

Особенности защиты персональных данных в телекоммуникационных компаниях



В информационных системах компаний-операторов связи обрабатываются как персональные данные (ПДн) собственных сотрудников (возможно так же – акционеров-физических лиц), так и персональные данные абонентов.

Правовым основанием обработки ПДн в первом случае является трудовое законодательство Российской Федерации (включая Трудовой кодекс и Постановление Госкомстата РФ от 5 января 2004 г. № 1 «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты»), а так же, в ряде случаев – законодательство об акционерных обществах (Федеральный закон «Об акционерных обществах» от 26.12.1995 г. № 208-ФЗ).

Персональные данные абонентов обрабатываются в телекоме на основании Федерального закона «О связи» от 07.07.2003 г. № 126-ФЗ, статья 53 которого устанавливает возможность сбора и обработки сведений об абонентах и оказываемых им услугах связи, т. е. такой информации, как фамилия, имя, отчество или псевдоним абонента-гражданина, адрес абонента или адрес установки оконечного оборудования, абонентские номера и другие данные, позволяющие идентифицировать абонента или его оконечное оборудование, сведения баз данных систем расчета за оказанные услуги связи, в том числе о соединениях, трафике и платежах абонента.

Реализуя требования законодательства в области защиты персональных данных в отношении телекоммуникационных операторов, необходимо учитывать ряд особенностей.

Как правило, телекоммуникационные компании располагают системами, характеризующимися большим количеством субъектов персональных данных, персональные данные которых обрабатываются в информационной системе (определение параметра $X_{\text{нлд}}$ из Приказа ФСТЭК, ФСБ РФ и Мининформсвязи РФ от 13 февраля 2008 г. № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных», известного как т. н. «приказ трех»). Кроме того, такие информационные системы зачастую являются технологической основой производственной деятельности компании-оператора связи. Среди характерных примеров информационных систем персо-

нальных данных (ИСПДн) в телекоме можно назвать такие OSS/BSS, как биллинг (учет оказываемых услуг, тарификация, платежи и т. п.), системы CRM (управление взаимодействием с клиентами), OMS (управление заказами), системы активации услуг, а так же системы информационно-справочного обслуживания. Это сказывается на предъявлении дополнительных требований к системе защиты персональных данных (СЗПДн), которая, с одной стороны, должна соответствовать уровню угроз и масштабу ИСПДн, с другой стороны – не должна снижать производительность ключевых информационных систем телекоммуникационной компании.

Специфика организации обработки персональных данных в телекоммуникационной отрасли заключается так же в том, что в соответствии с ФЗ-152 «О персональных данных» не требуется согласие субъекта ПДн на обработку его персональных данных, если обработка ПДн необходима для осуществления операторами электросвязи расчетов с пользователями услуг связи за оказанные услуги связи, а также для рассмотрения претензий пользователей услугами связи. Этот фактор позволяет оптимизировать некоторые организационные процессы защиты персональных данных и упростить взаиморасчеты между операторами связи.

Следует отметить, что в большинстве случаев состав угроз информационной безопасности и взгляды руководства компании-оператора связи требуют создания более широкого поля сервисов безопасности, нежели это предусмотрено руководящими и методическими документами уполномоченных федеральных органов исполнительной власти. В таких случаях осуществляется разработка системы защиты персональных данных в составе более масштабной комплексной системы обеспечения информационной безопасности (СОИБ), реализующей дополнительные требования по обеспечению защиты информации, в т. ч. – по противодействию мошенничеству на сетях связи. Объединение в одном проекте СЗПДн и комплексной СОИБ позволяет более рационально осуществлять инвестиции в информационную безопасность. Кроме того, с целью повышения ARPU одновременно могут быть проведены и работы по развертыванию дополнительных видов обслуживания – услуг в области информационной безопасности, предоставляемых абонентам.



107023,
Россия, Москва
ул. Семеновская Б., 45
Тел.: +7 (495) 730-74-88
Факс: +7 (495) 580-51-15
info@inforion.ru
www.inforion.ru