УДК 347

К ВОПРОСУ О ПРАВОВОМ РЕГУЛИРОВАНИИ РАБОТЫ С ИНФОРМАЦИОННЫМИ СИСТЕМАМИ ПЕРСОНАЛЬНЫХ ДАННЫХ

М. А. Лапшова

Очень важно грамотно подходить к созданию защищённой информационной системы, которая обрабатывает персональные данные. В настоящее время сложно представить себе организацию, которой бы не пришлось работать с ними. Для обеспечения безопасности персональных данных при их обработке в информационных системах, необходимы как организационные, так и технические меры защиты. Базовый набор этих мер определяется, исходя из уровня защищённости персональных данных, который необходимо обеспечить. В данной работе приведён план анализа информационной системы персональных данных с целью определения необходимого уровня её защищённости на основании характеристик этой системы. Также рассмотрены возможные способы обеспечения информационной безопасности.

Ключевые слова: система безопасности, уровни защищённости, тип угроз безопасности, сертифицирование, средства защиты информаци.

В настоящее время сложно представить себе организацию, которой бы не пришлось работать с персональными данными. Фамилии, имена, ИНН, СНИЛС предоставляются сейчас практически везде. Куда бы Вы ни обратились, вероятнее всего, Вас попросят предъявить паспорт. Поэтому крайне важно грамотно подойти к созданию защищённой информационной системы, которая обрабатывает персональные данные. Отношения, которые связаны с обработкой персональных данных, регулируются Федеральным законом Российской Федерации № 152-ФЗ «О персональных данных» [1].

Также не стоит забывать и о персональных данных сотрудников организации, работа с которыми ведётся постоянно и в большом объёме, особенно в отделе кадров и в бухгалтерии. В этом случае необходимо руководствоваться Трудовым Кодексом Российской Федерации, главой 14 [2].

При проектировании системы безопасности первым действием должно быть назначено ответственное лицо и выпущен соответствующий приказ о назначении. Далее устанавливается, какие данные, и в каком объёме будут обрабатываться в информационной системе. Это нужно для того, чтобы определить круг лиц, которым необходимо предоставить доступ к персональным данным, а также, чтобы составить и утвердить модель нарушителя и модель угроз.

Для обеспечения безопасности персональных данных при их обработке в информационных системах необходимы как организационные, так и технические меры защиты. Базовый набор этих мер определяется, исходя из уровня защищённости персональных данных, который необходимо обеспечить [3]. Всего выделяется четыре уровня, четвёртый – наиболее слабый.

Для определения необходимого уровня защищённости персональных данных нужно знать тип актуальных угроз безопасности персональных данных, какие категории данных обрабатывает информационная система (общедоступные, специальные, биометрические или иные персональные данные), а также количество субъектов персональных данных, не являющихся сотрудниками оператора (более или менее 100 000 субъектов). Зная эти данные, по Постановлению Правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» определяется необходимый уровень защищённости (пункты 9–12 Постановления Правительства РФ № 1119).

Лапшова Марина Александровна,
(lapshova.marina.smr@gmail.com),
студент V курса факультета информатики
Самарского университета,
443086, Россия, г. Самара, Московское шоссе, 34.

Чтобы узнать тип актуальных угроз, обратимся к пунктам 6–7 Постановления Правительства РФ № 1119. Всего классифицируют три типа угроз. Они отличаются наличием недекларированных возможностей в системном или прикладном программном обеспечении.

В приложении к Составу и содержанию организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных подробно описаны меры, которые необходимо осуществить для каждого уровня защищённости. Также помимо минимальных требований для большей надежности можно дополнять защиту другими мерами, которые не предусмотрены базовым списком.

Для всех уровней защищённости к информационным системам, обрабатывающим персональные данные, необходимо ограничить физический доступ. Для этого рекомендуется устанавливать двери с замками, решётки на окнах, постоянную охрану, а также ввести пропускной режим.

Главное требование по выбору средств защиты информации – это наличие сертификата. Только при этом условии возможна правомерная работа с персональными данными. В открытом доступе можно получить перечень средств защиты информации, которые были сертифицированы.

Также следует обратить внимание на стоимость средств и набор возможных способов защиты в одном комплексе. Зачастую использование более дорогого составного программного обеспечения выгоднее, чем покупка отдельных модулей. Ещё одно преимущество покупки комплекса программно-аппаратных средств защиты – это отсутствие проблем с совместимостью его частей.

Практически все меры по обеспечению безопасности персональных данных, относящиеся к программно-аппаратному обеспечению, можно осуществлять с помощью Secret Net. Это сертифицированное средство защиты, которое может работать как с операционной системой Windows, так и с Linux/GNU. Этот комплекс широко распространён, так как очень удобен в использовании. Многие проблемы, связанные с защитой персональных данных, решаются покупкой одного такого средства защиты.

Также комплекс некоторых мер из списка можно проводить с помощью аппаратно-программного модуля «Соболь», который тоже сертифицирован.

Антивирусная защита должна быть организованна, независимо от уровня защищённости данных. Сертифицированные средства, которые можно применять при работе с персональными данными: Kaspersky Endpoint Security, Dr. Web Desktop Security Suite, ESET NOD32 SECURE Enterprise newsale.

Межсетевой экран (например, Check-Point) обеспечит безопасный доступ к сети Internet. Он контролирует и фильтрует все пакеты, как входящие в сеть, так и исходящие из неё, по заданным правилам. Check-Point также прошел процедуру сертифицирования. Возможности межсетевого экрана есть и в Secret Net.

Для первого и второго уровня защищённости необходимо вести учёт носителей персональных данных, а также управлять доступом к ним. Для этого используются организационные меры, такие как создание и ведение журнала учёта носителей персональных данных, а также программное обеспечение для ограничения доступа. Съёмные носители следует хранить в сейфе или металлическом ящике. Также следует предусмотреть периодическое резервное копирование персональных данных на резервные носители.

Таким образом, для достижения цели необходимо назначить ответственное лицо, определить необходимый уровень защищённости персональных данных, выбрать средства защиты информации и подготовить соответствующий пакет документов.

Защита персональных данных – это одна из наиболее важных задач в современном мире. Каждый человек хочет, чтобы его личные данные были в безопасности и обрабатывались только в действительно необходимых случаях. Поэтому государство уделяет особое внимание созданию законодательства в сфере информационной безопасности, которое регламентирует проектирование надлежащим образом защищённых информационных систем персональных данных, а также поддерживает их в безопасности.

Литература

1. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 21.07.2014) «О персональных данных» [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

2. Трудовой кодекс РФ от 30.12.2001 № 197-ФЗ (ред. от 03.07.2016) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

3. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

ON THE ISSUE OF LEGAL REGULATION OF USING INFORMATION SYSTEM OF PERSONAL DATA

M. A. Lapshova

It is important to approach the creation of secure information system that processes personal data. Currently, it is difficult to imagine organization that wouldn't have to work with them. Organizational and technical protection measures are necessary to provide the security of personal data at processing in information systems. The basic set of these measures is determined by level of personal data protection. This article includes the outline of the analysis of the personal data information system, also possible ways to provide information security.

Keywords: safety system, security level, sort of security threat, certification, information security products.

Статья поступила в редакцию 04.11.2016 г.

Lapshova Marina Alexandrovna,
(lapshova.marina.smr@gmail.com),
student V course of the faculty of Informatics
of the Samara University,
443086, Russia, Samara, Moskovskoye shosse, 34.