

Мнение специалиста



Владимир ЧЕРНЫШЕВ,
директор по работе с ключевыми заказчиками,
ЗАО «С-Терра СиЭсПи»

Необходимость мер по защите персональных данных в последние годы прочувствовали на себе не только операторы, работающие с такими данными, но и обычные граждане, по роду своей профессиональной деятельности с этой областью никак не связанные. Несмотря на принятый в 2006 г. Федеральный закон «О защите персональных данных», сведения о частной жизни граждан с досадной

периодичностью становятся доступны всем желающим, в том числе и представителям криминальных структур, служа им хорошим подспорьем в осуществлении противоправных действий. Согласно данным, размещенным на сайте Роскомнадзора, в 2011 г. только на радиоынках Москвы правоохранительными органами было изъято несколько сотен физических носителей информации, содержащих персональные сведения.

В этих условиях естественным стало принятие в России дополнительных мер по дальнейшему наведению порядка в сфере защиты персональных данных, в том числе совершенствование нормативной правовой базы. На это, в частности, направлен и упоминаемый в статье Федеральный закон от 25.07.2011 № 261-ФЗ «О внесении изменений в Федеральный закон «О персональных данных», несколько упростивший стоящую перед операторами задачу реализации требований по защите персональных данных.

Несмотря на некоторые упрощения, при выполнении этого закона малые и средние предприятия оказались все-таки в довольно сложном положении. Во многом это определено нехваткой или отсутствием у них специалистов в области информационной безопасности. В таких условиях целесообразно привлечь к решению своих проблем компании, специализирующиеся в области информационной безопасности и имеющие соответствующие лицензии. Благо, таких предложений достаточно много.

С другой стороны, многие малые и средние предприятия по-прежнему занимают выживательную позицию, рассчитывая на то, что уполномоченные органы не дойдут до них с проверкой выполнения этого закона.

Несомненно, для операторов из числа малых и средних предприятий требуется формирование хорошей мотивационной базы, определяющей необходимость соблюдения требований закона. Положительное влияние могут оказать как ужесточение и неизбежность наказания за нарушения установленных требований, так и укрепление репутации добросовестного предприятия-оператора в сознании бизнес-сообщества.

В старой редакции вопросам обеспечения безопасности была посвящена статья 19, суть которой сводилась к следующему:

- оператор обязан принимать необходимые организационные и технические меры для защиты персональных данных;

- Правительство Российской Федерации устанавливает требования к обеспечению безопасности персональных данных, а ФСБ России и ФСТЭК России в пределах своей компетенции осуществляют контроль и надзор за их исполнением.

В новой редакции ст. 19 подверглась существенным изменениям. В частности:

1) она была дополнена перечнем конкретных мероприятий, с помощью которых достигается безопасность персональных данных. Кстати, большинство этих мероприятий звучало и ранее, в той или иной степени они были отражены в Постановлении Правительства № 781,

которое в соответствии с законом определяло перечень требований к обеспечению безопасности персональных данных;

2) введены новые понятия – «уровни защищенности» и «угрозы безопасности»;

3) изменился и порядок проведения работ. В настоящее время он выглядит следующим образом:

- обязанность принимать необходимые организационные и технические меры (или обеспечивать их принятие) по-прежнему лежит на операторе;

– Правительство Российской Федерации с учетом возможного вреда субъекту персональных данных, объема и содержания обрабатываемых персональных данных, вида деятельности, актуальности угроз безопасности устанавливает:

а) уровни защищенности персональных данных в зависимости от угроз безопасности этих данных;

б) требования к защите персональных данных, исполнение

которых обеспечивает устойчивые уровни защищенности

– ФСБ России и ФСТЭК России определяют состав и содержание организационных и технических мер, необходимых для выполнения установленных Правительством требований к защите персональных данных для каждого из привлекаемых юридических лиц, юридических лиц, имеющих право на осуществление контроль и надзор. Но в отличие от предыдущей редакции – не ко в отношении государственных информационных систем. Возможность проверить операторов государственных информационных систем появляется только в случае принятия решения Правительства о введении учетом значимости и специфики обрабатываемых операторами персональных данных.

Удалось ли в Федеральном законе о защите персональных данных урегулировать все вопросы, связанные с соблюдением прав и свобод граждан в сфере обработки персональных данных, и в какой мере соблюден баланс интересов оператора и государства, упростилась ли процедура применения норм законодательства, покажут временные испытания, которые предстоит пройти в практике его применения.

Во многом это будет зависеть от содержания создаваемого в ближайшее время ФСБ России и МИДом России перечисленных нормативных и правовых документов. Главное, чтобы требования, ли реализуемы, а нормы, в том числе и операторам, не имеют специальной прописки и опыта проведения работ.

В значительной степени
могли бы способствовать:
1) создание методических
распределенных документов, в
которых бы нашли отражение
проведения работ инспекци-
ями, малыми, средними органи-
зациями, были бы изложены
и понятные операторам
и методики защиты, а
сходство бизнес-процессов
данные на типизации реаль-

Такие рекомендации должны не только оптимизировать функции щиты и минимизировать риски, но и на обеспечение безопасности информационных систем, а также операторов профессиональных навигационных систем в данной области.

Опыт создания и разработки отраслевых документов