Майшев В.В. Касается ли меня защита персональных данных? /Налоговый вестник Удмуртии. 2009. № 6 (8), С. 2.

Чем ближе 1 января 2010 года, тем больше руководителей разного уровня задаются этим вопросом. Действительно, тема специфическая и не каждый (даже квалифицированный специалист по защите информации) может сходу в ней разобраться, определиться с тем, что нужно сделать в оставшееся время.

История вопроса

Принятие Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» положило начало процессу систематизации работы с персональными данными (ПДн) — отдельной категории конфиденциальной информации. Цель закона — обеспечение защиты прав и свобод человека при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Закон определяет, какие сведения собственно являются ПДн, какие действия считаются их обработкой и кто такой оператор персональных данных и каковы его обязанности.

В соответствии с законом оператор при обработке ПДн обязан принимать необходимые организационные и технические меры. Причем, надо понимать, что одними организационными или только техническими мерами обеспечить защиту ПДн не удастся — нужен комплекс мероприятий.

Что делать?

По мнению представителей рынка информационной безопасности мероприятия по защите информационных процессов обработки Пдн являются технически сложными, требуют высокой квалификации исполнителей, специальных знаний, а также выделения значительных финансовых средств.

Для начала нужно разобраться, есть ли в вашей организации сведения, которые можно квалифицировать как ПДн, законным ли образом они у вас собираются, обрабатываются ли они с помощью систем автоматизации или без них, относится ли ваша организация к категории «оператор персональных данных», ну и уже после этого размышлять о построении системы обеспечения безопасности ПДн.

На первый взгляд, может показаться, что ПДн есть только у банков, страховых и транспортных компаний, операторов связи и госорганов, и поэтому закон касается только их.

Статья 85 Трудового кодекса Российской Федерации вводит понятие ПДн работника. Согласно другим статьям главы 14 ТК защита ПДн работника должна быть обеспечена работодателем за счет его средств.

Таким образом, с уверенностью можно говорить, что каждый работодатель (и большой, и малый) получает, хранит и обрабатывает ПДн своих работников. И, разумеется, он обязан обеспечить все требования законодательства о защите персональных данных.

Является ли работодатель оператором ПДн? Да, хотя и направлять предусмотренное законом уведомление в уполномоченный орган по защите прав субъектов ПДн не требуется, т.к. работника связывают с оператором трудовые отношения.

Важный момент — ПДн относятся к сведениям ограниченного доступа (конфиденциальная информация), организация и обеспечение защиты которых устанавливается и регламентируется государством. В отличие от служебной или коммерческой тайны персональные данные не обрабатываются сами по себе, а распределены по разным информационным системам — от почтовых адресных книг до информационных систем учета кадров, начисления заработной платы и многопользовательских баз данных по работе с клиентами.

Почему 1 января 2010 года? Именно эта дата является «временной точкой», к которой все информационные системы персональных данных (ИСПДн) должны быть приведены в соответствие с требованиями законодательства и в «полном объеме» будет организована контрольная деятельность государства.

Регуляторы

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) — уполномоченный орган по защите прав субъектов персональных данных, на который возлагается обеспечение контроля и надзора за обработкой ПДн.

Функции контроля и надзора за выполнением требований к обеспечению безопасности ПДн при их обработке в ИСПДн и технологиям хранения таких данных вне ИСПДн осуществляются Федеральной службой безопасности Российской Федерации (ФСБ России) и Федеральной службой по техническому и экспортному контролю (ФСТЭК России) в пределах их компетенции.

Легитимность обработки персональных данных

Для обработки ПДн необходимо основание. Для большинства организаций предусмотренные законом основания это:

— наличие закона, устанавливающего цель обработки, условия получения ПДн и круг субъектов, Пдн которых подлежат обработке;

— наличие согласия субъектов ПДн;

— наличие договора, одной из сторон которого является субъект ПДн.

Как правило, обработка Пдн в большинстве государственных информационных ресурсов предусмотрена соответствующими законами, обработка Пдн собственных работников прямо предусматривается главой 14 ТК, с физическими лицами - абонентами операторов связи и пассажирами имеются прямые договоры.

Сложнее определиться, когда существует договор между двумя юридическими лицами, но ничего не сказано о Пдн сотрудников/должностных лиц этих организаций, так или иначе используемых в рамках исполнения этих договоров. Еще сложнее, когда заходит разговор о передаче ПДн третьим лицам, например в банк, страховую компанию и т.п.

В этих и других случаях без письменного согласия субъекта (конкретного физического лица) обрабатывать и передавать его Пдн нельзя. Содержание этого согласия предусматривается ст. 9 закона, причем обязанность предоставить доказательство получения согласия субъекта на обработку его ПДн возлагается на оператора.

Технологии обработки персональных данных

Обработка ПДн, осуществляемая без использования средств автоматизации, безусловно, должна быть защищенной — это регламентируется Постановлением Правительства РФ от 15.09.2008 № 687. Среди особенностей можно отметить

требования к типовым формам документов, условия ведения журналов (реестров, книг), содержащих ПДн, необходимые для однократного пропуска на территорию оператора, или в иных аналогичных целях.

Но все же в наш информационный век практически любая обработка сведений производится в автоматизированном виде — в ИСПДн. Удобство и оперативность обработки информации в ИСПДн должны быть сбалансированы надежной защитой применяемых информационных технологий.

В этом случае, опираясь на нормативные документы регуляторов, нужно в оставшееся время провести «полномасштабные исследования» своей информационно-телекоммуникационной инфраструктуры и технологических процессов обработки информации, разработать модели угроз и классифицировать ИСПДн, выбрать и установить требуемые сертифицированные средства защиты информации, а также в некоторых случаях произвести аттестацию Вашей автоматизированной системы на предмет соответствия требованиям по защите информации.

О наказании

За неисполнение требований законодательства в области обработки ПДн операторы и их должностные лица могут быть привлечены к административной (ст. 13.11 — 13.14 КоАП), гражданско-правовой, уголовной (ст. 137 УК) и дисциплинарной (ст. 192 ТК) ответственности.