DOI dx.doi.org/10.24866/VVSU/2073-3984/2019-2/083-101

УДК 341.171

Э.В. Горян

Владивостокский государственный университет экономики и сервиса
Владивосток. Россия

Роль финансового регулятора в обеспечении кибербезопасности в России и Сингапуре: сравнительно-правовой аспект

Объектом исследования являются отношения, возникающие при функционировании национального правового механизма обеспечения кибербезопасности. Определяется роль государственных финансовых регуляторов в обеспечении кибербезопасности финансового и банковского секторов России и Сингапура (на примере Центрального банка Российской Федерации и Валютно-финансового управления Сингапура). Выделяются и сравниваются особенности правового статуса финансовых регуляторов, детерминирующие координационную роль в институциональном механизме обеспечения кибербезопасности. Исследуются ключевые документы, формирующие нормативно-правовые механизмы обеспечения кибербезопасности России и Сингапура. С целью получения наиболее достоверных научных результатов были использованы общенаучные (системно-структурный, формально-логический и герменевтический) и специальные юридические методы познания (сравнительно-правовой и формально-юридический). Финансовые регуляторы России и Сингапура являются субъектами, ответственными за информационную безопасность финансовой и банковской систем. С этой целью они уполномочены принимать нормативные акты, которые охватывают такие важные аспекты банковской и финансовой деятельности, как защита объектов информационной инфраструктуры и информации при осуществлении переводов денежных средств, безопасность персональных данных, аутсорсинг услуг и др. Преимуществом российского финансового регулятора является наличие в его структуре специального Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере, взаимодействующего с субъектами из публичного и частного секторов. Интересным для изучения и дальнейшего применения является опыт сингапурского финансового регулятора по сотрудничеству с научными центрами для сбора данных и моделирования киберрисков с дальнейшей разработкой средств оценки киберугроз и использованием инструментов страхования киберрисков, а также по созданию консультативной комиссии международных экспертов в сфере кибербезопасности. Заслуживают внимания и полномочия сингапурского финансового регулятора вмешиваться в процессы аутсорсинга путем издания предписания о возврате процесса из аутсор-

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

синга или смене аутсорсингового контрагента. Подтверждением и логическим продолжением декларируемой законодательством главной роли в обеспечении стабильности финансовой системы должно стать определение Банка России в качестве центра компетенций федерального проекта «Цифровая экономика», поскольку финансовый регулятор имеет для этого все организационно-правовые полномочия и материальные ресурсы (ФинЦЕРТ).

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

E.V. Gorian

Vladivostok State University of Economics and Service
Vladivostok. Russia

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

The object of the research is the relations arising from the functioning of the national cybersecurity mechanism. The role of financial regulatory authority in ensuring the cybersecurity of the financial and banking sectors of Russia and Singapore is determined (by the example of the Central Bank of the Russian Federation and the Monetary Authority of Singapore). The features of the legal status of financial regulatory authorities, which determine the coordinating role in the institutional mechanism for ensuring cybersecurity, are identified and compared. The key documents that form the regulatory mechanisms for ensuring cybersecurity of Russia and Singapore 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. Financial regulatory authorities of Russia and Singapore are entities responsible for the information security for the financial and banking systems. To this end, they are authorized to adopt regulations that cover such important aspects of banking and financial activities as the protection of critical information infrastructure and money transfers, personal data protection, outsourcing services, etc. The advantage of the Russian financial regulator is its own Special Center for Monitoring and Responding to Computer Attacks in the Credit and Financial Sphere (FinCERT) that cooperates with the public and private sectors. Interesting for study and further application is the experience of the Singapore financial regulator cooperation with research centers for data collection and modeling of cyber risks with the further development of cyber risk assessment tools and the use of cyber risk insurance tools, as well as the creation of a consultative commission of international cyber security experts. The powers of the Singapore financial regulator to interfere in the outsourcing process by issuing instructions for returning the process from the outsourcing or changing the outsourcing counterparty deserve attention. The confirmation and logical continuation of the main role declared by the legislation in ensuring the stability of the financial system should be the definition of the Bank of Russia as the center of competence of the federal project "Digital Economy", since the financial regulator has all the organizational and legal powers, and material resources (FinCERT).

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

Актуальность темы исследования. Информационные системы банковского и финансового секторов имеют статус объектов критических информационных инфраструктур (КИИ). Наряду с информационными системами энергетического и транспортного секторов они являются первоочередной мишенью компьютерных атак со стороны как преступного сообщества, так и специализированных государственных служб. Если в первом случае целью подобных атак является, как правило, получение определенной материальной выгоды или идеологического преимущества (кибертерроризм), то во втором случае цели лежат в политической плоскости, когда речь идет о международных спорах и вооруженных конфликтах. Поэтому объекты КИИ представляют собой зону ответственности прежде всего специализированных государственных институтов, выполняющих функции по обеспечению национальной безопасности [5, с. 55–57]. Но усилий одних таких институтов недостаточно, они обеспечивают всего лишь неприкосновенность и бесперебойное функционирование компьютерных систем, однако иные вопросы безопасности (например, конфиденциальность данных) остаются под ответственностью субъектов, которые используют эти системы. Особое место среди таких субъектов занимают финансовые институты, доверие к которым и зависит от обеспечения конфиденциальности и гарантийных обязательств. Координирующую роль в финансовом и банковском секторе играет финансовый регулятор, устанавливающий правила осуществления деятельности финансовыми институтами, в том числе в сфере обеспечения безопасности их функционирования [6, с. 26]. Чем более значительным для международной безопасности (например, Российская Федерация) и международной экономики (например, Сингапур) является государство, тем более серьезные атаки совершаются и на его финансовые институты. Поэтому как Российская Федерация, так и Сингапур постоянно совершенствуют свое законодательство с учетом возникающих вызовов. Существует объективная необходимость в обеспечении соответствия российского институционального механизма кибербезопасности современным вызовам и требованиям эффективности, что вынуждает обращаться не только к наработкам международных специализированных учреждений, но и опыту государств, преуспевающих в рассматриваемой сфере, в данном случае – Сингапура. Все вышесказанное свидетельствует об актуальности темы исследования.

Постановка проблемы исследования. Как отмечалось ранее в одном из наших исследований [5], обеспечение кибербезопасности КИИ осуществляется несколькими институтами публичного и частного секторов, находящимися в постоянном взаимодействии. В такой ситуации представители публичного сектора несут ответственность за координацию действий в рамках конкретного сектора КИИ. Финансовый регулятор выполняет функции по координированию и управлению отношениями в рамках финансового и банковского секторов (ст. 3, 4) [18], (ст. 4) [27], поэтому определение его роли в обеспечении информационной безопасности указанных сегментов КИИ является научно и практически обоснованным [6, с. 27]. Несмотря на общие для финансовых и банковских сфер России и

Сингапура последствия кризиса 2008–2013 гг., ситуация в Российской Федерации усугубляется еще и экономическими факторами 2014–2015 гг., повлекшими необходимость пересмотра экономической политики государства. Сравнение деятельности финансовых регуляторов России и Сингапура по обеспечению кибербезопасности и выявление положительного опыта последнего необходимы для совершенствования российского механизма кибербезопасности.

Цели и задачи исследования. Цель нашего исследования – определить преимущества и недостатки правового регулирования деятельности финансовых регуляторов Российской Федерации и Сингапура 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 Сингапура.

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

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 Сингапура по обеспечению кибербезопасности, а также ряд научных исследований по теме.

Выбранная нами для исследования тема мало представлена в российской научной литературе. Среди отечественных научных исследований роли российского финансового регулятора в обеспечении информационной безопасности банковской и финансовой систем следует отметить работу О.А. Василенко [3], где подробно изложены меры, которые Центральный банк России выделил в качестве приоритетных. Особенности применения стандарта финансового регулятора по обеспечению информационной безопасности организаций банковской системы анализировали В.В. Александров и Ю.В. Малий [1]. В.Н. Алексеев, Н.Н. Шарков изложили подходы к разработке информационно-регулятивной системы финансовой инфраструктуры [2]. Однако сравнительно-правовые исследования в указанной сфере практически отсутствуют [4, с. 108].

В зарубежной научной литературе роль финансового регулятора в обеспечении кибербезопасности представлена в работах практикующих специалистов в сфере кибербезопасности (как правило, размещаемых на официальных сайтах упоминаемых выше компаний). Поэтому в нашем исследовании мы будем обращаться к таким работам: они находятся в открытом доступе и отражают оперативную реакцию участников отношений в сфере обеспечения кибербезопасности.

Основная часть. Функцию финансового регулятора в России исполняет Центральный банк Российской Федерации (Банк России), а в Сингапуре – Валютно-финансовое управление (Monetary Authority of Singapore, далее – MAS).

Для начала охарактеризуем правовой статус финансовых регуляторов.

Сингапур. Валютно-финансовое управление Сингапура было создано в 1970 году специальным актом Парламента (Акт о Валютно-финансовом управлении

Сингапура, Monetary Authority of Singapore Act 1970) [27], в соответствии с которым MAS приступил к реализации своих полномочий по регулированию сектора финансовых услуг 1 января 1971 года. MAS получил полномочия банка и финансового агента правительства, в 1977 году – полномочия по регулированию страховой сферы, а в 1984 году – полномочия во исполнение законодательства о ценных бумагах. На сегодняшний день MAS регулирует отношения в сфере банковского дела, страхования, ценных бумаг и финансового сектора в целом.

Россия. Особый правовой статус Банка России устанавливается Конституцией Российской Федерации (ст. 75) [8], определившей его в качестве единственного субъекта защиты и обеспечения устойчивости рубля в качестве денежной единицы Российской Федерации. Он был учрежден в 1990 году на базе Российского республиканского банка Госбанка СССР. Федеральный закон от 10.07.2002 №86-ФЗ «О Центральном банке Российской Федерации (Банке России)» (далее – ФЗ-86) устанавливает статус финансового регулятора, указывая дополнительно такие цели его деятельности, как развитие и укрепление банковской системы Российской Федерации; обеспечение стабильности и развитие национальной платежной системы; развитие и обеспечение стабильности финансового рынка Российской Федерации (ст. 3) [18]. Особо следует отметить такие функции Банка России, как установление правил проведения банковских операций и осуществления расчетов; осуществление контроля (валютный) и надзора (банковский), а также валютного регулирования (ст. 4 ФЗ-86).

Как российский, так и сингапурский финансовый регуляторы курируют все финансовые институты, формируют финансовую систему путем поддержания устойчивой системы корпоративного управления и строгого соблюдения международных стандартов бухгалтерского учета.

Рассмотрим, какие инструменты используются Банком России и MAS для реализаций своих полномочий.

Сингапур. Для регулирования правоотношений MAS задействует широкий перечень инструментов. Во-первых, это принимаемые непосредственно MAS подзаконные акты (subsidiary legislation), конкретизирующие положения соответствующих актов парламента и излагающие подробные требования, которые должны соблюдаться финансовыми институтами или иными субъектами (например, представителями финансовых консультантов).

Вторую группу инструментов формируют инструкции (directions), содержащие обязательные к исполнению специфические указания финансовым институтам или особым субъектам. Они имеют силу закона, поскольку MAS определяет правовые последствия в виде привлечения к ответственности в случае определенного нарушения инструкции. Инструкции делятся на директивы (directives) и предписания (notices). Директивы содержат юридически обязательные требования к отдельному финансовому институту или указанному лицу. Исключение относится к определенному классу инструментов – Директивам для торговых банков, которые, по сути, являются «предписаниями», но по историческим причинам используется термин «директивы».

Третью группу инструментов финансового регулятора Сингапура составляют «руководства» (guidelines). Они устанавливают принципы, так называемые «стандарты лучшей практики», регулирующие поведение финансовых институтов или лиц, например, Руководство по управлению технологическими рисками для финансовых институтов (Technology Risk Management Guidelines for Financial Institutions). Нарушение таких предписаний не является правонарушением и не влечет гражданско-правовых последствий, однако степень соблюдения таких руководств влияет на общую оценку риска для конкретного института или лица.

Кодексы (codes) представляют собой систему правил, регламентирующих осуществление определенных видов деятельности. Хотя их положения не имеют силы закона, их нарушение может повлечь определенные последствия (выговор или публичное порицание). Объем и характер последствий определяется в соответствии с Актами, во исполнение которых разработан тот или иной кодекс. Практические предписания (practice notes) предназначены для руководства финансовых институтов или лиц, ответственных за административные процедуры, в случаях лицензирования, отчетности и подтверждения соответствия. Нарушение практического предписания не является правонарушением, если процедура, указанная в практическом предписании, не предусмотрена актом или регламентом. Циркуляры (circulars) – документы, адресованные конкретным лицам для их информирования или опубликованные на официальном сайте MAS для широкой общественности. Циркуляры не имеют силы закона.

Россия. Для осуществления своих полномочий и регулирования вышеуказанных отношений 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.

Инструкции определяют порядок применения положений федеральных законов, иных нормативных правовых актов (в том числе, нормативных актов Банка России) по вопросам, отнесенным к компетенции Банка России, посредством установления совокупности правил, регулирующих процесс осуществления отдельных видов деятельности в определенной области правоотношений (п. 1.4.1) [15]. Положение Банка России устанавливает системно связанные между собой правила по вопросам, отнесенным к компетенции Банка России (п. 1.4.2) [15]. В форме указания издается нормативный акт, устанавливающий отдельные правила по вопросам, отнесенным к компетенции Банка России, а также изменяющий или признающий утратившими силу нормативные или иные акты Банка России (п. 1.4.3) [15].

Кроме указанных нормативных актов финансовый регулятор может издавать иные, не являющиеся нормативными акты: официальные разъяснения, распорядительные акты, методические рекомендации, положения о структурных подразделениях, акты, содержащие исключительно технические форматы и иные технические требования (п. 1.3) [15].

Для обеспечения информационной безопасности банковского и финансового секторов финансовые регуляторы разработали ряд важных нормативных инструментов. Рассмотрим их подробнее.

Сингапур. Для регулирования отношений в сфере кибербезопасности финансовым регулятором Сингапура используются следующие инструменты: Руководство по управлению технологическими рисками (Technology Risk Management Guidelines), Руководство по аутсорсингу (Guidelines on Outsourcing), Инструкция по уведомлению об инцидентах и отчетности в MAS (Instructions on Incident Notification and Reporting to MAS) и Предписание по управлению технологическими рисками (Notice on Technology Risk Management).

В 2001 году MAS утвердило Руководство по интернет-банкингу и управлению технологическими рисками (Internet Banking and Technology Risk Management (IBTRM) Guidelines). Со временем этот документ неоднократно пересматривался: дважды в 2001 году (версии 1.0 и 1.1), в 2002 (версия 1.2), 2003 (версия 2.0) и 2008 (версия 3.0) годах. В связи с появлением новых технических инноваций – мобильных технологий, виртуализации систем – финансовые институты смогли расширить свои услуги и охват клиентов. Изобилие аутсорсинговых услуг в сфере информационных технологий привело к большой востребованности их у представителей финансового и банковского секторов. На фоне растущей зависимости от сложных информационных систем и операций в финансовом секторе наблюдался повышенный риск кибератак и системных сбоев. Поэтому MAS неоднократно указывал в циркулярах на необходимость усиления работы по управлению технологическими рисками и готовности справиться с инцидентами в области информационной безопасности и сбоями системы. В связи с этим в 2012–2013 годах Руководство по интернет-банкингу и управлению технологическими рисками было пересмотрено и расширено для лучшего управления существующими и устранения возникающих технологических рисков, с которыми сталкиваются финансовые институты. В новую редакцию руководства были включены все циркуляры по безопасности и защите данных и конечных устройств, обеспечению надежности, доступности и восстанавливаемости информационных систем и проч., в результате в 2013 году документ был издан как Руководство по управлению технологическими рисками (Technology Risk Management Guidelines) [29].

Вместе с указанным руководством в 2013 году MAS издала предписание по управлению технологическими рисками (Notice on Technology Risk Management) [28], изложив в нем требования к управлению рисками в финансово-банковском секторе, среди которых были указаны высокий уровень надежности, доступности и возможности восстановления КИИ, а также обязанность внедрения информационно-технических средств защиты информации о клиентах от несанкционированного доступа или раскрытия. Следует отметить тот факт, что рассматриваемое руководство MAS в отличие от таких стандартов безопасности, как ISO 27001 и BASEL II, усиливает требования к финансовым институтам в части борьбы с киберугрозами: необходимо усовершенствовать механизмы киберзащиты, оперативно реагировать на инциденты и держать на постоянном контроле процессы управления рисками. Финансовым институтам настоятельно

рекомендуется внедрять технологии управления технологическими рисками и методы обеспечения безопасности, включая учет и анализ инцидентов в области ИТ-безопасности, контроль над восстановлением и надежностью системы, уведомлениями о сбоях основных систем и защитой информации о клиентах.

Руководство по управлению технологическими рисками состоит из 14 разделов и 6 приложений. Тематика разделов включает: контроль технологических рисков руководством финансовых институтов; структуру технологии управления рисками; управление рисками информационно-технологического аутсорсинга; приобретение и развитие информационных систем; управление информационно-технологическими услугами; надежность, доступность и восстанавливаемость системы; управление безопасностью оперативной инфраструктуры; защита центров данных и контроль; контроль доступа; финансовые услуги онлайн; безопасность платежных карт; аудит в сфере информационных технологий. Приложение A устанавливает стандарты проверок систем безопасности и исходного кода; Приложение B – требования к устойчивости систем хранения; Приложение C посвящено использованию криптографии; Приложение D регулирует порядок использования защиты «отказ в обслуживании»; Приложение E содержит рекомендации по мерам безопасности для онлайн-систем, а Приложение F – по защите и обучению клиентов.

В 2004 году MAS издало первую версию Руководства по аутсорсингу (Guidelines on Outsourcing), которое пересматривалось в 2005, 2014–2016 и 2018 годах [22]. Основные изменения в Руководстве MAS по аутсорсингу включают следующее: 1) больше внимания уделяется внутренней системе управления рисками аутсорсинга; 2) усиливается ответственность высшего руководства финансовых учреждений; 3) устанавливается новое требование о ведении реестра аутсорсинга (Outsourcing Register); 4) отменяется ожидание уведомления MAS о существенных процессах, передаваемых на аутсорсинг; 5) дается новый перечень процессов, передаваемых на аутсорсинг, и более широкое определение таковых; 6) пересматривается определение «существенный процесс, передаваемый на аутсорсинг» со включением положений, связанных с информацией о клиентах; 7) вводятся дополнительные предписания, которые должны быть включены в контракты на аутсорсинг; 8) устанавливаются новые положения об облачном сервисе как форме аутсорсинга [24]. Руководство по аутсорсингу предусматривает обязанность финансовых институтов в течение установленного срока провести самооценку на предмет соответствия положениям руководства и устранить имеющиеся несоответствия.

Руководство по аутсорсингу состоит из 6 разделов и 3 приложений. Конкретные обязывающие предписания содержатся в разделах 4–6: обязательство перед MAS по аутсорсингу (соблюдение положений руководства; уведомление о неблагоприятных событиях); практики управления рисками (ответственность руководства финансового учреждения; оценка рисков и поставщиков услуг; мониторинг и контроль соглашений об аутсорсинге; аудит и проверки; требования в зависимости от вида аутсорсинга; облачные технологии).

Приложение 1 содержит открытый перечень процессов, передаваемых на аутсорсинг, а также перечни процессов, которые не могут быть квалифицированы как аутсорсинговые и, следовательно, переданы на аутсорсинг. Приложение 2

устанавливает критерии определения «существенных процессов», которые могут быть переданы на аутсорсинг. Приложение 3 устанавливает обязанность финансовых институтов вести реестр процессов, переданных на аутсорсинг, по форме, установленной MAS. Финансовый регулятор наделен также полномочиями по вмешательству в процессы аутсорсинга (п. 4.1.3) [22].

Инструкция по уведомлению об инцидентах и отчетности в MAS (Instructions on Incident Notification and Reporting to MAS) [23] предусматривает обязанность финансового института сообщить о киберинциденте в MAS максимум в течение одного часа. Она устанавливает перечень сведений, которые должны быть сообщены в первом уведомлении, а предписание по управлению технологическими рисками (Notice on Technology Risk Management) [28] устанавливает сроки и порядок составления подробного отчета о причинах и последствиях инцидента.

Россия. Для обеспечения обмена электронными сообщениями между финансовым регулятором и другими субъектами в целях осуществления банковских операций и других видов деятельности, предусмотренных законодательством, была создана Электронная информационная система Банка России, функционирующая в соответствии с утвержденным Положением [10] и включающая в себя вычислительные и технические центры Банка России, оснащенные аппаратными и программными средствами, в целях сбора, обработки, хранения и передачи административной, экономической, учетной, отчетной, операционной информации, информации о расчетных операциях (в том числе, платежной информации) и другой информации в соответствии с правилами и условиями, установленными в нормативных актах и организационно-распорядительных документах Банка России, договорах обмена информацией. Электронная информационная система Банка России взаимодействует с телекоммуникационной системой Банка России (п. 1.2) [10]. 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» [12], который состоит из девяти разделов, среди которых нужно отметить разделы, посвященные: 1) исходной концептуальной схеме (парадигме) обеспечения информационной безопасности организаций банковской системы; 2) моделям угроз и нарушителей информационной безопасности; 3) системе информационной безопасности; 4) системе менеджмента информационной безопасности; 4) проверке и оценке информационной безопасности.

В разделе 6 «Модели угроз и нарушителей информационной безопасности организаций банковской системы Российской Федерации» стандарта определяется иерархия основных уровней информационной инфраструктуры, обеспечивающей реализацию банковских технологий: а) физический (линии связи, аппаратные средства и пр.); б) сетевое оборудование (маршрутизаторы, коммутаторы, концентраторы и пр.); в) сетевые приложения и сервисы; г) операционные системы; д) системы управления базами данных; е) банковские технологические процессы и приложения; ж) бизнес-процессы организации (п. 6.2) [12].

Далее приводится перечень основных источников угроз информационной безопасности: 1) неблагоприятные события природного, техногенного и социального характера; 2) террористы и криминальные элементы; 3) зависимость от поставщиков/провайдеров/партнеров/клиентов; 4) сбои, отказы, разрушения/повреждения программных и технических средств; 5) работники организации банковской системы России, реализующие угрозы информационной безопасности с использованием легально предоставленных им прав и полномочий (внутренние нарушители информационной безопасности); 6) работники организации банковской системы России, реализующие угрозы информационной безопасности вне легально предоставленных им прав и полномочий, а также субъекты, не являющиеся работниками организации БС РФ, но осуществляющие попытки несанкционированного доступа и нерегламентированных действий в рамках предоставленных полномочий (внешние нарушители информационной безопасности); 7) несоответствие требованиям надзорных и регулирующих органов, действующему законодательству (п. 6.6) [12].

Рассматриваемый стандарт содержит также перечни наиболее актуальных угроз на трех основных уровнях: 1) на физическом уровне, уровне сетевого оборудования и уровне сетевых приложений (п. 6.7); 2) на уровнях операционных систем, систем управления базами данных, банковских технологических процессов (п. 6.8); 3) на уровне бизнес-процессов (п. 6.9) [12].

Раздел 7 «Система информационной безопасности организаций банковской системы Российской Федерации» содержит принципы распределения прав доступа работников и клиентов к информационным активам организации банковской системы России: а) «знать своего клиента» (know your customer); б) «знать своего служащего» (know your employee); в) «необходимо знать» (need to know); г) «двойное управление» (dual control) (п. 7.1.4). Стандарт устанавливает, что в рамках банковских платежных технологических процессов в качестве активов, защищаемых в первую очередь, следует рассматривать: 1) банковский платежный технологический процесс; 2) платежную информацию; 3) информацию, отнесенную к защищаемой информации в соответствии с пунктом 2.1 Положения Банка России от 09.06.2012 №382-П «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» в редакции Указания Банка России от 05.06.2013 №3007-У (п. 7.1.9) [12]. В указанном разделе стандарта содержатся общие требования по обеспечению информационной безопасности: а) при назначении и распределении ролей и обеспечении доверия к персоналу (п. 7.2); б) автоматизированных банковских систем на стадиях жизненного цикла (п. 7.3); в) при управлении доступом и регистрацией (п. 7.4); г) средствами антивирусной защиты (п. 7.5); д) при использовании ресурсов сети Интернет (п. 7.6); е) при использовании средств криптографической защиты информации (п. 7.7); ж) банковских платежных технологических процессов (п. 7.8); з) банковских информационных технологических процессов (п. 7.9); и) банковских технологических процессов, в рамках которых обрабатываются персональные дан-

ные (п. 7.11), а также общие требования по обработке персональных данных в организации банковской системы Российской Федерации (п. 7.10) [12].

В разделе 8 «Система менеджмента информационной безопасности организаций банковской системы Российской Федерации» изложены требования к: 1) организации и функционированию службы информационной безопасности организации банковской системы Российской Федерации (п. 8.2); 2) определению/коррекции области действия системы обеспечения информационной безопасности (п. 8.3); 3) выбору/коррекции подхода к оценке рисков нарушения информационной безопасности и проведению оценки рисков нарушения информационной безопасности (п. 8.4); 4) разработке планов обработки рисков нарушения информационной безопасности (п. 8.5); 5) разработке/коррекции внутренних документов, регламентирующих деятельность в области обеспечения информационной безопасности (п. 8.6); 6) принятию руководством организации банковской системы Российской Федерации решений о реализации и эксплуатации системы обеспечения информационной безопасности (п. 8.7); 7) организации реализации планов внедрения системы обеспечения информационной безопасности (п. 8.8); 8) разработке и организации реализации программ по обучению и повышению осведомленности в области информационной безопасности (п. 8.9); 9) организации обнаружения и реагирования на инциденты информационной безопасности (п. 8.10); 10) организации обеспечения непрерывности бизнеса и его восстановления после прерываний (п. 8.11); 11) мониторингу информационной безопасности и контролю защитных мер (п. 8.12); 12) проведению самооценки информационной безопасности (п. 8.13); 13) проведению аудита информационной безопасности (п. 8.14); 14) анализу функционирования системы обеспечения информационной безопасности (п. 8.15); 15) анализу системы обеспечения информационной безопасности со стороны руководства организации банковской системы Российской Федерации (п. 8.16); 16) принятию решений по тактическим улучшениям системы обеспечения информационной безопасности (п. 8.17); 17) принятию решений по стратегическим улучшениям системы обеспечения информационной безопасности (п. 8.18) [12].

В отношении проверки и оценки информационной безопасности организаций банковской системы России предусмотрены следующие процессы и дается их характеристика: а) мониторинг информационной безопасности и контроль защитных мер; б) самооценка информационной безопасности; в) аудит информационной безопасности; г) анализ функционирования системы обеспечения информационной безопасности (в том числе, со стороны руководства) (п. 9.1) [12].

Еще одним важным инструментом обеспечения информационной безопасности следует указать дополненное в прошлом 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 № 382-П [17]. Его подробно проанализировала О.А. Василенко в своей статье [3]. Отметим, прежде всего, такие ключевые меры, предпринимаемые финансовым регулятором, как обязанность банков и операторов по

переводу денежных средств информировать о хакерских атаках, обязанность банков раскрывать финансовый ущерб от кибератак, обязательная сертификация технических мер защиты информации.

В начале 2019 года финансовый регулятор утвердил распространяемое на объекты информационной инфраструктуры Положение о требованиях к защите информации в платежной системе Банка России №672-П [16], применяемых для обработки защищаемой информации, перечисленной в п. 2.1 Положения Банка России от 9 июня 2012 года №382-П: 1) об остатках денежных средств на банковских счетах; 2) об остатках электронных денежных средств; 3) о совершенных переводах денежных средств, в том числе об информации, содержащейся в извещениях (подтверждениях), касающихся приема к исполнению распоряжений участников платежной системы, а также в извещениях (подтверждениях), касающихся исполнения распоряжений участников платежной системы; об отнесении информации о совершенных переводах денежных средств к защищаемой информации, хранящейся в операционных центрах платежных систем с использованием платежных карт или находящейся за пределами Российской Федерации, которое устанавливается оператором платежной системы; 4) о содержащейся в оформленных в рамках применяемой формы безналичных расчетов распоряжениях клиентов операторов по переводу денежных средств, распоряжениях участников платежной системы, распоряжениях платежного клирингового центра; 5) о платежных клиринговых позициях; 6) необходимая для удостоверения клиентами права распоряжения денежными средствами, в том числе данных держателей платежных карт; 7) ключевая информация средств криптографической защиты информации, используемых при осуществлении переводов денежных средств (о криптографических ключах); 8) о конфигурации, определяющей параметры работы автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования, эксплуатация которых обеспечивается оператором по переводу денежных средств, оператором услуг платежной инфраструктуры, банковским платежным агентом (субагентом), и используемых для осуществления переводов денежных средств, а также информация о конфигурации, определяющей параметры работы технических средств защиты информации; 9) информация ограниченного доступа, в том числе персональных данных и иная информация, подлежащая обязательной защите в соответствии с законодательством Российской Федерации, обрабатываемая при осуществлении переводов денежных средств [17].

В качестве дополнительных инструментов обеспечения кибербезопасности следует отметить ряд стандартов [11; 13; 14] и Указание Банка России от 10.12.2015 №3889-У «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных» [9].

Отдельно необходимо остановиться на аутсорсинге – передаче выполнения отдельных собственных бизнес-функций на основании договорных отношений сторонним (внешним) организациям, специализирующимся на предоставлении соответствующих услуг (поставщикам услуг). Финансовый регулятор определяет

следующие бизнес-функции для возможной передачи на аутсорсинг: а) связанные с применением информационных технологий, обслуживанием и администрированием средств вычислительной техники, серверного и телекоммуникационного оборудования, устройств самообслуживания, с разработкой программного обеспечения; б) административные, включая связанные с финансовой деятельностью, функционалом back-офиса, call-центра, организационным и административным обеспечением; в) связанные с хранением и обработкой информации, в том числе на внешних центрах обработки данных и облачных сервисах (облачных службах); г) обеспечения информационной безопасности организации банковской системы России; д) административно-хозяйственные [14]. Соответствующий стандарт состоит из 12 разделов и 3 приложений. Непосредственные требования к аутсорсингу в аспекте информационной безопасности содержат разделы 5–12 (риск нарушения информационной безопасности и основные требования к управлению таким риском; оценка риска; содержание задач и зона ответственности руководства организации банковской системы; требования к проведению оценки поставщика услуг и к содержанию соглашений об аутсорсинге; мониторинг и контроль риска нарушения информационной безопасности при аутсорсинге; особенности аутсорсинга процессов информационной безопасности).

Приложение 1 устанавливает допустимые виды международной сертификации по информационной безопасности: сертификацию международной ассоциации ISACA (Information Systems Audit and Control Association) и сертификацию международного консорциума по информационной безопасности ISC (International Information Systems Security Certifications Consortium, Inc.). Приложение 2 содержит перечень вопросов для оценки политики поставщика услуг в части обеспечения информационной безопасности, а приложение 3 – примеры бизнес-функций, которые могут быть переданы на аутсорсинг.

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 [20]. 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 этого ФинЦЕРТ готовит аналитические материалы о фактах кибератак и устанавливает рекомендации в области обеспечения защиты информации при осуществлении переводов денежных средств [20] на основании положений специального стандарта об управлении инцидентами информационной безопасности [11].

Инструменты, создаваемые рассматриваемыми финансовыми регуляторами с целью регулирования информационной безопасности, охватывают основные аспекты: защита информационных систем, управление рисками, аутсорсинг, и содержат не только детальный перечень организационно-правовых мер, но и массу технических предписаний. Заслуживают внимания и рассмотрения возможности применения в российской реальности полномочий финансового регулятора в установлен-

ных законом случаях вмешиваться в процессы аутсорсинга путем издания предписания о возврате процесса из аутсорсинга или смене аутсорсингового контрагента.

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

Сингапур. Начиная с 2017 года MAS совместно с Агентством кибербезопасности Сингапура (Singapore Cyber Security Agency, центральный орган исполнительной власти, отвечающий за обеспечение информационной безопасности на уровне государства) запустил проект управления киберрисками [21], в котором принимают участие представители публичного и частного секторов. Проект осуществляется на базе Наньянгского технологического университета (Nanyang Technological University) и направлен на систематический сбор данных и моделирование киберрисков с дальнейшей разработкой средств оценки киберугроз и использованием инструментов страхования киберрисков. Среди целей проекта целесообразно отметить следующие: 1) разработку классификации киберрисков и соответствующих вариантов реагирования для каждой юрисдикции; 2) создание пакетов данных (big data) об ущербах от киберинцидентов с дальнейшим переводом в оценочные страховые претензии на основе «стандартизованного» набора определенных формулировок контракта; 3) разработку набора сценариев кибер-событий для количественной оценки воздействия и изучения риска накопления в системных событиях; 4) разработку стандартных моделей потерь для разных сценариев кибератак для ведения актуарных расчетов; 5) разработку методологии невмешательственной оценки уровня кибербезопасности финансовых институтов для поддержания их рейтинга и интеграции с процессами андеррайтинга [21].

В том же 2017 году MAS сформировал Консультативную комиссию по кибербезопасности (Cyber Security Advisory Panel, CSAP), состоящую из ведущих международных экспертов в сфере кибербезопасности, назначаемых на 2 года с возможностью продления членства. CSAP разрабатывает рекомендации для MAS и финансовых институтов для усиления безопасности финансовой системы Сингапура. Среди действующих членов комиссии – руководители подразделений кибербезопасности в сфере финансовых услуг таких компаний, как Accenture Security, IronNet Cybersecurity Inc., JP Morgan Chase & Co, London Stock Exchange Group, F-Secure, Pricewaterhousecoopers Risk Services Pte Ltd, FireEye Inc, Standard Chartered Bank, CyberArk, IBM Resilient, а также руководитель Агентства кибербезопасности Сингапура [26]. CSAP проводит консультационные встречи с Постоянным комитетом по кибербезопасности Ассоциации банков Сингапура, а также с представителями Ассоциации страхования жизни и Ассоциации общего страхования Сингапура [25].

Россия. 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) [7]. Руководство финансового регулятора неоднократно обращалось к Правительству Российской Федерации с просьбой пересмотреть решение об определении ПАО «Сбербанка России» в качестве центра компетенций в пользу Банка России или хотя бы передать ему часть полномочий, но безрезультатно [19]. На наш взгляд, следует согласиться с аргументами руководителей Банка России: во-первых, в его структуре успешно действует центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере, во-вторых, его участие «гармонизирует программу со стратегическими целями развития финансового рынка и снизит риски возникновения конфликта интересов при формировании и исполнении программы… эти функции являются «исключительно государственными и не свойственны коммерческим банкам» [19]. Ведь именно финансовый регулятор несет ответственность за стабильное функционирование финансового рынка и банковской системы России (ст. 2) [18].

Выводы. Вышесказанное позволяет сделать следующие выводы. Как российский, так и сингапурский финансовые регуляторы курируют все финансовые институты, формируют финансовую систему путем поддержания устойчивой системы корпоративного управления и строгого соблюдения международных стандартов бухгалтерского учета. Для обеспечения информационной безопасности банковского и финансового секторов финансовые регуляторы уполномочены принимать нормативные акты, которые охватывают такие важные аспекты банковской и финансовой деятельности, как защита объектов информационной инфраструктуры и информации при осуществлении переводов денежных средств, безопасность персональных данных, аутсорсинг услуг и др. Целесообразно рассмотреть возможности применения в российской реальности полномочий финансового регулятора в установленных законом случаях вмешиваться в процессы аутсорсинга путем издания предписания о возврате процесса из аутсорсинга или смене аутсорсингового контрагента. Преимуществом российского финансового регулятора является наличие в его структуре специального Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере, взаимодействующего с субъектами публичного и частного секторов. Интересным для изучения является опыт сингапурского финансового регулятора по сотрудничеству с научными центрами для сбора данных и моделирования киберрисков с дальнейшей разработкой средств оценки киберугроз и использованием инструментов страхования киберрисков, а также по созданию консультативной комиссии международных экспертов в сфере кибербезопасности. Эти организационно-правовые меры подтверждают ведущую роль MAS в обеспечении стабильности банковско-финансовой системы Сингапура. В то же время российский финансовый регулятор, несмотря на возложенные на него законодательством задачи, по неизвестным причинам исключается из федерального проекта «Цифровая экономика». На наш взгляд, Банк России должен быть определен в качестве центра компетенций этого проекта (единолично или совместно со Сбербанком России). Реализация вышеуказанных предложений подтвердит и укрепит роль российского финансового регулятора в обеспечении информационной безопасности.

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. Алексеев В.Н., Шарков Н.Н Подходы к разработке информационно-регулятивной системы финансовой инфраструктуры // Научно-исследовательский финансовый институт. Финансовый журнал. 2019. № 2 (48). С. 109–121.
3. Василенко О.А. Меры Центрального банка России по защите информации в финансовой сфере // Наука, техника и образование. 2018. № 8 (49). С. 66–68.
4. Горян Э.В. Ведущая роль Сингапура в обеспечении кибербезопасности в АСЕАН: промежуточные результаты и перспективы дальнейшего расширения // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. 2018. Т. 10, №3. С. 103–117.
5. 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.
6. Горян Э.В. Роль финансового регулятора в обеспечении кибербезопасности: опыт Сингапура // Финансовое право и управление. 2018. № 2. С. 25–38.
7. Информационная безопасность [Электронный ресурс] // Цифровая экономика России 2024: официальный сайт. URL: https://data-economy.ru/security
8. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 №6-ФКЗ, от 30.12.2008 №7-ФКЗ, от 05.02.2014 №2-ФКЗ, от 21.07.2014 №11-ФКЗ) [Электронный ресурс] // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_28399/.
9. Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных: указание Банка России от 10.12.2015 №3889-У [Электронный ресурс] // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_195662/
10. Об Электронной информационной системе Банка России: положение Банка России от 04.08.2005 №274-П [Электронный ресурс] // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_55289/
11. 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 [Электронный ресурс] // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_310165/
12. 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 [Электронный ресурс] // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_163762/
13. О вводе в действие стандарта Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Сбор и анализ технических данных при реагировании на инциденты информационной безопасности при осуществлении переводов денежных средств. СТО БР ИББС-1.3-2016»: приказ Банка России от 30.11.2016 №ОД-4234 [Электронный ресурс] // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_208423/

14. 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 [Электронный ресурс] // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_294526/
15. О правилах подготовки нормативных актов Банка России: положение Банка России от 22.09.2017 №602-П [Электронный ресурс] // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_278566/.
16. 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 [Электронный ресурс] // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_320979/
17. 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) [Электронный ресурс] // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_131473/
18. О Центральном банке Российской Федерации (Банке России): федеральный закон от 10.07.2002 №86-ФЗ (ред. от 01.05.2019) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_37570/
19. Разумный Е. Сбербанк и ЦБ спорят, кто главный по кибербезопасности: ЦБ хочет часть полномочий Сбербанка в «Цифровой экономике» // Ведомости (Vedomosti): электронное периодическое издание: URL: https://www.vedomosti.ru/finance/articles/2018/10/31/785328-sberbank-i-tsb-sporyat
20. Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ) // Банк России: официальный сайт. URL: https://www.cbr.ru/fincert/
21. Cyber Risk Management Project (CyRiM) // Nanyang Technological University: официальный сайт. URL: http://irfrc.ntu.edu.sg/Research/cyrim/Pages/Project-Brief.aspx
22. Guidelines on Outsourcing 2016 (revised 5 October 2018) // Monetary Authority of Singapore: официальный сайт. URL: http://www.mas.gov.sg
23. Instructions on Incident Notification and Reporting to MAS // Monetary Authority of Singapore: официальный сайт. URL: http://www.mas.gov.sg
24. Long J.-A. MAS Outsourcing Guidelines: Upcoming Remediation Deadline (26 July 2017)/ J.-A. Long, G. Kaur // Lexology. URL: https://www.lexology.com/library/detail.aspx?g=b8ea2219-75b2-4062-ac0c-edb016429904
25. MAS' Cyber Security Advisory Panel Proposes Ways to Enhance Financial Sector Cyber Resilience // Monetary Authority of Singapore: официальный сайт. URL: http://www.mas.gov.sg
26. MAS Sets Up International Advisory Panel for Cyber Security// Monetary Authority of Singapore: официальный сайт. URL: http://www.mas.gov.sg
27. Monetary Authority of Singapore Act 1970 [revised edition 1999 // Singapore Statutes Online: официальный сайт. URL: https://sso.agc.gov.sg/Act/MASA1970
28. Notice on Technology Risk Management CMG-N02 from 21 June 2013 [Last revised on 3 October 2018] // Monetary Authority of Singapore: официальный сайт. URL: http://www.mas.gov.sg

29. Technology Risk Management Guidelines 2013 // Monetary Authority of Singapore: официальный сайт. URL: http://www.mas.gov.sg

Транслитерация

1. 1. Aleksandrov V.V., Malij YU.V. Primenenie standarta Banka Rossii po obespecheniyu informacionnoj bezopasnosti organizacij bankovskoj sistemy Rossijskoj Federacii // Vestnik Belgorodskogo universiteta kooperacii, ekonomiki i prava. 2015. № 2 (54). P. 289-292.
2. Alekseev V.N., SHarkov N.N Podhody k razrabotke informacionno-regulyativnoj sistemy finansovoj infrastruktury // Nauchno-issledovatel'skij finansovyj institut. Finansovyj zhurnal. 2019. № 2 (48). P. 109-121.
3. Vasilenko O.A. Mery Central'nogo banka Rossii po zashchite informacii v finansovoj sfere // Nauka, tekhnika i obrazovanie. 2018. № 8 (49). P. 66-68.
4. Goryan E.V. Vedushchaya rol' Singapura v obespechenii kiberbezopasnosti v ASEAN: promezhutochnye rezul'taty i perspektivy dal'nejshego rasshireniya // Territoriya novyh vozmozhnostej. Vestnik Vladivostokskogo gosudarstvennogo universiteta ekonomiki i servisa. 2018. T. 10, №3. P. 103-117.
5. 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. P.49-60.
6. Goryan E.V. Rol' finansovogo regulyatora v obespechenii kiberbezopasnosti: opyt Singapura // Finansovoe pravo i upravlenie. 2018. №2. P. 25-38.
7. Informacionnaya bezopasnost' [Elektronnyj resurs] // Cifrovaya ekonomika Rossii 2024: oficial'nyj sajt. URL: https://data-economy.ru/security
8. Konstituciya Rossijskoj Federacii (prinyata vsenarodnym golosovaniem 12.12.1993) (s uchetom popravok, vnesennyh Zakonami RF o popravkah k Konstitucii RF ot 30.12.2008 №6-FKZ, ot 30.12.2008 №7-FKZ, ot 05.02.2014 №2-FKZ, ot 21.07.2014 №11-FKZ) [Elektronnyj resurs] // SPS «Konsul'tantPlyus». URL: http://www.consultant.ru/document/cons_doc_LAW_28399/.
9. Ob opredelenii ugroz bezopasnosti personal'nyh dannyh, aktual'nyh pri obrabotke personal'nyh dannyh v informacionnyh sistemah personal'nyh dannyh: ukazanie Banka Rossii ot 10.12.2015 №3889-U [Elektronnyj resurs] // SPS «Konsul'tantPlyus». URL: http://www.consultant.ru/document/cons_doc_LAW_195662/
10. Ob Elektronnoj informacionnoj sisteme Banka Rossii: polozhenie Banka Rossii ot 04.08.2005 №274-P [Elektronnyj resurs] // SPS «Konsul'tantPlyus». URL: http://www.consultant.ru/document/cons_doc_LAW_55289/
11. O vvode v dejstvie standarta Banka Rossii «Bezopasnost' finansovyh (bankovskih) operacij. Upravlenie incidentami informacionnoj bezopasnosti. O formah i srokah vzaimodejstviya Banka Rossii s uchastnikami informacionnogo obmena pri vyyavlenii incidentov, svyazannyh s narusheniem trebovanij k obespecheniyu zashchity informacii. STO BR BFBO-1.5-2018»: prikaz Banka Rossii ot 14.09.2018 №OD-2403 [Elektronnyj resurs] // SPS «Konsul'tantPlyus». URL: http://www.consultant.ru/document/cons_doc_LAW_310165/
12. O vvode v dejstvie standarta Banka Rossii «Obespechenie informacionnoj bezopasnosti organizacij bankovskoj sistemy Rossijskoj Federacii. Obshchie polozheniya. STO BR IBBS-1.0-2014»: rasporyazhenie Banka Rossii ot 17.05.2014 №R-399 [Elektronnyj resurs] // SPS «Konsul'tantPlyus». URL: http://www.consultant.ru/document/cons_doc_LAW_163762/
13. O vvode v dejstvie standarta Banka Rossii «Obespechenie informacionnoj bezopasnosti organizacij bankovskoj sistemy Rossijskoj Federacii. Sbor i analiz tekhnicheskih dannyh pri

reagirovanii na incidenty informacionnoj bezopasnosti pri osushchestvlenii perevodov denezhnyh sredstv. STO BR IBBS-1.3-2016»: prikaz Banka Rossii ot 30.11.2016 №OD-4234 [Elektronnyj resurs] // SPS «Konsul'tantPlyus». URL: http://www.consultant.ru/document/cons_doc_LAW_208423/

14. O vvode v dejstvie standarta Banka Rossii «Obespechenie informacionnoj bezopasnosti 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 [Elektronnyj resurs] // SPS «Konsul'tantPlyus». URL: http://www.consultant.ru/document/cons_doc_LAW_294526/
15. O pravilah podgotovki normativnyh aktov Banka Rossii: polozhenie Banka Rossii ot 22.09.2017 №602-P [Elektronnyj resurs] // SPS «Konsul'tantPlyus». URL: http://www.consultant.ru/document/cons_doc_LAW_278566/.
16. 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 infrastrukture 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 [Elektronnyj resurs] // SPS «Konsul'tantPlyus». URL: http://www.consultant.ru/document/cons_doc_LAW_320979/
17. 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) [Elektronnyj resurs] // SPS «Konsul'tantPlyus». URL: http://www.consultant.ru/document/cons_doc_LAW_131473/
18. O Central'nom banke Rossijskoj Federacii (Banke Rossii): federal'nyj zakon ot 10.07.2002 №86-FZ (red. ot 01.05.2019) // SPS «Konsul'tantPlyus». URL: http://www.consultant.ru/document/cons_doc_LAW_37570/
19. Razumnyj E. Sberbank i CB sporyat, kto glavnyj po kiberbezopasnosti: CB hochet chast' polnomochij Sberbanka v «Cifrovoj ekonomike» // Vedomosti (Vedomosti): elektronnoe periodicheskoe izdanie: URL: https://www.vedomosti.ru/finance/articles/2018/10/31/785328-sberbank-i-tsb-sporyat
20. Centr monitoringa i reagirovaniya na komp'yuternye ataki v kreditno-finansovoj sfere (FinCERT) // Bank Rossii: oficial'nyj sajt. URL: https://www.cbr.ru/fincert/

Для цитирования: 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.

For citation: Gorian E.V. The role of the financial regulatory authority in cyber security of Russia and Singapore: a comparative legal aspect, *The Territory of New Opportunities. The Herald of Vladivostok State University of Economics and Service*, 2019, Vol. 11, № 2, pp. 83–101.

DOI dx.doi.org/10.24866/VVSU/2073-3984/2019-2/083–101

Дата поступления: 14.05.2019.