ОЛЕГ СЕДОВ

Двенадцать месяцев спустя

На момент написания этой статьи законопроект о переносе на один год сроков приведения информационных систем в соответствие с федеральным законом № 152-ФЗ «О персональных данных» был принят в двух чтениях. Шансы, что его примут и в третьем чтении, довольно высоки. Если сроки перенесут, что будет через год?

Федеральный закон РФ № 152-ФЗ «О персональных данных» от 27 июля 2006 года предписывал привести информационные системы в той части, которая касается персональных данных, в соответствие с требованиями этого закона не позднее 1 января 2010 года.

«Требования закона были настолько невнятны, а масштабы паралитического воздействия на компании страны столь велики, что возникшее ощущение обреченности и перспектива эпидемиологической гибели компаний привели к бездействию их руководства как до вступления закона в силу, так и после», — вспоминает Сергей Захарцев, заместитель директора департамента ИТ АКБ «Инвестбанк».

По мере того, как проходил первый шок, появлялось и осознание необходимости выработать стратегию действий. Сложились три стратегии поведения компаний по реализации требований закона: выполнить требования закона; соблюсти формальные процедуры, чтобы избежать или минимизировать наказание; ничего не делать и решать проблемы по мере их возникновения неформальным путем. «Соотношение компаний, придерживающихся таких стратегий, можно выразить пропорцией 1:10:100», — так оценивает ситуацию Захарцев.

По мнению Рустэма Хайретдинова, заместителя генерального директора компании InfoWatch, на сегодняшний день у предприятий уже есть осмысленная стратегия поведения в новых условиях: «Одни провели аудит и внедрили определенные регламентные процедуры, полагая, что таким образом выполнили требования закона и смогут «отмахиваться» сертификатом. Другие решили, что ничего делать не станут, а будут откупаться от проверок, потому что так дешевле. Третьи подготовили документы, из которых следует, что организация относится к более низкой категории (поскольку, например, персональные данные у них обезличены) и не обязаны соответствовать требованиям закона. Я видел реальное распоряжение в одной компании, в котором предписывалось термин «персональные данные» вслух не произносить. В общем, все «окопались» наилучшим, по их мнению, образом и ждут проверок. А проверки покажут, кто был прав».

Алексей Лукацкий, менеджер по развитию бизнеса компании Cisco Systems, трагикомизм сложившейся ситуации комментирует следующем образом: «Те, кто поторопился или испугался, станут кусать локти, вспоминая о потраченных деньгах. Те, кто спустил все на тормозах, получили годовую передышку и возможность обдуманно подготовиться к реализации требований закона. Ну а те, кто уже ведут соответствующие проекты, просто продолжат их дальше».

«Я не знаю компаний, которые бы сделали что-то практическое. Подозреваю, что полноценно разработанных и выполненных программ по обеспечению требований этого закона просто нет», — считает Алексей Затопляев, директор по ИТ управляющей компании «Бауцентр Рус».

В целом стоит признать, что все инициативы компаний, направленные на то, чтобы соответствовать требованиям закона, не имели смысла с точки зрения сертификации (аттестации). «Поначалу никто (ни компании, ни регулирующие органы) толком не понимал, как проходить сертификацию, что для этого требуется, какие процедуры следует выполнять. Даже если сертификация пройдена, то это не исключает возможность ее повторного прохождения. Парадоксально, но оно может оказаться гораздо проблематичнее, чем прохождение сертификации впервые», — отмечает Захарцев.

Повод для переноса сроков

Перенос на год сроков приведения систем в соответствие с законом № 152-ФЗ продиктован здравым смыслом, считает Евгений Модин, руководитель

направления консалтинга компании Aladdin: «Перенос сроков — это действительно серьезное событие, возможно, главное для 2009 года. Прежде всего потому, что отраслевое сообщество было услышано государством. Эта отсрочка свидетельствует о том, что диалог между бизнесом и властью возможен и, более того, можно найти компромиссное решение».

Лукацкий считает, что основная причина переноса сроков связана с непрозрачностью требований и невозможностью их выполнить за отведенное до 1 января 2010 года время: «Это действительно серьезно. Требования ФСТЭК менялись неоднократно, а процесс их изменения и утверждения вызывал огромное количество вопросов и нареканий. Не случайно на парламентских слушаниях в Госдуме не раз говорилось, что перенос сроков — крайняя мера, но необходимая, чтобы дать возможность операторам персональных данных серьезно подготовиться, а регуляторам извлечь уроки из вполне выпущенных на рынок требований (кстати, гриф «для служебного пользования» с них сняли только в середине ноября 2009 года)».

Захарцев более сдержанно оценивает события: «Истинная причина лежит в осознании регулирующими органами масштабов бедствия, которое возникнет при попытке соблюсти требования этого закона. Исполнение санкций по закону приведет к массовой ликвидации компаний, что обернется экономическим бедствием для страны. Если же это делать не массово, то получится, что закон обязателен не для всех. В стране нет ресурсов даже для контроля за соблюдением закона. Отсюда вывод: закон невозможно исполнить ни тем, кто должен соблюдать его требования, ни тем, кто должен контролировать его исполнение. Перенос сроков — это попытка хоть в какой-то мере снизить массовые репрессивные санкции закона».

Что будет через год?

По мнению Модина, требования закона изначально были достаточно внятными, особенно для тех, кто интересовался вопросами информационной безопасности и до его появления: «Был ряд положений и требований, смысл которых можно было трактовать двояко, но почти все они уже разъяснены. На мой взгляд, в части адекватного восприятия требований закона № 152-ФЗ изменилось только одно — всем стало понятно, что работу по приведению в надлежащий вид своих систем придется выполнять».

Лукацкий считает, что требования закона понятны, но невнятно изложены. «Неразумно требовать от гостиниц, ЖЭКов, поликлиник и школ выполнять требования, превышающие требования к защите государственной тайны. Многие из упомянутых категорий операторов персональных данных относятся к бюджетным организациям, но в бюджетах ни на 2009, ни 2010 годы денег на реализацию закона не было предусмотрено. Сейчас идет активная работа с регуляторами в части изменения требований в сторону отраслевых стандартов».

По прогнозам Хайретдинова, возможно совсем парадоксальное развитие событий: «Требования закона защищать данные абсолютно адекватные. А вот требования наказывать тех, кто неправильно защищает, а не тех, кто допустил утечки, абсолютно неадекватное, особенно в силу неполноты модели угроз. Другими словами, если я защищался правильно (имею сертификат) и потерял данные миллиона человек, то я не виноват, а если я защищал данные, но не так, как рекомендуют регуляторы, и не допустил утечки, я виноват. Вполне возможно, что после утечки данных из сертифицированных систем через инсайдера, например, сначала появятся иски от пострадавших к оператору персональных данных (строго в соответствии с законом), а потом — от оператора к регулятору, сертифицировавшему его систему».

Захарцев убежден, что внятность и понятность требований регуляторов для компаний пока недостаточна: «При том многообразии средств автоматизации обработки персональных данных, архитектур построения информационных систем, разномасштабности компаний формулировать единые требования весьма проблематично. Если их делать едиными, то они будут носить слишком общий характер, и тогда их реализацию сложно регламентировать в конкретном случае. Если же их делать детальными, то невозможно будет реализовать в условиях конкретной компании, поэтому требования носят компромиссный характер, то есть они универсальные и конкретные. Отсюда и невысокая степень их внятности и понятности».

По результатам парламентских слушаний в Госдуме были утверждены рекомендации Госдуме, Правительству РФ, профильным министерствам и органам исполнительной власти по изменению закона № 152-ФЗ, смежных законов и подзаконных актов. «Эти рекомендации здравы, нынешний год уйдет именно на их включение в различные нормативные акты. Одной из таких рекомендаций является создание отраслевых стандартов. По этому пути сейчас пошли многие отраслевые ассоциации, — рассказывает Лукацкий. — Как бы там ни было, времени на передышку очень мало и расслабляться не стоит».

С ним согласен и Модин: «За работу надо браться уже сейчас. В течение года возможны изменения в законодательстве в части ужесточения наказания за невыполнение требований по защите персональных данных. Также возможно появление новых продуктов и решений для обеспечения выполнения требований нормативной базы №152-ФЗ. Чтобы не «наломать дров», грамотные операторы, скорее всего, будут активно пользоваться услугами аудита и консалтинга в этой области, а значит, данный рынок получит хорошее подспорье».

Захарцев опасается, что компании так и не начнут ничего предпринимать для выполнения требований закона № 152-ФЗ: «Все компании выбрали стратегию своего поведения в отношении реализации требований этого закона. Подавляющее большинство компаний делать ничего не будет. Да и не могут они что-либо делать, потому что для предприятия реализация требований закона о персональных данных — это крупный проект, который требует значительных финансовых и людских ресурсов. Выделение таких ресурсов в большинстве компаний не запланировано. В целом принятие закона очень напоминает показную кампанейщину». CIO.RU