Административное и муниципальное право
Правильная ссылка на статью:
Горян Э.В., Баранник И.Н. — Обеспечение информационной безопасности в финансовом секторе в рамках реализации Национальной программы «Цифровая экономика Российской Федерации» // Административное и муниципальное право. – 2019. – № 4. – С. 27 - 40. DOI: 10.7256/2454-0595.2019.4.29911 URL: https://nbpublish.com/library_read_article.php?id=29911

Обеспечение информационной безопасности в финансовом секторе в рамках реализации Национальной программы «Цифровая экономика Российской Федерации»

Горян Элла Владимировна

кандидат юридических наук

доцент, Владивостокский государственный университет экономики и сервиса

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

ella-gorjan@yandex.ru

Баранник Игорь Николаевич

кандидат юридических наук

доцент, кафедра гражданско-правовых дисциплин, Владивостокский государственный университет экономики и сервиса

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

barannik_08@mail.ru

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

Аннотация.

Объектом исследования являются отношения, возникающие при реализации Национальной программы «Цифровая экономика» в аспекте обеспечения информационной безопасности в финансовом секторе России. Определяется роль государственного финансового регулятора в реализации указанной программы с учетом особенностей его правового статуса. Исследуются ключевые документы, формирующие нормативно-правовые механизмы обеспечения информационной безопасности финансового и банковского сектора России. Определяется содержание деятельности центра компетенций федерального проекта "Информационная безопасность" и обосновывается необходимость определения Банка России в качестве центра компетенций. В исследовании использованы общенаучные (в частности, структурно-функциональный и герменевтический) и специальные юридические методы познания (формально-юридический и историко-правовой). Несмотря на серьезный конституционно-правовой статус и опыт практического управления процессами по обеспечению безопасности финансовых институтов, потенциал финансового регулятора не в полной мере используется в Национальной программе «Цифровая экономика Российской Федерации», хотя задачи, поставленные перед центром компетенций по информационной безопасности, носят государственный характер и соответственно должны исполняться соответствующим субъектом. 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: финансовый регулятор, Банк России, финансовая система, банковская система, цифровая экономика, информационная безопасность, кибербезопасность, критическая информационная инфраструктура, ФинЦЕРТ, центр компетенций

DOI:

10.7256/2454-0595.2019.4.29911

Дата направления в редакцию:

02-06-2019

Дата рецензирования:

03-06-2019

Дата публикации:

24-07-2019

Актуальность темы исследования. В целях реализации Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы [1] в 2017 году была утверждена национальная программа «Цифровая экономика Российской Федерации» [2] (далее - Программа). В качестве ее основной цели было указано создание цифровой среды, обеспечивающей взаимодействие всех участников публичного и частного секторов во всех сферах жизнедеятельности в достаточных и необходимых условиях институционального и инфраструктурного характера для развития высоких технологий, используемых как в традиционных, так и новых отраслях экономики. Дорожная карта Программы первоначально предусматривала пять направлений развития цифровой экономики в России: 1) нормативное регулирование; 2) кадры и образование; 3) формирование исследовательских компетенций и технологических заделов; 4) информационная инфраструктура; 5) информационная безопасность [2]. Однако в конце 2018 года был утвержден Паспорт национальной программы «Цифровая экономика Российской Федерации» [3], которым была предусмотрена реализация шести федеральных проектов в рамках Программы (пп. 4.1-4.6): а) нормативное регулирование цифровой среды; б) информационная инфраструктура; в) кадры для цифровой экономики; г) информационная безопасность; д) цифровые технологии; е) цифровое государственное управление. Для реализации Программы была разработана система управления, включающая, помимо всего прочего, так называемые «центры компетенций» (п. 4). Центры компетенций занимаются а) обеспечением сбора предложений и осуществлением подготовки проектов паспортов федеральных проектов Программы, включая пояснительную записку и финансово-экономическое обоснование, и запросов на изменения паспортов федеральных проектов Программы; б) направлением

указанных проектов в соответствующую рабочую группу и другим участникам системы управления; в) рассмотрением итоговых отчетов о реализации Программы и о реализации федеральных проектов Программы; г) рассмотрением проектов актов и проектов поправок к законопроектам, принятие которых может оказать влияние на реализацию Программы и выполнение федеральных проектов Программы, а также проекты официальных отзывов на такие законопроекты; д) выполнением мероприятий федеральных проектов Программы в рамках своей компетенции, в том числе подготовки проектов актов (п. 12) [4].

Одним из федеральных проектов Программы, как указывалось выше, является «Информационная безопасность», задачей которого определено обеспечение информационной безопасности на основе отечественных разработок при передаче, обработке и хранении данных, гарантирующей защиту интересов личности, бизнеса и государства (п. 4.4) [3]. Результаты выполнения данной задачи запланированы следующие: 1) создание условий для глобальной конкурентоспособности в области экспорта отечественных разработок и технологий обеспечения безопасности информации; 2) обеспечение устойчивости и безопасности функционирования информационной инфраструктуры и сервисов передачи, обработки и хранения данных; 3) обеспечение защиты прав и законных интересов личности, бизнеса и государства от угроз информационной безопасности в условиях цифровой экономики; 4) обеспечение использования отечественных разработок и технологий при передаче, обработке и хранении данных. Однако в качестве центра компетенций этого федерального проекта Программы был определен ПАО «Сбербанк России», а руководителем рабочей группы по направлению «Информационная безопасность» - президент группы компаний InfoWatch Н. Касперская) [5]. При этом функцию финансового регулятора в России исполняет Центральный банк Российской Федерации (Банк России), имеющий особый конституционно-правовой статус и соответствующие полномочия. Его руководство 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 [6]. В качестве аргументов были указаны следующие: во-первых, в структуре Банка России успешно действует центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ), 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» [6]. Ведь именно финансовый регулятор несет ответственность за стабильное функционирование финансового рынка и банковской системы России (ст. 2) [7], он играет координирующую роль, устанавливая правила осуществления деятельности финансовыми институтами, в том числе в сфере обеспечения безопасности их функционирования [8, С. 26]. Поэтому необходимо теоретическое исследование и обоснование роли Банка России в качестве центра компетенций федерального проекта «Информационная безопасность» Национальной программы «Цифровая экономика Российской Федерации». Все вышесказанное свидетельствует об актуальности темы исследования.

Постановка проблемы исследования. Обеспечение информационной безопасности государства осуществляется взаимодействующими институтами публичного и частного секторов. В такой ситуации представители публичного сектора несут ответственность за координацию действий в рамках конкретного сегмента экономики. Финансовый регулятор

выполняет функции по координированию и управлению отношениями в рамках финансового и банковского секторов (ст. 3, 4) [7], поэтому определение его роли в обеспечении информационной безопасности в рамках реализации государственной программы по создание цифровой среды, обеспечивающей взаимодействие всех участников публичного и частного секторов во всех сферах жизнедеятельности, является научно и практически обоснованным.

Цели и задачи исследования. Цель нашего исследования – обосновать необходимость определения Банка России в качестве центра компетенций федерального проекта «Информационная безопасность» Национальной программы «Цифровая экономика Российской Федерации». Задачи исследования заключаются в определении правового статуса указанного субъекта, характеристике полномочий в сфере обеспечения информационной безопасности и определении роли в реализации Программы.

Методология. В исследовании использованы общенаучные (в частности, структурно-функциональный и герменевтический) и специальные юридические методы познания (формально-юридический и историко-правовой).

Предмет исследования, источниковая база исследования. Предмет исследования составляют основные нормативно-правовые акты, определяющие содержание Программы и полномочия Банка России по обеспечению информационной безопасности, а также ряд научных исследований по теме.

Выбранная нами для исследования тема мало представлена в российской научной литературе. Среди отечественных научных исследований можно выделить работы о роли российского финансового регулятора в обеспечении информационной безопасности банковской и финансовой систем [9; 10], а также работу о подходах к разработке информационно-регулятивной системы финансовой инфраструктуры [11].

Основная часть. Перед определением правового статуса Банка России необходимо остановиться на вопросе об особенности объекта, к которому применяются полномочия финансового регулятора. Речь идет об информационных системах банковского и финансового секторов, имеющих 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 иностранных государств. Объекты КИИ представляют собой зону ответственности прежде всего специализированных государственных институтов, выполняющих функции по обеспечению национальной безопасности [12, с. 55-57]. Как мы указывали выше, финансовый регулятор уполномочен государством на установление правил деятельности всех финансовых институтовами, в том числе и в сфере безопасности их функционирования [8, с. 26].

Особый правовой статус Банка России устанавливается Конституцией Российской Федерации (ст. 75) [13], 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) [7]. Среди функций Банка России, определенных в статье 4 ФЗ-86, особо следует отметить такие, которые имеют непосредственное отношение к обеспечению безопасности финансовой и банковской сферы: установление правил проведения банковских операций и осуществления расчетов; валютное регулирование; осуществление валютного контроля и банковского надзора, а также надзора в национальной платежной системе; разработка и проведение политики развития и обеспечения стабильности функционирования финансового рынка; проведение анализа и прогнозирования состояния экономики государства с публикацией соответствующих материалов и статистических данных; организация оказания услуг по передаче электронных сообщений по финансовым операциям.

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) [14]. Положение Банка России устанавливает системно связанные между собой правила по вопросам, отнесенным к компетенции Банка России (п. 1.4.2) [14]. 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) [14].

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) [14]. Рассмотрим те из них, имеющие отношение к обеспечению информационной безопасности финансовой и банковской сфер.

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 [15] 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) [15]. 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» [16], 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) [16].

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) [16].

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) [16].

Раздел 7 «Система информационной безопасности организаций банковской системы Российской Федерации» содержит принципы распределении 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) [16].

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 данные (п. 7.11), а также общие требования по обработке персональных данных в организации банковской системы Российской Федерации (п. 7.10) [16].

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) [16].

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 система обеспечения информационной безопасности (в том числе со стороны руководства) (п. 9.1) [16].

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 [10]. 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 Положение о требованиях к защите информации в платежной системе Банка России №672-П [18], которое распространяется на объекты информационной инфраструктуры, применяемые для обработки защищаемой информации, перечисленной в пункте 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 информация, содержащаяся в извещениях (подтверждениях), касающихся приема к исполнению распоряжений участников платежной системы, а также в извещениях (подтверждениях), касающихся исполнения распоряжений участников платежной системы; требование об отнесении информации о совершенных переводах денежных средств к защищаемой информации, хранящейся в операционных центрах платежных систем с использованием платежных карт или находящихся за пределами Российской Федерации, устанавливается оператором платежной системы; 4) содержащаяся 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, обрабатываемой при осуществлении переводов денежных средств [19].

В качестве дополнительных инструментов обеспечения кибербезопасности следует отметить ряд стандартов [20; 21; 22] 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» [23].

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 [22]. 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 [24]. 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 [24] на основании положений специального стандарта об управлении инцидентами информационной безопасности [20].

Инструменты, издаваемые Банком России 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.

Вышеуказанные инструменты нормативно-правового и институционального характера определяют финансового регулятора в качестве ключевого, более того, единственного субъекта, обладающего широкими полномочиями по регулированию финансовых отношений.

Рассмотрим теперь положения Программы, устанавливающие объем и пределы вовлеченности Банка России в ее федеральные проекты. Руководителями проектов назначены заместители глав следующих министерств: Министерства экономического развития Российской Федерации – для проектов «Нормативное регулирование цифровой

среды» и «Кадры для цифровой экономики»; Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации – для проектов «Информационная инфраструктура», «Информационная безопасность», «Цифровые технологии» и «Цифровое государственное управление» (раздел 3) [3].

В федеральном проекте «Нормативное регулирование цифровой среды» Банк России указан в качестве ответственного исполнителя задачи обеспечения правовых условий для внедрения и использования инновационных технологий на финансовом рынке. В качестве одного из результатов данного проекта было указано принятие к 31.12.2018 года федерального закона, регулирующего оборот криптовалют и проведения ICO, определения статуса цифровых технологий, применяемых в финансовой сфере, и их понятий (п. 1.8) [3]. Для его достижения финансовый регулятор взаимодействовал с Минфином России, Минэкономразвития России, Минкомсвязи России, Фондом «Сколково», АНО «Цифровая экономика» и иными заинтересованными федеральными органами исполнительной власти и организациями. Соответствующий законопроект [25] был принят Государственной Думой Федерального Собрания РФ в первом чтении 22.05.2018 года, экспертное заключение Совета при Президенте РФ по кодификации и совершенствованию гражданского законодательства было получено 29.11.2018 года и 20.03.2019 года рассмотрение законопроекта во втором чтении было перенесено Государственной Думой ФС РФ на другое пленарное заседание[26]. Еще одним результатом в рамках федерального проекта «Нормативное регулирование цифровой среды» было указано принятие федерального закона, предусматривающего регулирование осуществления краудфандинговой деятельности (деятельности по привлечению инвестиций с использованием инвестиционных платформ) (п. 1.9) к 31.12.2018 года [3]. Соисполнителями с Банком России были указаны Минэкономразвития России, Минкомсвязи России, Минфин России, Фонд «Сколково», АНО «Цифровая экономика» и иные заинтересованные федеральными органами исполнительной власти и организации. Соответствующий проект федерального закона «О привлечении инвестиций с использованием инвестиционных платформ» [27] был принят в первом чтении 22.05.2018 года. Экспертное заключение Совета при Президенте РФ по кодификации и совершенствованию гражданского законодательства на этот законопроект было дано 17.01.2019 года [28].

Федеральный проект «Информационная инфраструктура» включил Банк России для достижения задачи внедрения цифровых технологий и платформенных решений в сферах государственного управления, бизнеса и общества. К 31.12.2023 года Банк России совместно с ПАО «Ростелеком» должен создать платформу, обеспечивающую обмен информацией между государством, гражданами, а также коммерческими и некоммерческими организациями, в том числе с согласия гражданина (инфраструктура «Цифровой профиль») (п. 1.66) [3].

Следует отметить, что в работе центра компетенций по информационной безопасности не задействованы представители Банка России, несмотря на то, что работа этого центра ведется в 16 подгруппах по следующим направлениям: 1) обеспечение устойчивости и безопасности функционирования единой сети электросвязи Российской Федерации (включая российский сегмент сети «Интернет»); 2) управляемость и надежность функционирования сети российского сегмента сети «Интернет»; 3) технологическая независимость и безопасность функционирования аппаратных средств и инфраструктуры обработки данных; 4) обеспечить устойчивость и безопасность функционирования информационных систем и технологий; 5) правовой режим и технические инструменты

функционирования сервисов и использования данных; 6) правовой режим межмашинного взаимодействия для киберфизических систем; 7) правовой режим функционирования машинных и когнитивных интерфейсов, включая интернет вещей; 8) защита прав, свобод и законных интересов личности в условиях цифровой экономики; 9) технические инструменты, обеспечивающие безопасное информационное взаимодействие граждан в условиях цифровой экономики; 10) защита прав и законных интересов бизнеса в условиях цифровой экономики; 11) организационная и правовая защита государственных интересов в условиях цифровой экономики; 12) создание эффективных механизмов государственного регулирования и поддержки в области информационной безопасности при интеграции национальной цифровой экономики в международную экономику; 13) создание основ для построения доверенной среды ЕАЭС, обеспечивающей коллективную информационную безопасность; 14) участие России в подготовке и реализации международных документов по вопросам информационной безопасности, относящимся к цифровой экономике; 15) правовое обеспечение реализации направления информационной безопасности; 16) кадровое обеспечение реализации направления информационной безопасности [5]. В деятельности этих групп принимают участие представители как публичного, так и частного секторов, однако финансовый регулятор не представлен ни в одной из них, что никак не соотносится с его возможностями и полномочиями.

Выводы. Вышесказанное позволяет сделать следующие выводы. Банк России курирует все финансовые институты, формирует финансовую систему путем поддержания устойчивой системы корпоративного управления и строгого соблюдения международных стандартов бухгалтерского учета. Для обеспечения информационной безопасности банковского и финансового секторов Банк России уполномочен 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. Важную роль в обеспечении информационной безопасности играет специальный Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере, взаимодействующий с субъектами публичного и частного секторов. Несмотря на серьезный конституционно-правовой статус и опыт практического управления процессами по обеспечению безопасности финансовых институтов, потенциал финансового регулятора не в полной мере используется в Национальной программе «Цифровая экономика Российской Федерации», хотя задачи, поставленные перед центром компетенций по информационной безопасности, носят государственный характер и соответственно должны исполняться соответствующим субъектом. На наш взгляд, Банк России должен быть определен в качестве центра компетенций этого проекта (единолично или совместно со Сбербанком России), что является логическим продолжением реализации предоставленных ему государством полномочий.

Библиография

1. О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы: Указ Президента Российской Федерации от 09.05.2017 №203 [Электронный ресурс] // СПС «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_216363/
2. Об утверждении программы «Цифровая экономика Российской Федерации» : распоряжение Правительства Российской Федерации от 28.07.2017 №1632-р [Электронный ресурс] // СПС «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_221756/

3. Паспорт национальной программы «Цифровая экономика Российской Федерации» (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 24.12.2018 №16) [Электронный ресурс] // СПС «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_319432/
4. О системе управления реализацией национальной программы «Цифровая экономика Российской Федерации» (вместе с Положением о системе управления реализацией национальной программы «Цифровая экономика Российской Федерации»): постановление Правительства РФ от 02.03.2019 №234 [Электронный ресурс] // СПС «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_319701/
5. Информационная безопасность [Электронный ресурс] // Цифровая экономика России 2024: официальный сайт. – Режим доступа: https://data-economy.ru/security
6. Разумный Е. Сбербанк и ЦБ спорят, кто главный по кибербезопасности: ЦБ хочет часть полномочий Сбербанка в «Цифровой экономике» [Электронный ресурс] / Е. Разумный // Электронное периодическое издание «Ведомости» (Vedomosti). – Режим доступа: https://www.vedomosti.ru/finance/articles/2018/10/31/785328-sberbank-i-tsb-sporyat
7. О Центральном банке Российской Федерации (Банке России) : федеральный закон от 10.07.2002 №86-ФЗ (ред. от 01.05.2019) [Электронный ресурс] // СПС «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_37570/
8. Горян Э.В. Роль финансового регулятора в обеспечении кибербезопасности: опыт Сингапура / Э.В. Горян // Финансовое право и управление.-2018.-№2.-С. 25-38.
9. Александров В.В. Применение стандарта Банка России по обеспечению информационной безопасности организаций банковской системы Российской Федерации / В.В. Александров, Ю.В. Малий // Вестник Белгородского университета кооперации, экономики и права. 2015. № 2 (54). С. 289-292.
10. Василенко О.А. Меры Центрального банка России по защите информации в финансовой сфере / О.А. Василенко // Наука, техника и образование.-2018.-№ 8 (49).-С. 66-68.
11. Алексеев В.Н. Подходы к разработке информационно-регулятивной системы финансовой инфраструктуры / В.Н. Алексеев, Н.Н. Шарков // Научно-исследовательский финансовый институт. Финансовый журнал.-2019.-№ 2 (48).-С. 109-121.
12. Горян Э.В. Институциональные механизмы обеспечения безопасности критической информационной инфраструктуры Российской Федерации и Сингапура: сравнительно-правовой аспект / Э.В. Горян // Административное и муниципальное право.-2018.-№9.-С.49-60.
13. 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». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_28399/
14. О правилах подготовки нормативных актов Банка России : положение Банка России от 22.09.2017 №602-П [Электронный ресурс] // СПС «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_278566/
15. Об Электронной информационной системе Банка России : положение Банка России

от 04.08.2005 №274-П [Электронный ресурс] // СПС «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_55289/

16. 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». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_163762/
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». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_131473/
18. 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». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_320979/
19. 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». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_131473/
20. 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». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_310165/
21. 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». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_208423/
22. 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». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_294526/
23. 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». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_195662/

24. Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ) [Электронный ресурс] // Банк России: официальный сайт. – Режим доступа: https://www.cbr.ru/fincert/
25. О цифровых финансовых активах : проект федерального закона №419059-7 (ред., принятая ГД ФС РФ в I чтении 22.05.2018) [Электронный ресурс] // СПС «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&ts=169150414804605276596829 3574&cacheid=E86A60337A9AB058728DA45CFA2FC424&mode=splus&base=PRJ&n=172447&rnd=0D5BCB2A5355B88F17E045BC4D1B428B#1o85lvcl2r3
26. О цифровых финансовых активах : паспорт проекта федерального закона №419059-7 (внесен депутатами Государственной Думы ФС РФ А.Г. Аксаковым, И.Б. Дивинским, О.А. Николаевым, Р.М. Марданшиным, А.А. Гетта, М.Л. Шаккумом, А.Б. Выборным, К.Г. Слыщенко, Е.Б. Шулеповым, В.И. Афонским, Н.Д. Боевой, И.Е. Марьяш, С.В. Железняком, А.И. Воеводой, С.А. Вострецовым, А.В. Чернышевым, членами Совета Федерации ФС РФ Н.А. Журавлевым, А.Н. Епишиным, В.В. Полетаевым) [Электронный ресурс] // СПС «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?rnd=0D5BCB2A5355B88F17E045BC4D1B428B&req=doc&base=PRJ&n=170088&stat=refcode%3D16876%3Bindex%3D0#2kcep97peb0
27. О привлечении инвестиций с использованием инвестиционных платформ : проект федерального закона №419090-7 (ред., принятая ГД ФС РФ в I чтении 22.05.2018) [Электронный ресурс] // СПС «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?rnd=0D5BCB2A5355B88F17E045BC4D1B428B&req=doc&base=PRJ&n=172448&dst=100053&fld=134&REFFIELD=134&REFDST=100008&REFDOC=320475&REFBASE=LAW&stat=refcode%3D10881%3Bdstident%3D100053%3Bindex%3D16#1ycrfbuohhg
28. О привлечении инвестиций с использованием инвестиционных платформ : паспорт проекта федерального закона №419090-7 (внесен депутатами Государственной Думы ФС РФ А.Г. Аксаковым, И.Б. Дивинским, О.А. Николаевым, А.А. Гетта, М.Л. Шаккумом, К.Г. Слыщенко, В.И. Афонским, Е.Б. Шулеповым, С.В. Железняком, С.А. Вострецовым, Р.М. Марданшиным, Д.Е. Шилковым, членами Совета Федерации ФС РФ Н.А. Журавлевым, В.В. Полетаевым) [Электронный ресурс] // СПС «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?rnd=0D5BCB2A5355B88F17E045BC4D1B428B&req=doc&base=PRJ&n=170089&stat=refcode%3D16876%3Bindex%3D0#xfqwm5jws