Личный кабинет

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ (БАНК РОССИИ)

107016, Москва, ул. Неглинная, д. 12, к. В
www.cbr.ru
тел.: (499) 300-30-00, 8 (800) 300-30-00

Ассоциация банков России

ИНН 7702077663

От 02.04.2024 № 56-27/733

на № 02-05/238 от 11.03.2024

О рассмотрении обращения

Департамент информационной безопасности Банка России (далее – ДИБ) рассмотрел обращение Ассоциации банков России по вопросам информационной безопасности и соблюдения требований нормативных актов в области обеспечения защиты информации и сообщает следующее.

По вопросу 1. Проектом федерального закона № 404786-8 «О внесении изменений в отдельные законодательные акты Российской Федерации» планируется внесение изменений в законодательство Российской Федерации, направленных на снятие ограничений, связанных с передачей охраняемых законом видов тайн на аутсорсинг. Предполагается, что положения законопроекта будут распространяться в том числе на случаи использования организациями финансового рынка облачных услуг по обеспечению информационной безопасности.

С учетом широко признанных практик[1] применение кредитными организациями облачного решения, реализующего функции аппаратного модуля безопасности информационной инфраструктуры платежной системы (HSM модуля), на текущем этапе не рассматривается в качестве допустимого сценария аутсорсинга в рамках осуществления переводов денежных средств.

По вопросу 2. Требование о реализации уровня защиты информации, предусмотренного национальным стандартом Российской Федерации ГОСТ Р

[1] В частности, документы The Payment Card Industry Security Standards Council.

57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер», является одним из набора требований, установленных Положением Банка России от 17.04.2019 № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента» и Положением Банка России от 20.04.2021 № 757-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций».

Выполнение указанного требования не влияет на необходимость выполнения иных требований, установленных указанными нормативными актами Банка России.

По вопросу 3. В настоящее время ДИБ располагает недостаточными данными относительно практики применения положений раздела 7.4 Профиля защиты[2], в котором изложены требования к гибкой безопасной разработке, тестированию и внедрению прикладного программного обеспечения автоматизированных систем с соблюдением требований положений нормативных актов Банка России.

В целях разработки и внедрения безопасных программных продуктов при сохранении гарантированного и достаточного уровня защищенности прикладного программного обеспечения автоматизированных систем и приложений, используемых при осуществлении финансовых (в том числе банковских) операций, ДИБ рекомендует использовать новый раздел документа.

При этом в рамках сопровождения Профиля защиты ДИБ ориентируется на выпускаемые, а также планируемые к выпуску национальные стандарты

---

[2] С учетом Информационного письма Банка России от 02.02.2022 № ИН-014-56/5 о разработке нового раздела 7.4 методического документа «Профиль защиты прикладного программного обеспечения автоматизированных систем и приложений кредитных организаций и некредитных финансовых организаций».

Российской Федерации по разработке безопасного программного обеспечения, работа над которыми ведется в техническом комитете по стандартизации № 362 «Защита информации», а также на международные стандарты и лучшие практики.

В связи с изложенным пересмотр раздела 7.4 Профиля защиты в части расширения случаев применения, а также рассмотрение возможности использования оценки с учетом положений раздела 7.4 Профиля защиты для допуска программного обеспечения к использованию наряду с программным обеспечением, включенным в реестр Минцифры России, планируется осуществлять после апробации применения финансовыми организациями подходов к безопасной разработке программного обеспечения и приложений согласно перспективным правовым условиям.

По вопросу 4. Распространение на безвозмездной основе для физических и юридических лиц шифровального (криптографического) средства, соответствующего требованиям к шифровальным (криптографическим) средствам, указанным в части 1 статьи 19 Федерального закона от 29.12.2022 № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» (далее – Федеральный закон № 572-ФЗ), относится к полномочиям Минцифры России.

Участие со стороны Банка России в создании и распространении среди финансовых организаций таких средств не планируется.

По вопросу 5. В соответствии с пунктом 6.1 Положения Банка России от 17.04.2019 № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента» в том случае, если кредитная организация применяет средства криптографической защиты информации (далее – СКЗИ) российского производства, СКЗИ должны иметь сертификаты соответствия федерального органа

исполнительной власти в области обеспечения безопасности (далее – ФСБ России). При этом необходимость проведения оценки влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование СКЗИ, на выполнение предъявляемых к ним требований определяется требованиями технической документации на СКЗИ и Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденным приказом ФСБ России от 09.02.2005 № 66.

Необходимость проведения работ по оценке влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование программного модуля Банка России (далее – ПМ БР), на выполнение предъявленных к входящему в его состав СКЗИ требований определяется пунктом 6 Положения Банка России от 07.12.2023 № 833-П «О требованиях к обеспечению защиты информации для участников платформы цифрового рубля».

Дополнительно отмечаем, что Банком России разработан стандарт платформы цифрового рубля «Порядок проведения работ по оценке влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование ПМ БР, на выполнение предъявленных к входящему в его СКЗИ требований», который позволяет оптимизировать процесс взаимодействия кредитной организации – участника платформы цифрового рубля и аккредитованной ФСБ России испытательной лаборатории с ФСБ России, а также сократить сроки проведения оценочных процедур относительно «стандартного» подхода к оценке.

На текущем этапе рассмотрение вопроса о пересмотре подхода к проведению оценки влияния для всех случаев применения СКЗИ в приложениях кредитных организаций ДИБ полагает преждевременным ввиду недостатка накопленной информации о применении на практике

подхода по оптимизации взаимодействия кредитной организации и аккредитованной ФСБ России испытательной лаборатории с ФСБ России.

По вопросу 6. Указание Банка России от 25.09.2023 № 6541-У «О перечне угроз безопасности, актуальных при обработке биометрических персональных данных, векторов единой биометрической системы, проверке и передаче информации о степени соответствия векторов единой биометрической системы предоставленным биометрическим персональным данным физического лица в информационных системах организаций финансового рынка, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц, за исключением единой биометрической системы, а также актуальных при взаимодействии информационных систем организаций финансового рынка, иных организаций, индивидуальных предпринимателей с указанными информационными системами» (далее – Указание Банка России № 6541-У) определяет перечень угроз безопасности, актуальных при обработке биометрических персональных данных, векторов единой биометрической системы, проверке и передаче информации о степени соответствия векторов единой биометрической системы предоставленным биометрическим персональным данным физического лица в информационных системах организаций финансового рынка, указанных в части 1 статьи 3 Федерального закона № 572-ФЗ и осуществляющих аутентификацию на основе биометрических персональных данных физических лиц, за исключением единой биометрической системы, а также актуальных при взаимодействии информационных систем организаций финансового рынка, иных организаций, индивидуальных предпринимателей с указанными информационными системами, с учетом оценки возможного вреда, проведенной в соответствии с законодательством Российской Федерации о персональных данных.

В соответствии с частью 3 статьи 16 Федерального закона № 572-ФЗ обработка биометрических персональных данных в информационных системах организаций финансового рынка, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц, допускается при одновременном выполнении условий, включающих

использование шифровального (криптографического) средства, определенного пунктом 5 части 2 статьи 6 данного Федерального закона, либо шифровальных (криптографических) средств, позволяющих обеспечить безопасность персональных данных от угроз, определенных в том числе Указанием Банка России № 6541-У.

Необходимость применения СКЗИ определенных классов обусловлена целью обеспечить конфиденциальность и целостность биометрических персональных данных на уровне, пропорциональном рискам компрометации или подмены биометрических персональных данных (в результате реализации которых для субъекта персональных данных могут возникнуть значимые негативные последствия).

С учетом технической возможности применения на стационарных средствах вычислительной техники СКЗИ класса КС 2 пересмотр перечня угроз, установленных Указанием Банка России № 6541-У, не планируется.

По вопросу 7. Разделом 2 функционально-технических требований, утвержденных Банком России 28.02.2020 № ФТ-56-3/33, определен закрытый перечень платежных устройств с терминальным ядром, которые входят в область применения указанных функционально-технических требований.

Указанный перечень не включает биоPOS-терминалы, в связи с чем ДИБ полагает, что в случае размещения закрытых ключей в неизвлекаемой области памяти биоPOS-терминала срок действия закрытых ключей может совпадать со сроком эксплуатации биоPOS-терминала.

По вопросу 8. В настоящее время в Государственной Думе Федерального Собрания Российской Федерации готовится ко второму чтению проект федерального закона № 502104-8 «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях».

В связи с этим полагаем, что основным инструментом стимулирования заинтересованности операторов персональных данных в высоком уровне защиты данных будет являться вышеуказанный законопроект, так как наряду с установлением штрафов он предусматривает условия, при которых для организаций снижается размер штрафа.

В условиях перспективных изменений в Кодекс Российской Федерации об административных правонарушениях инициатива об установлении требования по страхованию киберрисков и (или) оформлению банковской гарантии в качестве обязательного условия получения статуса оператора персональных данных может создать дополнительную регуляторную нагрузку для операторов персональных данных.

Дополнительно отмечаем, что проведение оценки защиты данных на стороне операторов персональных данных не является профильной деятельностью страховой или кредитной организации. ДИБ полагает, что на текущем этапе у указанных организаций недостаточно инструментов для принятия обоснованных решений об уровне киберриска, присущего деятельности оператора персональных данных.

Вместе с тем ДИБ планирует принимать активное участие в рамках проработки вопросов развития страхования киберрисков, включая указанную инициативу.

Заместитель директора Департамента
информационной безопасности А.О. Выборнов