О применении банками шифровальных (криптографических) средств защиты информации и юридической ответственности за невыполнение предписаний регуляторов

Применение шифровальных (криптографических) средств защиты информации

В соответствии с ч. 1 ст. 27 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе» (далее – 161-ФЗ) операторы по переводу денежных средств, банковские платежные агенты (субагенты), операторы платежных систем, операторы услуг платежной инфраструктуры обязаны обеспечивать защиту информации о средствах и методах обеспечения информационной безопасности, персональных данных и об иной информации, подлежащей обязательной защите в соответствии с законодательством Российской Федерации. Согласно п.9 «Положения о защите информации в платежной системе», утв. постановлением Правительства РФ от 13.06.2012 № 584 применение шифровальных (криптографических) средств защиты информации операторами и агентами осуществляется в соответствии с законодательством Российской Федерации.

ФСБ России - регулятором в части области разработки, производства, реализации, эксплуатации, ввоза в Российскую Федерацию и вывоза из Российской Федерации шифровальных (криптографических) средств (согласно разделу 3 «Положения о Федеральной службе безопасности Российской Федерации», утв. Указом Президента РФ от 11.08.2003 № 960) - разработан ряд документов в данной области. Среди них «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации», утв. приказом ФСБ России от 09.02.2005 № 66 (далее - Положение ПКЗ-2005).

Согласно п.12 Положения ПКЗ-2005 для защиты информация конфиденциального характера должны использоваться средства криптографической защиты информации (далее – СКЗИ), удовлетворяющие требованиям по безопасности информации, устанавливаемым в соответствии с законодательством Российской Федерации. Обязанность соблюдения конфиденциальности персональных данных установлена также ст.7 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – 152-ФЗ), следовательно, вышесказанное положение распространяется и на защиту персональных данных. В ч.4 ст.19 152-ФЗ определено, что состав и содержание необходимых для выполнения требований к защите персональных данных для каждого из уровней защищенности, организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных устанавливаются ФСБ России в пределах ее полномочий. В настоящий момент новые документы ФСБ России еще не утверждены, поэтому необходимо руководствоваться теми, которые действуют с 2008 г. В частности, согласно п.2.3 «Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утв. ФСБ России 21.02.2008 г. № 149/6/6-622, при разработке и реализации мероприятий по организации и обеспечению безопасности персональных данных при их обработке в информационной системе оператор или уполномоченное оператором лицо осуществляет: определение необходимости использования криптосредств для обеспечения безопасности персональных данных и, в случае положительного решения, определение на основе модели угроз цели использования криптосредств для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных и (или) иных неправомерных действий при их обработке.

В соответствии с Методическими рекомендациями по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (утв. ФСБ России 21.02.2008 г. № 149/54-144) основными каналами атак являются, в том числе, каналы связи (как внутри, так и вне контролируемой зоны), не защищенные от несанкционированного доступа к информации организационно-техническими мерами. Понятийный аппарат, содержащийся в Положение ПКЗ-2005, дает основание для возможности применения шифровальных средств для защиты информации при ее передаче по каналам связи: средства шифрования – это аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении (пп «а» п.2 Положение ПКЗ-2005).

Вышесказанное позволяет сделать вывод о целесообразности применения банками шифровальных средств для защиты персональных данных при их передаче по каналам связи. Во исполнение 161-ФЗ Центральным Банком Российской Федерации было принято «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» (утв. Банком России 09.06.2012 г. № 382-П). П.2.9.1 указанного Положения дает основания для возможности использования несертифицированных СКЗИ: «в случае если оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры применяют СКЗИ российского производителя, указанные СКЗИ должны иметь сертификаты уполномоченного государственного органа». Решение об отсутствии необходимости применения СКЗИ может быть принято банком на основании Модели угроз.

Юридическая ответственность

В соответствии с ч.9 ст.19 152-ФЗ решением Правительства Российской Федерации с учетом значимости и содержания

обрабатываемых персональных данных ФСБ России может быть наделена полномочиями по контролю за выполнением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности и не являющихся государственными информационными системами персональных данных. На данный момент такого решения Правительства Российской Федерации еще не принято, в связи с чем правомерно предполагать невозможность проведения проверок ФСБ России в данной сфере до принятия такого решения.

Тем не менее, в соответствии со ст.19.5 КоАП РФ невыполнение в установленный срок законного предписания (постановления, представления, решения) органа (должностного лица), осуществляющего государственный надзор (контроль), об устранении нарушений законодательства влечет наложение административного штрафа на должностных лиц - от одной тысячи до двух тысяч рублей или дисквалификацию на срок до трех лет; на юридических лиц - от десяти тысяч до двадцати тысяч рублей.

Кроме того, согласно ст.74 Федерального закона от 10.07.2002 г. № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» в случаях нарушения кредитной организацией федеральных законов, издаваемых в соответствии с ними нормативных актов и предписаний Банка России, непредставления информации, представления неполной или недостоверной информации Банк России имеет право требовать от кредитной организации устранения выявленных нарушений, взыскивать штраф в размере до 0,1 процента минимального размера уставного капитала либо ограничивать проведение кредитной организацией отдельных операций на срок до шести месяцев. А в соответствии со ст. 15.36 КоАП РФ повторное в течение года неисполнение оператором платежной системы, операционным центром, платежным клиринговым центром предписания Банка России, направленного им при осуществлении надзора в национальной платежной системе, влечет наложение административного штрафа на должностных лиц в размере от тридцати тысяч до пятидесяти тысяч рублей; на юридических лиц - от ста тысяч до пятисот тысяч рублей.

защита информации в национальной платежной системе, персональные данные, средства защиты информации, аналитика