УДК 004.056

С.К. Варлатая, А.В. Белёв, С.В. Ширяев

Алгоритм создания и введения в эксплуатацию информационных систем персональных данных

Представлен материал, описывающий практическую реализацию осуществления организационного обеспечения защиты в информационных системах персональных данных. Описан алгоритм реализации защиты информационных систем персональных данных. Разработан комплекс организационных мер.

Ключевые слова: информационная система, персональные данные, комплекс мероприятий.

Проектирование системы защиты персональных данных (ПД) заключается в том, чтобы создать оптимальную совокупность механизмов обеспечения защиты информации и механизмов управления ими. Оптимальность системы, т.е. достижение заданного уровня защищенности при минимальных затратах, определяется характером персональных данных, условиями обработки и хранения и возможностями злоумышленника.

Проблема установления между эффективностью и безопасностью рационального баланса – это главная задача. Надо отметить, что для организации важно и опасно, когда деятельность сотрудников, вне зависимости от их намерения, увеличивает степень риска.

Информационная система персональных данных (ИСПДн) обеспечивает передачу информации за пределы предприятия через закрытые каналы передачи данных. Осуществляются основные сетевые протоколы, включаются веб-трафик, поисковые запросы, корпоративная почта, организуется доступ пользователей корпоративной сети к интернет-ресурсам [3]. Для того, чтобы в таком потоке информации сохранить ее целостность и избежать утечки, необходимо создать защищенную информационную систему и для ввода ее в эксплуатацию необходимо осуществить следующий алгоритм основных действий (рис. 1).

В организации приказом руководителя назначаются ответственные лица за обеспечение безопасности ПД. После этого проводится комплексное обследование информационной системы (баз данных), содержащей сведения, относящиеся к персональным данным [1].

Далее проводится классификация информационных систем персональных данных, которая включает в себя следующие этапы: сбор и анализ исходных данных по информационной системе персональных данных; присвоение информационной системе персональных данных соответствующего класса и его документальное оформление.

В зависимости от состава персональных данных определяется категория, к которой относится та или иная информационная система персональных данных.

Порядок проведения классификации информационных систем персональных данных (ИСПДн) утвержден приказом Федеральной службы по техническому и экспортному контролю, ФСБ РФ и Министерства информационных технологий и связи РФ от 13 февраля 2008 г. № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных».

От класса ИСПДн зависит, какие требования по обеспечению безопасности персональных данных должны выполняться в данной информационной системе.

Оформление Акта классификации информационной системы персональных данных осуществляется на основе постановления [2], согласно п. 6 которого информационные системы классифицируются государственными органами, муниципальными органами, юридическими или физическими лицами, организующими и (или) осуществляющими обработку персональных данных, а также определяющими цели и содержание обработки персональных данных, в зависимости от объема обрабатываемых ими персональных данных и угроз безопасности жизненно важным интересам личности, общества и государства.

В Управление федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций Роскомнадзор направляется уведомление об обработке (намерении осуществлять обработку) ПДн.

Рис. 1. Алгоритм введения в эксплуатацию информационной системы защиты персональных данных

Классификация информационной системы персональных данных

Категория ПДн	Объем ПДн (субъектов ПДн)		
	До 1000	1000–100000	Более 100000
4	К4	К4	К4
3	К3	К3	К2
2	К3	К2	К1
1	К1	К1	К1

Оператор обязан (за исключением случаев, указанных в ст. 22 Федерального закона № 152-ФЗ «О персональных данных») уведомить Роскомнадзор об обработке персональных данных. Образец формы уведомления об обработке (намерении осуществлять обработку) персональных данных, а также рекомендации по его заполнению утверждены приказом Роскомнадзора № 8 от 17.07.2008 г. с изменениями, внесенными приказом Роскомнадзора № 42 от 18.02.2009 г.

Комплекс мероприятий по обеспечению защиты персональных данных состоит из организационных и технических мер защиты информации. Организационные меры по защите персональных данных включают в себя разработку организационно-распорядительных документов, которые регламентируют процесс обработки персональных данных (сбор, систематизацию, накопление, хранение). Примерный перечень организационно-распорядительных документов:

- положение об обработке персональных данных;
- положение о защите персональных данных;
- положение о подразделении по защите информации;
- должностные регламенты лиц, ответственных за защиту ПДн;
- план мероприятий по защите ПДн;
- план внутренних проверок состояния защиты ПДн;
- приказы о назначении ответственных лиц по ПДн;
- копия уведомления РКН с исходящим номером и датой подписания;
- типовая форма и письменные согласия субъекта ПДн на обработку ПДн;
- список лиц, обрабатывающих ПДн, утверждённый оператором или уполномоченным лицом;
- инструкции администраторов безопасности персональных данных;
- инструкции пользователей по работе с персональными данными;
- журнал по учету мероприятий по контролю;
- журнал учёта обращений субъектов ПДн;
- журнал обращений пользователей информационной системы к ПДн;
- журналы (книги) учёта ПДн;
- правила пользования средствами защиты информации;
- эксплуатационная и техническая документация;
- отражение в трудовом договоре (контракте) ответственности работника за разглашение ПДн;
- иные документы.

В каждой организации перечень мероприятий и документов может варьироваться в зависимости от специфики обработки ПДн, организационной структуры и других особенностей конкретной организации. Реализация организационных мер защиты информации осуществляется с учетом категорий персональных данных.

Определение методов и способов защиты информации в ИСПДн, а также внедрение средств защиты осуществляется на основе приказа Федеральной службы по техническому и экспортному контролю от 05 февраля 2010 г. № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных».

После вышеуказанных мероприятий производится ознакомление под роспись персонала с утвержденными инструкциями и правилами обеспечения безопасности персональных данных в подразделении.

В заключение необходимо осуществлять постоянный контроль за выполнением сотрудниками подразделения требований обеспечения безопасности персональных данных согласно нормативно-правовым документам и собственным инструкциям.

Литература

1. Приказ Федеральной службы по техническому и экспортному контролю, ФСБ РФ, Министерства информационных технологий и связи РФ от 13.02.2008 г. № 55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных» [Электронный ресурс]. – Режим доступа: http://itsec.ru/articles2/inf_security/porjadok-klassifikatsii-personalnyh-dannyh, свободный (дата обращения: 3.08.2011).

2. Постановление Правительства Российской Федерации от 17.11.2007 г. № 781, г. Москва, «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс]. – http://www.rg.ru/2007/11/21/personalnie-dannye-dok.html (дата обращения: 2.08.2011).

3. Мещеряков Р.В. Комплексное обеспечение информационной безопасности автоматизированных систем / Р.В. Мещеряков, А.А. Шелупанов. – Томск: В-Спектр, 2007. – 350 с.

Варлатая Светлана Клементьевна
Канд. техн. наук, профессор каф. информационной безопасности Дальневосточного федерального университета (ДВФУ)
Тел.: +7-924-244-40-33
Эл. почта: sk-varl@yandex.ru

Белёв Александр Викторович
Аспирант каф. информационной безопасности ДВФУ, начальник управления защиты государственной тайны и информационной безопасности Приморского края
Тел.: +7-914-703-52-26
Эл. почта: belev_av@primorsky.ru

Ширяев Сергей Вячеславович
Аспирант каф. информационной безопасности ДВФУ
Тел.: +7-921-447-71-08
Эл. почта: ssv.pda@gmail.com

Varlataya S.K., Belev A.V., Shiryaev S.V.
Algorithm of development and usage of the personal data information systems

The article presents material that describes the practical implementation of institutional protection of personal data information systems. The algorithm of the implementation of the protection of personal data information systems is described. The complex of organizational measures is developed.
Keywords: information system, personal data, action plan.