**Организация обработки и защиты персональных данных**

**в малых организациях**

Автор Картамышев А.В.

Источник: журнал "Information Security/ Информационная безопасность"№6, 2008.

В связи с приближением даты приведения в соответствие с требованиями действующего законодательства информационных систем персональных данных, указанной в ФЗ № 152-ФЗ "О персональных данных", перед операторами встает вопрос порядка их действий по выполнению этих требований.

В крупных организациях, имеющих в своем составе службы администрирования ЛВС, безопасности информации, сопровождения баз данных, а также юридическую службу, вопросами защиты персональных данных, как правило, занимаются довольно давно и плотно. В малых же организациях, в которых нет таких подразделений (их функции выполняют либо приходящие специалисты, либо "продвинутые" родственники или знакомые), в лучшем случае о появлении законодательства о персональных данных только слышали. К последним можно отнести школы, отделы администрации, малые предприятия и многие другие. Бюджеты данных организаций сильно ограничены, и появление еще одной статьи расходов - это кошмарный сон руководителя.

В рамках данной статьи мы попытаемся определить, какие действия должен предпринять руководитель такой организации, чтобы с минимальными финансовыми затратами выполнить требования законодательства по вопросам персональных данных.

**Наличие персональных данных**

Для начала необходимо определить, имеются ли в организации персональные данные, их объем и где они содержатся. В этом помогут ФЗ № 152-ФЗ "О персональных данных" и Трудовой кодекс, которые определяют, что такое персональные данные и их обработка. Объем персональных данных имеет две составляющие: перечень идентификаторов (полей в форме) о субъекте персональных данных и количество субъектов. Персональные данные могут обрабатываться как с использованием средств автоматизации (например, СУБД "1С: Зарплата", установленная на ПЭВМ), так и без использования таких средств (например, на бумаге). В первом случае необходимо выполнять требования постановления Правительства РФ № 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных", во втором - требования постановления Правительства РФ № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации".

**Необходимость обработки персональных данных**

Следующий шаг - важно определить необходимость обработки этих данных и правовое основание на их обработку. Дело в том, что объем персональных данных непосредственно влияет на требования к системе их защиты и соответственно на общую стоимость всех мероприятий, поэтому чем меньше обрабатывается данных, тем меньше будут затраты на их защиту. Правовым основанием обработки персональных данных можно считать перечень соответствующих виду деятельности кодов ОКВЭД в свидетельстве о государственной регистрации юридического лица (индивидуального предпринимателя) и, как следствие, законы и нормативные акты, регламентирующие заявленный вид деятельности. Стоит обратить внимание, что к разделу 72 ОКВЭД можно отнести обработку персональных данных средствами вычислительной техники, например, СУБД "1С: Зарплата" или "Парус". В случае отсутствия соответствующих статей в учредительных документах имеет смысл провести работу по их добавлению.

**Сбор данных и определение необходимости отправки уведомления**

Затем необходимо собрать исходные данные, перечень которых можно взять из приказа ФСТЭК России, ФСБ России, Мининформсвязи России № 55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных".

После всего вышеперечисленного нужно проанализировать статью 22 ФЗ № 152-ФЗ и определить необходимость отправки уведомления о намерении обработки персональных данных в территориальный орган Россвязькомнадзора. Форму уведомления и адреса территориальных органов можно найти на сайте Федеральной службы по надзору в сфере связи и массовых коммуникаций по адресу http://www.rsoc.ru/main/di-rections/874/

**Документация**

Далее необходимо создать внутреннюю документацию организации, регламентирующую обработку персональных данных. Ее условно можно разделить на две части: общая документация и документация по защите персональных данных.

В первую группу должны войти: положение о персональных данных и общий технологический регламент их обработки. В первом документе необходимо отразить следующие вопросы:

* цели обработки персональных данных;
* круг субъектов, персональные данные которых подлежат обработке;
* состав персональных данных, необходимый для обработки;
* источники получения персональных данных;
* сроки хранения и сроки обработки;
* способы обработки персональных данных;
* маркировка и учет персональных данных;
* требования к персоналу;
* порядок взаимодействия с владельцем персональных данных;
* юридические последствия, возникающие при нарушении конфиденциальности персональных данных;
* сроки реагирования на обращения субъектов персональных данных;
* определение технических и программных средств обработки персональных данных;
* порядок защиты персональных данных;
* порядок контроля над соблюдением требований по обращению и защите персональных данных;
* требования к внутренней документации;
* должностные инструкции персонала, допущенного к обработке персональных данных.

Общий технологический регламент обработки персональных данных должен содержать описание технологического процесса обращения с персональными данными на всех этапах жизненного цикла без учета средств защиты информации:

* порядок приема должностными лицами персональных данных, внесения их в базу данных, обработки, хранения, дополнения, исправления, передачи, обезличивания, уничтожения; время и сроки выполнения всех операций;
* порядок взаимодействия с субъектом персональных данных (получение согласия на обработку, реагирование на запросы, предоставление собранной информации, уведомление о передаче, уничтожении);
* типовые формы документов (запросы, оповещения, разрешения и т.п.);
* порядок обращения с носителями информации: учета, хранения, присвоения и изменения класса персональных данных, передачи, приема, уничтожения, перевода в другой вид (например, распечатка электронного документа);
* порядок обращения с электронными и распечатанными носителями персональных данных при чрезвычайных ситуациях (наводнение, пожар, пропадание электропитания, теракт, вооруженное нападение, неадекватные действия клиентов, действия вирусов (атаки), отказы оборудования, переезды, нестыковки ключевой документации, введение военного положения);
* порядок обращения с электронными носителями персональных данных, средствами автоматизации, их содержащими, при техническом обслуживании и ремонте.

За разработкой документации по защите персональных данных рекомендуется обратиться к организациям, имеющим лицензии ФСТЭК и ФСБ России на деятельность по технической защите конфиденциальной информации.

**Выполнение требований**

Затем необходимо определиться и выполнить требования по инженерной защите объекта, на котором обрабатываются персональные данные в соответствии с требованиями постановления Правительства РФ № 687. Кроме того, рекомендуется привести в соответствие с требованиями пожарную и охранную сигнализацию.

Следующим шагом является выполнение требований руководящих документов ФСТЭК и ФСБ России по защите персональных данных. Данный вид деятельности является лицензируемым, и для его выполнения требуется привлекать организации, имеющие лицензии на деятельность по технической защите конфиденциальной информации. На этом же этапе необходимо разработать специальный технологический регламент, который должен включать все вопросы общего с наложенными требованиями, предъявляемыми системой защиты информации.

Далее необходимо организовать повышение квалификации сотрудников и их осведомленности в области защиты персональных данных.

Ссылка на статью: <http://www.itsec.ru/articles2/pravo/organizaciya-obrabotki-i-zaschiti-personalnih-dannih-v-malih-organizaciyah/>