



**Михаил Емельяников**

директор по развитию бизнеса компании «Информзащита»

## Персональные данные в энергетической компании

**В**ы держите в руках извещение об оплате электроэнергетики. На нем указаны фамилия, имя и отчество абонента, его домашний адрес, сведения о расходе электроэнергии за определенный период и сумма к оплате. Но извещение — не только платежный документ. В терминах Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» это — бумажный носитель информации, относящейся к определенному или определяемому на ее основании физическому лицу. При этом энергосбытовая компания, выставившая счет, является оператором персональных данных, и на нее упомянутым законом возлагается целый ряд дополнительных обязанностей, связанных с правомочностью сбора и передачи сведений о гражданах, в том числе третьим лицам, принятием мер безопасности при обработке данных в информационных системах, а также предоставлением субъектам персональных данных возможности ознакомления с ними. К мероприятиям, требующим согласия абонентов, относится и передача функций тарификации услуг, доставки счетов и технического обслуживания электросетей, принадлежащих физическим лицам, каким-либо сторонним компаниям.

Любая энергосбытовая организация имеет дело с персональными данными не только абонентов, но еще нескольких категорий граждан, причем для каждой из этих групп существуют свои особенности, предусмотренные законом.

Так, организуя обработку инфор-

мации о персонале, как имеющейся в виде бумажных документов (личные дела, трудовые книжки, заявления, приказы по личному составу и т. п.), так и в электронном виде (автоматизированные системы бухгалтерского и кадрового учета), работодатель в соответствии со ст. 86 Трудового кодекса РФ обязан составить и принять документы, устанавливающие порядок действий в отношении персональных данных, и довести этот порядок до сведения всех сотрудников. Защита личной информации от неправомерного использования или утраты должна быть обеспечена работодателем за счет его средств. На передачу персональных данных третьим лицам — например в случаях командировки сотрудника в другие организации, при бронировании мест в гостиницах или приобретении проездных документов и даже в процессе реализации мероприятий социальной защиты (таких как добровольное медицинское или пенсионное страхование) — требуется согласие работника.

Между тем размещение биографических и иных сведений о менеджерах компании (персональных данных, идентифицирующих личность и позволяющих получить о ней дополнительную информацию) с их фотографиями (биометрическими персональными данными) на веб-сайте компании является переводом персональных данных в категорию общедоступных, на что необходимо специально составленное письменное согласие субъекта, в соответствии с ФЗ № 152 содержащее:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта;
- цель обработки персональных данных;
- перечень сведений, на обработку которых дается согласие субъекта;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки такой информации;
- срок, в течение которого действует согласие, а также порядок его отзыва.

Особую сложность представляет вопрос обработки персональных данных о сотрудниках контрагентов энергетических компаний — партнеров, клиентов из числа юридических лиц, ремонтных организаций, органов контроля и надзора и т. п. В соответствии с вышеупомянутым законом персональные данные можно получать только у самого субъекта. В случаях же, когда сведения получены не от гражданина, а, например, от его работодателя, оператор до начала обработки обязан сообщить субъекту следующую информацию:

- наименование (фамилию, имя, отчество) и адрес оператора или его представителя;

- цель обработки персональных данных и ее правовое основание;
- сведения о предполагаемых пользователях;
- установленные ФЗ № 152 права субъекта персональных данных.


Поэтому уже на этапе заключения договора с контрагентом целесообразно предусмотреть возложение на него проблем получения согласия работника на передачу персональных данных и гарантирования их достоверности. Это потребует и отражения в договоре в качестве существенного условия принятия мер по обеспечению конфиденциальности обработки информации принимающей стороной.

Достаточно сложным вопросом с точки зрения безопасности обработки персональных данных является организация деятельности call-центров и иных подразделений, обслуживающих клиентов по телефону. Большинство контактных центров ведет запись телефонных переговоров, о чем оператор предупреждает звонящих перед началом разговора. При этом клиент для получения услуг идентифицируется — указывает фамилию, имя, отчество, место жительства, номер лицевого (абонентского) счета, то есть опять-таки свои персональные данные. С позиций ФЗ № 152 call-центр — это самостоятельная информационная система, обрабатывающая персональные данные, помимо прочего и в виде речевого сигнала, и использующая средства передачи (телефон), звукозаписи, хранения и звуковоспроизведения. На такую организацию в полном объеме распространяются требования о защите сведений, при этом к мерам безопасности компьютерных сетей добавляются действия по защите речевой информации.

Ввиду ограниченности формата журнальной публикации нет возможности подробнее остановиться на правилах выполнения требований государственных регуляторов о технической защите персональных данных в информационных системах. Необходимо лишь отметить, что исходя из порядка классификации ИСПДн, определенного совместным приказом ФСБ, ФСТЭК и Минсвязи РФ от 13.02.2008 г. № 55/86/20, практически все крупные энергосбытовые компании страны эксплуатируют информационные

системы персональных данных 1-го класса, поскольку каждая из них обслуживает более 100 тыс. клиентов — физических лиц — и имеет соответствующее количество записей о субъектах в базах, а сами персональные данные позволяют получить о клиенте дополнительные сведения (об оказанных услугах, установленном учетном оборудовании, состоянии оплаты счетов и др.). Наличие системы 1-го класса означает применение сертифицированных средств защиты информации, обеспечивающих предотвращение несанкционированного доступа к персональным данным, межсетевое экранирование, антивирусную защиту, своевременное обнаружение атак, шифрование сведений при передаче их по общедоступным каналам связи (сети Интернет в том числе), а также необходимость аттестации такой информационной системы в соответствии с требованиями безопасности. Сама же энергетическая компания, эксплуатирующая ИСПДн 1-го или 2-го класса, должна иметь лицензию ФСТЭК на техническую защиту конфиденциальной информации, а при использовании средств шифрования, обязательных для территориально распределенной системы, — и комплект лицензий ФСБ на работу с этими средствами.

Невыполнение изложенных требований создает для энергетиков, как и для других предприятий и организаций, существенные риски, связанные с санкциями государственных регуляторов и с исками граждан, посчитавших свои права нарушенными в результате раскрытия личной информации из-за бездействия энергосбытовой компании в части защиты персональных данных. Созданная в стране специализированная система контроля и надзора включает в себя, помимо профильных подразделений ФСБ и ФСТЭК, уполномоченный орган по защите прав субъектов персональных данных — Роскомнадзор, который уже сейчас активно проводит как плановые, так и внеплановые (по жалобам граждан) проверки компаний, работающих с персональными данными.

А до 1 января 2010 г. — срока, определенного Федеральным законом № 152 для окончательного приведения порядка обработки персональных данных в соответствие с установленными требованиями, — осталось совсем немного времени. 



**Код безопасности**  
ГК «Информзащита»

## Защита персональных данных

### Security Studio

защита типовых систем обработки персональных данных

### Secret Net

Защита информации от несанкционированного доступа

### АПКШ «Континент»

защита информационных сетей компании и безопасное взаимодействие между ними

«Персональные данные — любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу...»

(из Статьи 3, ФЗ-№152 «О персональных данных» от 26.07.2006)

«Оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства, для защиты персональных данных...»

(из Статьи 3, ФЗ-№152 «О персональных данных» от 26.07.2006)



**Информзащита**  
Группа компаний

[www.infosec.ru](http://www.infosec.ru)

реклама