



ЦЕНТРАЛЬНЫЙ БАНК
РОССИЙСКОЙ ФЕДЕРАЦИИ
(Банк России)

Главное управление безопасности
и защиты информации

107016, Москва, ул. Неглинная, 12

№ _____

на № _____ от _____

Еход. № 1159
"20" 09 2010 г.

Президенту Ассоциации
русских банков

Г. А. Тосуняну

121069, г. Москва, Скатертный пер., д. 20, стр. 1

Уважаемый Гарегин Ашотович!

Главное управление безопасности и защиты информации сообщает следующее.

Относительно необходимости получения операторами персональных данных, в частности, кредитными организациями, лицензий на деятельность по технической защите конфиденциальной информации в действующем законодательстве существует коллизия. Федеральный закон от 8 августа 2001 г. № 128-ФЗ «О лицензировании отдельных видов деятельности» (далее ФЗ-128) содержит требования получения лицензии на деятельность по технической защите конфиденциальной информации, тогда как термин «конфиденциальная информация» в законодательстве не определен и, следовательно, не определено, относятся ли персональные данные к конфиденциальной информации. В настоящее время готовятся поправки в ФЗ-128, разрешающие данную коллизию.

Кроме того, в соответствии со статьей 2 ФЗ-128 действие данного закона не распространяется на деятельность кредитных организаций.

Исходя из этого, до внесения поправок или до получения прямого указания (замечания) Федеральной службы по техническому и экспортному контролю рекомендуем не заниматься вопросом лицензирования на осуществление деятельности по технической защите конфиденциальной информации при проведении мероприятий по обеспечению безопасности в информационных системах персональных данных для собственных нужд.

В целях выполнения в кредитных организациях требований Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и требований (рекомендаций) Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), Федеральной службы

025035

безопасности Российской Федерации (ФСБ России) и Федеральной службы по техническому и экспортному контролю (ФСТЭК России) разработаны отраслевые документы, регламентирующие обработку и обеспечение безопасности персональных данных в кредитных организациях. Эти документы включают:

1. Четыре документа, входящие в комплекс документов в области стандартизации Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации" (далее - Комплекс БР ИББС):

- четвертая редакция стандарта Банка России отраслевого применения СТО БР ИББС-1.0-2010 "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения" (далее - стандарт Банка России СТО БР ИББС-1.0), доработанная в части требований по обработке и обеспечению безопасности персональных данных в соответствии с Отраслевой моделью угроз;

- третья редакция стандарта Банка России отраслевого применения СТО БР ИББС-1.2-2010 "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0" (далее СТО БР ИББС-1.2-2010), доработанная в части требований по обработке и обеспечению безопасности персональных данных в соответствии с Отраслевой моделью угроз;

- рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Отраслевая частная модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных организаций банковской системы Российской Федерации» (РС БР ИББС-2.4) (далее - Отраслевая модель угроз);

- рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Требования по обеспечению безопасности персональных данных в информационных системах персональных данных организаций банковской системы Российской Федерации» (далее - рекомендации в области стандартизации Банка России РС БР ИББС-2.3).

2. Методические рекомендации по выполнению законодательных требований при обработке персональных данных в организациях БС РФ, разработанные совместно Банком России, Ассоциацией российских банков (АРБ) и Ассоциацией региональных банков России (Ассоциацией «Россия»).

Документы Комплекса БР ИББС согласованы ФСБ России, Роскомнадзором, ФСТЭК России.

Банк России, АРБ и Ассоциация региональных банков России рекомендуют ввести Комплекс БР ИББС решением организации БС РФ (приказом, распоряжением) и руководствоваться им при проведении работ по защите информации, отнесенной к персональным данным, к банковской тайне, к коммерческой тайне. Порядок применения документов Комплекса БР ИББС в кредитных организациях устанавливается в согласованном Роскомнадзором, ФСБ России, ФСТЭК России письменном обращении Банка России, АРБ и Ассоциации региональных банков России (Ассоциации «Россия») в кредитные организации о введении в действие Комплекса БР ИББС для приведения деятельности организаций банковской системы Российской Федерации в соответствие с требованиями законодательства в области персональных данных (от 28.06.2010 №01-23/3148).

В случае, если Комплекс БР ИББС в кредитной организации не вводится, она должна руководствоваться нормативно-правовыми актами ФСБ России, Роскомнадзора и ФСТЭК России.

Оценка (как самооценка, так и внешняя оценка) соответствия информационной безопасности кредитной организации требованиям стандарта Банка России СТО БР ИББС-1.0 проводится в соответствии со следующими документами:

- стандарт Банка России СТО БР ИББС-1.2-2010;

- стандарт Банка России СТО БР ИББС-1.1 -2007 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности» (внешняя оценка соответствия).

- рекомендации по стандартизации Банка России РС БР ИББС-2.1-2007 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Руководство по самооценке соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0» (самооценка соответствия).

Все обозначенные выше документы опубликованы на Web-сайте Банка России в сети Интернет (www.cbr.ru).

В качестве проверяющих организаций рекомендуется привлекать организации, входящие в состав Сообщества пользователей стандартов Банка России по обеспечению информационной безопасности организаций банковской системы Российской Федерации (ABISS - Association for Banking Information Security Standards, www.abiss.ru).

Заместитель начальника Главного управления
безопасности и защиты информации

А.П. Курило