Средства защиты персональных данных:
проблемы оценки соответствия

Александр СОКОЛОВ,
генеральный директор
компании «Элвис-Плюс»

Проблема защиты персональных данных не нова. Достаточно напомнить, что разработка Федерального закона «О персональных данных» заняла более десяти лет. Декларации о необходимости их защиты принимались и раньше (например, ст. 11 «трехглавого» Федерального закона «Об информации, информационных технологиях и о защите информации»). Однако долгое время было непонятно, что такое «персональные данные» и каковы механизмы их правовой защиты. Сегодня средства защиты персональных данных есть практически в каждой компании. Но насколько они отвечают предъявляемым требованиям? И как можно гарантировать их эффективность?

Законодатель в поисках золотой середины

Трудности подготовки Закона «О персональных данных» носили как объективный (проблема определения состава данных), так и субъективный характер (невозможность договориться по некоторым положениям). И все-таки закон приняли. В первую очередь это было продиктовано необходимостью исполнения Российской Федерацией положений международных договоров и общепринятых международных норм и принципов, а также создания гарантий и правовых механизмов защиты прав на личную тайну и неприкосновенность частной жизни при сборе и использовании персональных данных. Отсутствие такого закона существенно ограничивало международные контакты, поскольку в Европе щепетильно относятся к вопросу соблюдения прав на частную жизнь. Общепринятые международные нормы и принципы защиты персональных данных содержатся, например, в Конвенции Совета Европы «Об информации персонального характера» и в Директиве Европейского парламента и Совета 95/46/ЕС от 24.10.95 «О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных».

Иного рода сложности возникают при автоматизированной обработке информации в целом и персональных данных в частности, поскольку многократно возрастает вероятность их утечки и разглашения. Стоит обратить внимание на то, что Закон называется «О персональных данных», а не «О защите персональных данных», ибо охватывает все основные аспекты обращения с такими данными и определяет взаимоотношения субъектов в данной сфере. Защита – лишь один, пусть и очень важный, аспект работы с персональными данными. Законодателю было непросто найти ту самую «золотую середину», чтобы не скатиться в чисто техническую область и между тем не забыть о технических проблемах защиты персональных данных. Кажется, он с этой задачей справился – построил вполне логичную схему, определяющую меры обеспечения безопасности персональных данных и разделяющую полномочия:

- Правительство РФ устанавливает требования к обеспечению безопасности персональных данных при их обработке;
- оператор обязан принимать организационные и технические меры для защиты персональных данных от несанкционированного доступа, уничтожения, изменения, блокирования, копирования, распространения и иных неправомерных действий;
- федеральные органы в области обеспечения безопасности (подразумеваются ФСБ и ФСТЭК России. – **Прим. автора**) осуществляют контроль и надзор за правильностью обработки и использования персональных данных;
- лица, виновные в нарушении требований, несут гражданскую, уголовную, административную,

дисциплинарную и иную предусмотренную законодательством РФ ответственность.

Требования закона направлены на персонализацию ответственности за сохранность персональных данных: не поликлиника виновата в разглашении данных, а конкретный сотрудник. Очевидно, что закон будет внедряться медленно, но только до тех пор, пока не начнутся судебные иски по поводу утечки персональных данных. Для этого закон создал все условия. Вопрос в том, насколько российские граждане готовы отстаивать свои интересы в суде, и готов ли наш суд к рассмотрению подобных исков и строительству гражданского общества.

Между тем Россия все глубже интегрируется в мировую экономику. Взаимодействие с другими государствами постоянно развивается. Общепринятые нормы в области информационной безопасности, прежде всего международные стандарты, будут оказывать влияние на российский сегмент рынка. Многие из них уже широко применяются. Все более активное общение с другими странами предполагает и обмен персональными данными, что регламентируется рядом международных конвенций и резолюций.

Средства защиты и пароль над столом...

В настоящее время практически в каждой организации функционируют информационные системы, в которых фиксируются и обрабатываются различные данные о человеке – фамилия, инициалы, дата и место рождения, адрес, семейное, социальное и имущественное положение, образование, профессия, информация о доходах. Кроме того, в этих системах зачастую хранится сопутствующая информация, на основании которой можно получить подобные и иные данные о персоне. По оценкам экспертов, количество операторов персональных данных превышает сегодня 7,5 млн – впечатляющая цифра. Закон «О персональных данных» затрагивает интересы многих крупных и малых компаний. Если в Законе «Об информации, информационных технологиях и о защите информации» говорится о том, что именно надо защищать и что конкретно является объектом конфиденциальной информации, то Закон «О персональных данных» раскрывает состав персональных данных и предусматривает применение технических и организационных мер и средств для обеспечения защиты.

Приведем конкретный пример. В открытых источниках отсутствуют сведения по рынку информационной безопасности в области здравоохранения. По некоторым косвенным данным, можно утверждать, что затраты на информационную безопасность в здравоохранении (а для медучреждений это в основном и есть «персональные данные») составляют примерно 4–6% объема затрат на развитие информационно-телекоммуникационных технологий. В 2008 г. эта сумма может составить 1,1 млрд руб., или 44,6 млн долл. Аналогичные потребности испытывают учреждения ЖКХ, банки и т. д.

В большинстве организаций разумные меры защиты персональных данных все же реализуются, и им, наверно, не придется нести затрат, обусловленных выполнением требований законодательства. Однако нет уверенности в том, что малые и средние компании соблюдают даже минимальный набор уровней безопасности, который диктует закон. Лучшая иллюстрация тому – пароли, приклеенные над столами в офисах многих крупных компаний…

Вопросы без ответов

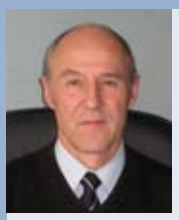
В развитие законов и постановлений Правительства РФ принят ряд нормативных подзаконных актов, разъясняющих некоторые технические аспекты защиты персональных данных. Однако эти документы не всегда учитывают существующие нормы по обеспечению безопасности информации в широком смысле. В частности, не все требования безопасности персональных данных взаимоувязаны с положениями о защите информации, предусмотренными ранее принятыми и действующими документами ФСТЭК и ФСБ.

Например, согласно документам ФСТЭК, автоматизированные системы управления средствами связи, осуществляющие обработку персональных данных, относятся к ключевым системам. Требования к обеспечению безопасности информации, предъявляемые к таким системам, установлены и национальным стандартом ГОСТ Р 52448-2005 «Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения». Ранее защита этих систем, как правило, осуществлялась по классу 1Г. Непонятно, какие требования, в конечном счете, должны предъявляться к подобным системам? Какие из разнородных требований более высокие? Также непонятно каким образом осуществлять классификацию подобных систем. Ведь не существует «чисто» информационных систем, только для обработки персональных данных. В используемых на практике системах могут обрабатываться:

- сведения, относящиеся к коммерческой тайне;
- персональные данные;
- сведения, составляющие служебную тайну, и др.

Новые документы вводят новые понятия, а предусмотренные ими условия не всегда учитывают уже действующие нормы. Например, при определении требований к классам информационных систем, обрабатывающих персональные данные, для ряда систем соответствующие параметры не установлены. Возникает проблема уточнения требований

мнение специалиста



Юрий ТАЧКОВ,
ведущий научный сотрудник Управления Центра безопасности связи ФСБ России

Персональные данные (ПД), защита которых должна обеспечиваться в соответствии с Федеральным законом «О персональных данных», относятся к информации, не содержащей сведений, составляющих государственную тайну. Поэтому для обеспечения безопасности ПД могут использоваться криптосредства, разработанные в соответствии с действующими требованиями. Тем самым хотелось бы развеять достаточно широко распространенный миф о необходимости использования для обеспечения безопасности ПД только специально разработанных для этой цели криптосредств. В ИСПДн можно использовать любое криптосредство, которое обеспечивает требуемый уровень криптографической защиты.

Уровень криптографической защиты ПД определяется в модели угроз, отражающей специфику обеспечения безопасности ПД с точки зрения возможных последствиях противоправных действий с ПД и возможностей потенциального нарушителя. Именно поэтому один из разработанных в соответствии с постановлением Правительства Российской Федерации от 17.11.2007 № 781 документов ФСБ России практически полностью посвящен методологии разработки модели угроз. Модель угроз должна учитывать также случай, когда одно и то же криптосредство в информационной системе используется как для обеспечения безопасности ПД, так и для защиты другой информации, не содержащей государственную тайну.

Операторам, которые не обрабатывают ПД в государственных интересах, но тем ни менее подпадают под действие Федерального закона «О персональных данных» советую в первую очередь изучать нормативную базу. Например, не требуется обеспечение конфиденциальности общедоступных и обезличенных ПД, и средства защиты, включая криптосредства, могут быть обоснованно заменены на организационные меры.

Предложение о декларировании и добровольной сертификации вызывает сомнение потому, что при такой оценке соответствия возможно создание иллюзии обеспечения безопасности ПД и возможность нарушения безопасности ПД в случае, если добровольную сертификацию осуществляет потенциальный нарушитель или он имеет доступ к материалам сертификационных испытаний.

В настоящее время готовятся новые редакции указанных выше документов ФСБ России, которые предполагается утвердить установленным порядком и зарегистрировать в Минюсте России. Замечания к действующим документам ФСБ России по ПД и предложения по их совершенствованию можно направить до 1.03.2009 по электронной почте: uvt4@mail.ru.

по защите персональных данных с уже используемыми в существующих информационных системах. Согласно ст. 5 Постановления Правительства РФ от 17.11.2007 № 781, «средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия». Получается, что в настоящее время отсутствуют средства защиты информации (СЗИ), которые формально можно применять для защиты персональных данных. Следовательно, остается открытым вопрос, как убедиться в том, что средства защиты действительно способны обеспечить требуемый уровень защиты персональных данных.

Институт декларирования

Государственные структуры и производители средств защиты информации уже не первый год проводят массированное устрашение обывателя. Со страниц специализированных (и не только) журналов не сходят заголовки типа «Волна киберпреступности захватила…», «Массовый взлом…», «Группа хакеров взломала сеть банка…». И вот свершилось... Сотрудники соответствующих служб начинают метаться в поисках панацеи, мучаясь вопросами: «Что выбрать?» и «Где гарантии?». Причем второй вопрос значительно сложнее первого.

К рекламе производителя потребитель относится, как правило, с большим подозрением. Что может гарантировать потенциальному клиенту, что предлагаемый продукт соответствует обещаниям его производителя. Остается надежда на государство – благо на эту сферу распространяются строгие требования лицензирования и сертификации. Но у государственных органов голова в первую очередь болит о соответствии продукта госстандартам, нормам и законам, что обеспечивает защиту государственных интересов. И если они начнут думать еще и о потребительских свойствах продуктов (что, кстати, оправданно), то сотрудники ФСТЭК и ФСБ России просто не смогут покидать своих рабочих мест.

Как тут не вспомнить о том, что закон говорит не о СЕРТИФИКАЦИИ продукции, а о ПОДТВЕРЖДЕНИИ соответствия. Закон «О техническом регулировании» предусматривает институт ДЕКЛАРИРОВАНИЯ заявленных функций безопасности. Следовательно, на данном этапе для определенного круга информационных систем, обрабатывающих персональные данные, главным становится не сертификат соответствия, а некая декларация производителя о том, что СЗИ соответствует установленным требованиям. Это хорошо сочетается с международными требованиями и выгодно потребителю.

Добровольная сертификация

Поиски ответа на вопрос, что делать, приводят к мысли о

создании независимой экспертизы средств защиты информации. Действующие законы это позволяют, а при решении такой задачи можно опираться на авторитет российских общественных организаций. Независимая экспертиза не будет конфронтационной существующим в стране системам сертификации. Напротив, лишь дополнит их в части оценки качества потребительских свойств СЗИ. И главное – путем проведения сравнительного анализа потребительских свойств однотипных продуктов даст потребителю возможность объективно оценивать и выбирать наиболее подходящие ему средств защиты. Естественно, в таком важном деле не должно быть анархии.

В целях эффективности и отражения запросов всех заинтересованных сторон независимая экспертиза должна придерживаться ряда основных принципов. Первый из них – добровольность. Проведение экспертизы возможно только при согласии производителя СЗИ на ее осуществление. Потребитель может и должен быть уведомлен об отказе производителя от экспертизы. Хотя добровольность экспертизы только на руку производителям, так как согласие на ее проведение – лишнее подтверждение качества предлагаемого продукта (по принципу «нам ли платного входа бояться»).

Другой не менее важный принцип – открытость. Любой потребитель и производитель вправе ознакомиться со всеми материалами экспертизы (методиками, составом экспертов, мнением каждого из них и результатами экспертизы), чтобы не возникло подозрений в подтасовке результатов. Конечно, должен быть соблюден паритет – все участники процесса экспертизы (заявители, потребители, производители и эксперты) имеют равные права при формировании программы и методики осуществления экспертизы. У нас демократия, в конце концов. По этой же причине обязательным условием является независимость – каждый эксперт имеет право на свое мнение при проведении экспертизы, которое может довести до потребителя любым удобным ему способом.

Еще один принцип – гарантированность, когда все действия по проведению экспертизы, ее независимости подтверждаются третьей стороной, которая несет ответственность перед потребителем. Важным гарантом качества результатов является осуществление контроля. Все результаты экспертизы должны иметь возможность проверки и подтверждения третьими независимыми экспертами (при соблюдении установленных процедур). И самое главное, это не противоречит закону. ■