst: elektronnyj // Cifrovaya ekonomika Rossii 2024: [cajt]. – URL: https://data-economy.ru/security (data obrashcheniya: 12.04.2020).
7. Nugaev F.SH. Formirovanie konkurentnyh preimushchestv bankovskih sistem Rossii, Kitaya i SSHA v koncepcii nacional'nyh interesov // Sovremennye issledovaniya osnovnyh napravlenij gumanitarnyh i estestvennyh nauk: materialy mezhdunar. nauch.-prakt. konf. / pod red. I.T. Nasretdinova, 2017. – S. 722−726.
8. O vvode v dejstvie standarta Banka Rossii «Bezopasnost' finansovyh (bankovskih) operacij. Upravlenie incidentami informacionnoj bezopasnosti. O formah i sro-kah vzaimodejstviya Banka Rossii s uchastnikami informacionnogo obmena pri vyyav-lenii incidentov, svyazannyh s narusheniem trebovanij k obespecheniyu zashchity in-formacii. STO BR BFBO-1.5-2018»: prikaz Banka Rossii ot 14.09.2018 №OD-2403. – Tekst: elektronnyj // SPS «Konsul'tantPlyus»: [sajt]. – URL: http://www.consultant.ru/document/cons_doc_LAW_310165/ (data obrashcheniya: 12.04.2020).
9. O vvode v dejstvie standarta Banka Rossii «Obespechenie informacionnoj bezopas-nosti organizacij bankovskoj sistemy Rossijskoj Federacii. Obshchie polozheniya. STO BR IBBS-1.0-2014»: rasporyazhenie Banka Rossii ot 17.05.2014 №R-399. – Tekst: elektronnyj // SPS «Konsul'tantPlyus»: [sajt]. – URL: http://www.consultant.ru/document/cons_doc_LAW_163762/ (data obrashcheniya: 12.04.2020).
10. O vvode v dejstvie standarta Banka Rossii «Obespechenie informacionnoj bezopas-nosti organizacij bankovskoj sistemy Rossijskoj Federacii. Upravlenie riskom narusheniya informacionnoj bezopasnosti pri autsorsinge. STO BR IBBS-1.4-2018»: prikaz Banka Rossii ot 06.03.2018 №OD-568. – Tekst: elektronnyj // SPS «Konsul'-tantPlyus»: [sajt]. – URL: http://www.consultant.ru/document/cons_doc_LAW_294526/ (data obrashcheniya: 12.04.2020).
11. O trebovaniyah k zashchite informacii v platezhnoj sisteme Banka Rossii (vmeste s «Pravilami material'no-tekhnicheskogo obespecheniya formirovaniya elektronnyh soobshchenij i kontrolya rekvizitov elektronnyh soobshchenij v informacionnoj infra-strukture uchastnika SSNP, a takzhe pravila material'no-tekhnicheskogo obespecheniya obrabotki elektronnyh soobshchenij i kontrolya rekvizitov elektronnyh soobshchenij v informacionnoj infrastrukture OPKC»): polozhenie Banka Rossii ot 09.01.2019 №672-P. – Tekst: elektronnyj // SPS «Konsul'tantPlyus»: [sajt]. – URL: http://www.consultant.ru/document/cons_doc_LAW_320979/ (data obrashcheniya: 12.04.2020).
12. O trebovaniyah k obespecheniyu zashchity informacii pri osushchestvlenii perevodov denezhnyh sredstv i o poryadke osushchestvleniya Bankom Rossii kontrolya za soblyudeniem trebovanij k obespecheniyu zashchity informacii pri osushchestvlenii perevodov denezhnyh sredstv: polozhenie Banka Rossii ot 09.06.2012 №382-P (red. ot 07.05.2018). – Tekst: elektronnyj // SPS «Konsul'tantPlyus»: [sajt]. – URL:

http://www.consultant.ru/document/cons_doc_LAW_131473/ (data obrashcheniya: 12.04.2020).
13. O Central'nom banke Rossijskoj Federacii (Banke Rossii): feder. zakon ot 10.07.2002 №86-FZ (red. ot 03.04.2020). – Tekst: elektronnyj // SPS «Konsul'tantP-lyus»: [sajt]. – URL: http://www.consultant.ru/document/cons_doc_LAW_37570/ (data obrashcheniya: 12.04.2020).
14. Ob elektronnoj informacionnoj sisteme Banka Rossii: polozhenie Banka Rossii ot 04.08.2005 №274-P. – Tekst: elektronnyj // SPS «Konsul'tantPlyus»: [sajt]. – URL: http://www.consultant.ru/document/cons_doc_LAW_55289/ (data obrashcheniya: 12.04.2020).
15. Centr monitoringa i reagirovaniya na komp'yuternye ataki v kreditno-finansovoj sfere (FinCERT). – Tekst: elektronnyj // Bank Rossii: [sajt]. – URL: https://www.cbr.ru/fincert/ (data obrashcheniya: 12.04.2020).

Для цитирования: Горян Э.В. Роль финансового регулятора в обеспечении информационной безопасности России и Китая: сравнительно-правовой аспект // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. – 2020. – Т. 12, № 2. – С. 88–102.

For citation: Gorian E.V. The role of the financial regulatory authority in information security of Russia and China: a comparative legal aspect, *The Territory of New Opportunities. The Herald of Vladivostok State University of Economics and Service*, 2020, Vol. 12, № 2, pp. 88–102.

DOI dx.doi.org/10.24866/VVSU/2073-3984/2020-2/088-102

Дата поступления: 13.04.2020.