

Пояснительная записка

Первого января 2010 года вступит в силу п. 3 статьи 25 Федерального закона «О персональных данных», в соответствии с которым операторы персональных данных (ПДн) обязаны привести информационные системы персональных данных (ИСПДн) созданные до января 2007 года в соответствие с требованиями закона.

Для формирования общих подходов и подготовки нормативно-методической базы для выполнения требований законодательства РФ по защите ПДн в ИСПДн операторов связи (ОС), в рамках Союза участников рынка инфокоммуникационных услуг (ИСУ), в настоящее время реализуется Проект «Разработка концепции защиты персональных данных в информационных системах персональных данных операторов связи» (шифр «Тритон»). В состав рабочей группы проекта входят представители крупнейших операторов сотовой связи (МТС, ВымпелКом, Мегафон), Главным Исполнителем работ является компания ReignVox.

Мы заинтересованы в реальной защите персональных данных субъектов. Имеем многолетний и успешный опыт защиты информации применительно к нашим предприятиям, многочисленным партнёрам и клиентам. Однако, практика выполнения требований по защите ПДн показала, что имеются правовые, финансовые, организационные, методические и технологические проблемы системного характера. В условиях объявленного руководством государства курса на ускоренное развитие инновационных отраслей экономики и интеграцию в мировое сообщество, существующее законодательство в области персональных данных требует качественной корректировки, чтобы не оказаться сдерживающим фактором.

В качестве основных трудностей следует отметить:

- противоречивость положений закона и подзаконных актов, а также отсутствие согласованности с другими разделами законодательства, недостаточная регламентация отдельных правовых вопросов, возникающих в отношении субъекта ПДн и оператора;

- требования по защите ПДн не учитывают риски безопасности, объемы и природу обрабатываемых ПДн, используемых информационных технологий, адекватную стоимость защитных мероприятий, отраслевую специфику операторов связи и провайдеров Интернет-услуг, особенности информационных отношений в негосударственной сфере. В ряде случаев содержат избыточные требования, которые характерны для защиты государственной тайны;

- методические документы, содержащие требования по защите ПДн выпущены только весной 2008 года, и в настоящее время происходит переработка требований во ФСТЭК и ФСБ.

- существующие требования по сертификации (аттестации) средств защиты информации и информационных систем не позволяют адекватно решать задачи по защите ПДн при существующих технологиях обработки и передачи информации современных операторов связи.

- отсутствуют объективные критерии для оценки достаточности уровня защиты ПДн. Меры по защите ПДн для специальных (не типовых) ИСПДн определяют сами операторы ПДн на основании методических документов. Достаточность принятых мер по обеспечению безопасности ПДн при их обработке в информационных системах оценивается при проведении государственного контроля и надзора. Однако однозначных критериев выбора требований нет.

С учетом изложенного, возможно говорить о проблемах выполнения требований регуляторов как в части порядка обработки персональных данных, так и требований по технической защите персональных данных.

Возможные меры:

1. Выполнение НИР по разработке общих, специальных (для конкретных технологий и систем) и отраслевых нормативных и методических документов по защите ПДн в ИСПДн операторов ПДн, в том числе, профилей защиты ПДн. Утверждение отраслевых стандартов с учетом адекватности защиты и специфики отраслей.

2. Рассмотреть возможность изменения порядка и сути проверок на соответствие требованиям закона. Начиная с 2010 года проводить проверки в тестовом режиме, собирая данные и реальные примеры использования защитных механизмов, как уже внедренных операторами ПДн, так и планируемых к внедрению на основе анализа угроз и моделей нарушителей, без применения в 2010 году карающих санкций, предусмотренных сейчас законом. Это позволит на основе собранной информации оптимизировать отраслевые профили защиты с учетом практики применения и новых требований (ГОСТы, переработанные требования ФСТЭК и ФСБ).

3. Разработать и опубликовать административный регламент по контролю соответствия ИСПДн требованиям безопасности представителями Регуляторов. Публикация методики контроля уменьшает регуляторные риски и позволяет Оператору ПДн перед процедурой контроля регулятором проверить свои ИСПДн на соответствие ожидаемым результатам. Результаты внутренней проверки, возможно заблаговременно посылать Регулятору для оценки. Такая процедура в результате упростит проведение контрольных операции со стороны регуляторов, позволит экономить ресурсы.

4. Организация совместной работы профильных научных организаций и консультантов, общественных организаций, представляющих операторов ПДн различных отраслей, ФСБ и ФСТЭК РФ, под общим руководством Минкомсвязи России, в целях получения научно-обоснованной методической базы для согласованного внесения изменений в законодательство, подзаконные акты и методические документы, разработки системных требований по организации обработки и обеспечению безопасности ПДн в РФ. Изменение законодательства, нормативной и методической базы в соответствии с результатами совместной работы.

Мы убеждены, что только совместными усилиями Минкомсвязи России, ФСТЭК России, ФСБ России и операторов ПДн можно обеспечить системное решение проблем законодательства и выполнения требований по обеспечению безопасности ПДн в информационных системах, сетях и системах связи.

В приложении представлены развернутые комментарии и Предложения по гармонизации нормативной правовой базы по защите персональных данных (Приложение: на 5 л. в 1 экз.)