ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ (Банк России)

Департамент информационной безопасности

107016, Москва, ул. Неглинная, 12

www.cbr.ru

тел.: (495) 771-91-00

От 28.09.2018 № 56-3-4/124

на № НСФР-02/1-478 от 06.09.2018

О рассмотрении обращения НСФР

Председателю Национального совета финансового рынка

А.В. Емелину

emelin@rosfinsovet.ru

Уважаемый Андрей Викторович!

Департамент информационной безопасности Банка России рассмотрел Ваше обращение о надзоре за соблюдением кредитными организациями требований Федерального закона от 31.12.2017 № 482-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» в части обработки персональных данных (далее – обращение) и сообщает следующее.

В соответствии с положениями Федерального закона от 10.07.2002 № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» Банк России не наделен полномочиями по предоставлению официального толкования законодательства Российской Федерации, в том числе Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ) и Федерального закона от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (далее – Федеральный закон № 115-ФЗ).

Вместе с тем полагаем возможным сообщить мнение Департамента информационной безопасности Банка России в отношении вопросов, отраженных в обращении.

1. По вопросу применения к банкам мер надзорного воздействия при обработке персональных данных в процессе сбора, обработки, размещения, проверки и обновления сведений, как при первичном размещении сведений о физических лицах в Единой системе идентификации и аутентификации (далее – ЕСИА) и Единой биометрической системе (далее – ЕБС), так и при осуществлении дистанционной идентификации физических лиц с использованием ЕСИА и ЕБС.

Согласно частям 1, 1.1 статьи 23 Федерального закона № 152-ФЗ уполномоченным органом по защите прав субъектов персональных данных является федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных, который обеспечивает, организует и осуществляет государственный контроль и надзор за соответствием обработки персональных данных требованиям Федерального закона 152-ФЗ и принятых в соответствии с ним нормативных правовых актов (государственный контроль и надзор за обработкой персональных данных).

На основании части 11 статьи 14.1 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» контроль и надзор за выполнением банками организационных и технических мер по обеспечению безопасности персональных данных при использовании ЕБС осуществляются Банком России.

Таким образом, при обработке персональных данных, как при первичном размещении сведений о физических лицах в ЕСИА и ЕБС, так и при дистанционной идентификации физических лиц с использованием ЕСИА и ЕБС, государственный контроль и надзор за обработкой персональных данных осуществляет федеральный орган исполнительной власти,

реализующий функции по контролю и надзору за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных, а контроль и надзор за выполнением банками организационных и технических мер по обеспечению безопасности персональных данных при использовании ЕБС осуществляет Банк России.

2. По вопросу аттестации рабочих мест сотрудников банков, на которых выполняется непосредственный сбор биометрических персональных данных, а также аттестации сетей связи, используемых для передачи собранных биометрических персональных данных между собственными внутренними структурными подразделениями банков, при условии применения сертифицированных программно-аппаратных средств и предусмотренных законодательством Российской Федерации процедур оценки корректности их встраивания, при реализации мер защиты, предусмотренных перечнем актуальных угроз.

Согласно пункту 10 статьи 3 Федерального закона № 152-ФЗ информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств. Следовательно, рабочие места сотрудников банков, на которых выполняется непосредственный сбор биометрических персональных данных, а также сети связи, используемые для передачи собранных биометрических персональных данных, являются информационной системой персональных данных.

Пунктом 4 части 2 статьи 19 Федерального закона № 152-ФЗ предусмотрена обязанность оператора при обработке персональных данных выполнить оценку эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных.

При этом форма оценки эффективности принимаемых мер по обеспечению безопасности персональных данных Федеральным законом № 152-ФЗ не определена. Нормативными правовыми актами Банка России

форма оценки эффективности принимаемых мер по обеспечению безопасности персональных данных также не определена.

Таким образом, форма оценки эффективности принимаемых мер по обеспечению безопасности персональных данных определяется внутренними документами банка, а также условиями подключения и использования ЕСИА и ЕБС.

При этом возможно выполнять аттестацию рабочих мест сотрудников банков, на которых осуществляется непосредственный сбор биометрических персональных данных, а также аттестацию сетей связи, используемых для передачи собранных биометрических персональных данных между собственными внутренними структурными подразделениями банков, при условии применения сертифицированных программно-аппаратных средств и предусмотренных законодательством Российской Федерации процедур оценки корректности их встраивания, как возможную форму оценки эффективности принимаемых мер по обеспечению безопасности персональных данных.

Директор В.А. Уваров

Исп. Бойко О.А.
2-74-40