Персональные данные граждан, защищают ли их?

Текст: Юлия ЮТКИНА

Назад к бумажной картотеке

На прошлой неделе Госдума России приняла во втором чтении поправки к 152-му Федеральному закону «О персональных данных». Если изменения в итоге будут окончательно приняты парламентариями, то срок приведения организациями своих информационных систем в соответствие с обязательными требованиями будет отодвинут ровно на год — до 1 января 2011 года.

Разговоры о несовершенстве абсолютно нового для России закона ведутся со времени его подписания президентом в 2006 году. Перенос срока, по сути, в канун вступления в силу ключевых требований закона свидетельствует, к сожалению, о массовой неготовности бизнеса и государственных учреждений к их выполнению и защите персональных данных граждан.

От сбора до уничтожения

Поясним, о чем идет речь. Известно, что учитывают нас очень многие ведомства: Пенсионный фонд и Федеральная налоговая служба, Фонд социального страхования и Минздрав, МВД и коммунальщики… Но дело в том, что повсеместно в России практика работы с приватными данными о гражданах складывалась стихийно. Где-то (по преимуществу в банках) действительно предпринимались меры по защите от утечек информации о клиентах, большинство же организаций защитой от так называемого инсайдерства («слив» нужных сведений за деньги) озабочено не было. В результате незаконная продажа всевозможных баз данных, содержащих личную информацию граждан, была поставлена, по сути, на поток, что приносило (да и приносит) продавцам огромные прибыли. Не секрет, что данные довольно оперативно обновляются на «пиратских» CD-дисках. И неприятные последствия доступа посторонних к личной информации испытали уже очень многие. К примеру, если соответствующее условие не было изначально прописано в кредитном договоре, банк охотно делится вашими координатами с коллекторами, выбивающими долги.

Собственно, приступить к разработке 152-го ФЗ Россию подвигли не только эти обстоятельства внутреннего плана, но во многом и процессы международной интеграции, игнорировать которые было невозможно: в конце 2001 года страна подписала конвенцию Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных».

Персональными данными, требующими защиты, теперь считаются сведения о фактах, событиях и обстоятельствах частной жизни конкретного гражданина. Скажем, в здравоохранении конфиденциальны Ф.И.О. пациентов, пол, дата рождения, адрес места жительства, реквизиты документа, удостоверяющего личность, номер полиса медицинского страхования, сведения о наличии льгот, страховой номер индивидуального лицевого счета в Пенсионном фонде, сведения о случаях обращения за медицинской помощью и о состоянии здоровья. А для работников конфиденциальны также ИНН, данные кадрового учета (образование, квалификация, должность и т.д.), сведения о заработной плате и прочее. Суть защиты этой информации в жестких технических требованиях, которые должны соблюдаться при любых операциях с ней — от сбора и обработки вплоть до уничтожения.

Изначально три года — до 1 января 2010 года — коммерческим и государственным структурам (операторам персональных данных) давалось на то, чтобы изменить практику документооборота. Проще говоря, установить на компьютеры сертифицированные ПО и системы защиты и провести их аттестацию. Параллельно каждая организация обязана разработать довольно большой пакет документов, отражающий все аспекты информационной безопасности: нужно обосновать и выбранный уровень защиты, и отдельные аспекты его обеспечения.

Типовые ошибки

Что ж, приходится констатировать — массового стремления к приведению в порядок баз данных в России все это время не наблюдалось. Организации «вдруг» не стали сознательными, тем более что репрессивных мер к ним пока не применялось. Процедура такова, что каждое предприятие независимо от формы собственности сначала обязано своевременно уведомить Роскомнадзор о намерении осуществлять обработку таких данных и указать ее цели.

Как показывает статистика по Ставрополью, управление Роскомнадзора по СК по регистрации уведомлений от операторов добилось высоких показателей по ЮФО. Однако очевидно, что заявили о себе пока далеко не все. И уже с 1 января территориальные подразделения ведомства должны приступить к проверкам операторов на предмет защищенности информационных систем и наказывать нарушителей. Санкции за нарушения закона предусмотрены серьезные — от штрафов до приостановления работы предприятия.

Но надо признать, что управление Роскомнадзора, ведущее реестр операторов, пока занимает достаточно конструктивную позицию.

— На данном этапе мы направляем усилия не только на то, чтобы применить санкции, но и стремимся по максимуму предварительно выявить существующие несоответствия требованиям закона, указать на них оператору и способствовать их устранению, — рассказывает начальник отдела по защите прав субъектов персональных данных Управления Роскомнадзора по СК В. Сергиенко. — Тенденция на ближайшее время сохранится. У нас есть понимание, что на данном этапе операторам сложно выполнить все регламентации и следовать букве закона. Потому работаем с организациями в том числе в консультативном режиме.

Типовыми нарушениями, подчеркивают в ведомстве, сейчас по-прежнему становятся случаи, когда информация о человеке передается без его письменного разрешения посторонним лицам. Операторы также не уведомляют Роскомнадзор об уничтожении баз со сведениями или, напротив, хранят информацию дольше, чем предусмотрено целью ее сбора.

— Кстати, мы продолжаем прием уведомлений об обработке персональных данных, — рассказывает руководитель Управления Роскомнадзора по СК Д. Поляничев. — Причем для упрощения процедуры функционирует общедоступный Портал персональных данных http://pd.rsoc.ru, где не только размещена вся необходимая информация, но также доступна интерактивная форма заполнения уведомления об обработке персональных данных.

Под одну гребенку

Многие эксперты высказывают мнение, что годовая отсрочка, которая скорее всего вот-вот будет одобрена Думой России, не принесет желаемых результатов без внесения серьезных изменений в сам закон. В частности, соответствующие предложения готовит Минкомсвязи и обещает внести их на рассмотрение уже в начале будущего года.

Основные проблемы видятся в том, что у нас в отличие от более продвинутой в этом вопросе Европы пока нет отраслевых стандартов защиты персональных данных. То есть по большому счету требования ко всем структурам идентичны. А ведь изначально понятно, что тот или иной оператор, обрабатывающий информацию, к примеру, не должен накапливать избыточные данные и должен вовремя от них избавляться. К примеру, очевидное нарушение может заметить каждый из нас, когда для выдачи дисконта в торговом центре в анкете вас просят указать адрес проживания, год рождения, место работы и т.д. Вот и задаешься вопросом — зачем информация в таком объеме нужна магазину?..

Крайне сложная ситуация складывается в здравоохранении. Так, рядовой городской поликлинике для защиты информации о своих клиентах нужно изыскать несколько миллионов рублей, чтобы закупить программное обеспечение, провести аттестацию, учебу сотрудников и т.д. Кроме того, штатные расписания практически всех учреждений здравоохранения и образования просто не предусматривают должностей по информационной безопасности, и в их бюджетах нет строки расходов на требуемую аттестацию и сертификацию техники. Как ни странно это звучит, но тогда тем же больницам и поликлиникам экономнее вернуться к карточной системе и заполнять документы вручную…

В прессе и публичных выступлениях политиков и экспертов в целом звучит положительная оценка закона о защите персональных данных как способного повлиять на общий уровень информационной безопасности в компаниях и стране. Но, учитывая приведенные выше и другие моменты, реально работать его требования начнут не сразу, обкатка закона, по некоторым прогнозам, грозит затянуться года на три… Хотя неизвестно, удастся ли в итоге преодолеть пресловутый человеческий фактор, который почти в семидесяти процентах, по данным исследований, является причиной утечки информации…