

Пока гром не грянул

Для создания систем защиты персональных данных времени не остается

Текст: Константин Совалин, эксперт компании ReignVox

На исходе август, до вступления в силу закона «О персональных данных» остается совсем немного. Но мало кто может похвастаться внедрением системы защиты этих данных в соответствии с нормативными требованиями. О серьезности намерений контролирующих органов свидетельствует отчет Роскомнадзора, а также план проверок, размещенный на официальном сайте этого ведомства.

НОВЫЙ ГОД ПРИДЕТ ВНЕЗАПНО

Закон напрямую касается учреждений, которые обслуживают физических лиц. Это кредитно-финансовые организации, а также медицинские, страховые компании, операторы сотовой связи. Принятие закона в 2006 году было воспринято почему-то пассивно, хотя предстояло выполнить большой объем работы для приведения систем в соответствие с требованиями закона. Кроме того, существующие на сегодняшний день методики защиты информации сложны и затратны, и была надежда на то, что удастся пролоббировать поправки в закон.

Однако все надежды исчезли в июне этого года, когда Роскомнадзор ответил на обращение банкиров по поводу переноса сроков аудита ИС на соответствие 152-ФЗ. Ведомство посчитало, что изменять дату нецелесообразно, но подсластило пилюлю, признав возможность изменения в законах, касающихся защиты персональных данных. Другими словами, с 1 января 2010 года все информационные системы операторов, работающих с персональными данными, должны будут соответствовать требованиям закона.

Авторы ответа признали, что существующая методология требует проведения классификации персональных данных и использования криптографических средств. Роскомнадзор одновременно отметил, что ведомство не наделено нужными законодательными полномочиями.



ПО-ДРУГОМУ И БЫТЬ НЕ МОГЛО

Роскомнадзор дал вполне корректный и ожидаемый ответ: закон не менялся, на подготовку к вступлению требований в силу отводилось три года – срок более чем достаточный. Эксперты считают, что операторы, работающие с персональными данными, в частности банки, проигнорировавшие требования закона, рискуют, что к неурядицам, вызванным финансовым кризисом, добавятся санкции регулятора.

Однако едва ли кто решится делать это в кризис. Поэтому банки, по-видимому, будут иметь некоторую фору, продолжительность которой, правда, никому не известна. Но, несмотря на это, банкиры намерены добиваться изменения закона. Так, по словам депутата Госдумы и президента Ассоциации региональных банков Анатолия Аксакова, осенью будут организованы парламентские слушания, участники которых попытаются доказать, что сроки аудита информационных систем на соответствие закону необходимо перенести на более позднее время. «Если сегодня Роскомнадзор будет проводить аудит соответствующих компаний, то ему нужно будет проверять ежедневно около 1000 организаций. То, что это нереально, прекрасно понимают все. А когда закон объективно невыполним, то возникают возможности для коррупции», – уверен законодатель.

НА ВСЕХ ФРОНТАХ

Но независимо от того, чего удастся добиться лоббистам, к приходу проверяющих надо тем не менее готовиться. Перечень требований и мероприятий, которые необходимо выполнить в ходе предпроектного обследования, содержится в нормативно-методических документах регуляторов, поэтому остановимся на вопросах, о которых говорят меньше и которые не получили широкого освещения.

В ходе обследования информационной системы надо изучить информационные потоки и построить модель обработки персональных данных в ходе бизнес-процессов. Как правило, такая задача наиболее успешно решается в организациях, где внедрен процессный подход: детально описаны процессы и их принадлежность, установлены границы и документированы источники.

В соответствии с требованиями регуляторов обработка персональных данных и их передача третьим лицам должна быть юридически обоснована. Поэтому при описании потоков необходимо выявить все системы, связанные с их обработкой, проанализировать все точки входа и выхода информации и для каждой из них определить юридическое обоснование в соответствии с требованиями п. 8 «Рекомендаций по заполнению образца формы уведомления об обработке (о намерении осуществлять обработку) персональных данных» и соответствующего гражданско-правового договора, определяющего условия обработки данных.

Таким образом, информационная модель потоков персональных данных на низком уровне позволяет составить матрицу соответствия процессов обработки ПД нормативно-правовым документам, подтверждающим легитимность их обработки. В дальнейшем актуализация информационной модели позволит поддерживать легитимность обработки ПД и уровень регуляторных рисков на должном уровне. 