Безопасность персональных данных

Необходимость обеспечения безопасности персональных данных в наше время объективная реальность. Информация о человеке всегда имела большую ценность, но сегодня она превратилась в самый дорогой товар. Информация в руках мошенника превращается в орудие преступления, в руках уволенного сотрудника — в средство мщения, в руках инсайдера — товар для продажи конкуренту. Именно поэтому персональные данные нуждаются в самой серьезной защите.

Автоматизированные информационные системы содержат персональные сведения субъектов образовательного процесса (Персональные данные). Обязанность образовательных учреждений, как операторов персональных данных, состоит в необходимости принятия всех требуемых законодательством мер по обеспечению защиты такого типа данных.

Отношения, связанные с обработкой персональных данных, регулируются Федеральным законом от 27.07.2006 № 152-ФЗ (ред. от 23.07.2013) «О персональных данных».

В соответствии с Законом № 152-ФЗ персональными данными является любая информация, с помощью которой можно однозначно идентифицировать физическое лицо (субъект ПДн). К персональным данным в связи с этим могут относиться фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, принадлежащая субъекту ПДн.

Категории персональных данных

Законодательство определяет различные категории персональных данных. К ним могут относиться общедоступные ПДн, специальные категории ПДн, категории ПДн, обрабатываемые в информационных системах персональных данных (далее ИСПДн), биометрические ПДн и другие.

Общедоступные ПДн

Общедоступными являются данные, доступ к которым предоставлен неограниченному кругу лиц с согласия субъекта ПДн или на которые в соответствии с федеральными законами не распространяются требования соблюдения конфиденциальности. Такие данные могут включать фамилию, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные ПДн. Источниками такой информации являются, к примеру, справочники, адресные книги и т.п. Сведения о субъекте ПДн могут быть в любое время исключены из общедоступных источников по требованию субъекта либо по решению суда или уполномоченных государственных органов.

Специальные категории ПДн

К специальным категориям относятся персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни. Их обработка допускается только в следующих случаях:

- субъект ПДн дал согласие в письменной форме на обработку своих персональных данных;
- персональные данные являются общедоступными;

- персональные данные относятся к состоянию здоровья субъекта ПДн и получение его согласия невозможно, либо обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;
- обработка персональных данных членов (участников) общественного объединения или религиозной организации при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов ПДн;
- обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о безопасности, об оперативно-розыскной деятельности, а также в соответствии с уголовно-исполнительным законодательством Российской Федерации или необходима в связи с осуществлением правосудия.

Категории персональных данных, обрабатываемых в ИСПДн

Совместный приказ ФСТЭК, ФСБ и Министерства информационных технологий и связи РФ от 13 февраля 2008 года № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных» определяет следующие категории персональных данных, которые обрабатываются в ИСПДн:

- Категория 1 — персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни.
- Категория 2 — персональные данные, позволяющие идентифицировать субъекта ПДн и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1.
- Категория 3 — персональные данные, позволяющие идентифицировать субъекта ПДн.
- Категория 4 — обезличенные и (или) общедоступные персональные данные.

Категорирование персональных данных при обработке в ИСПДн может также проводиться по параметру «объем обрабатываемых персональных данных». Под этим подразумевается количество субъектов, данные которых обрабатываются в информационной системе. Этот параметр может принимать следующие значения:

- В информационной системе одновременно обрабатываются персональные данные более чем 100000 субъектов ПДн или персональные данные субъектов ПДн в пределах субъекта РФ или Российской Федерации в целом.
- В информационной системе одновременно обрабатываются персональные данные от 1000 до 100000 субъектов ПДн или персональные данные субъектов ПДн, работающих в отрасли экономики Российской Федерации, в органе государственной власти, проживающих в пределах муниципального образования.
- В информационной системе одновременно обрабатываются данные менее чем 1000 субъектов ПДн или персональные данные субъектов ПДн в пределах конкретной организации.

Такое категорирование персональных данных необходимо для определения класса ИСПДн, от которого зависят меры по обеспечению безопасности ПДн при обработке в информационных системах.

Биометрические персональные данные

Биометрические персональные данные — это сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его

личность. Биометрические персональные данные обрабатываются в соответствии со статьей 11 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Они могут обрабатываться только при наличии согласия в письменной форме субъекта ПДн. Обработка биометрических персональных данных без согласия субъекта ПДн может осуществляться в связи с осуществлением правосудия, а также в случаях, предусмотренных законодательством Российской Федерации о безопасности, об оперативно-розыскной деятельности, о государственной службе, о порядке выезда из РФ и въезда в Российскую Федерацию, уголовно-исполнительным законодательством.

В каких случаях обеспечение безопасности персональных данных не требуется?

Обеспечение безопасности (в данном случае конфиденциальности) в соответствии с российским законодательством не требуется лишь для обезличенных и общедоступных персональных данных.

Персональные данные могут быть обезличенными, в случае, если над ними были произведены действия, в результате которых невозможно определить их принадлежность конкретному субъекту ПДн.

Персональные данные могут быть общедоступными только с письменного согласия субъекта ПДн. Они могут включать фамилию, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные субъектом ПДн.

Обеспечение безопасности ПДн при их обработке в ИСПДн достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование и распространение персональных данных. Обязанность по обеспечению безопасности ПДн при их обработке в ИСПДн полностью возлагается на оператора персональных данных. В связи с этим оператор обязан:

- проводить мероприятия, направленные на предотвращение несанкционированного доступа (далее НСД) к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;
- своевременно обнаруживать факты НСД к персональным данным;
- не допускать воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование;
- незамедлительно восстанавливать ПДн, модифицированные или уничтоженные вследствие несанкционированного доступа к ним;
- осуществлять постоянный контроль за обеспечением уровня защищенности ПДн.