МЕТОДИКА ОПРЕДЕЛЕНИЯ УРОВНЯ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Москва, 2017

Содержание

1. Введение

В образовательных организациях осуществляется обработка персональных данных (далее – ПД) с использованием информационных систем персональных данных (далее – ИСПД). Для соответствия законодательству Российской Федерации в области защиты ПД необходимо обеспечивать безопасность обрабатываемых ПД.

В соответствии с требованиями ч.3 ст.19 Федерального закона Российской Федерации № 152-ФЗ «О персональных данных» (далее – Закон о персональных данных) выбор мер для защиты ПД осуществляется в соответствии с устанавливаемым уровнем защищенности ПД для каждой ИСПД.

Порядок установления уровня защищенности ПД для ИСПД определен в Требованиях к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 (далее – 1119-ПП).

В настоящем документе описаны методические рекомендации по установлению уровня защищенности ПД в ИСПД, а также приведены проекты (шаблоны) актов об определении уровня защищенности ПД в ИСПД.

2. Общие положения

Уровень защищенности ПД при их обработке в ИСПД зависит от следующих критериев:

1) категория обрабатываемых ПД;

2) количество обрабатываемых субъектов ПД;

3) тип актуальных угроз безопасности ПД при их обработке в ИСПД.

2.1. Категория обрабатываемых ПД

Информационная система является информационной системой, обрабатывающей специальные категории ПД, если в ней обрабатываются ПД, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов ПД.

Информационная система является информационной системой, обрабатывающей биометрические ПД, если в ней обрабатываются сведения, которые характеризуют физиологические и биологические особенности субъекта ПД, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта ПД, и не обрабатываются сведения, относящиеся к специальным категориям ПД.

Информационная система является информационной системой, обрабатывающей общедоступные ПД, если в ней обрабатываются ПД субъектов ПД, полученные только из общедоступных источников ПД.

Информационная система является информационной системой, обрабатывающей иные категории ПД, если в ней не обрабатываются ПД, относящиеся к специальным, биометрическим или общедоступным.

2.1.1. Тип субъекта ПД

Информационная система является информационной системой, обрабатывающей ПД сотрудников, если в ней обрабатываются только ПД сотрудников образовательной организации. В остальных случаях ИСПД является информационной системой, обрабатывающей ПД субъектов ПД, не являющихся сотрудниками образовательной организации.

2.2. Количество обрабатываемых субъектов ПД

Требованиями к защите персональных данных при их обработке в информационных системах персональных данных определенно два значения показателя:

1) обработка ПД менее 100 000 субъектов ПД в информационной системе;

2) обработка ПД более 100 000 субъектов ПД в информационной системе.

2.3. Тип актуальных угроз безопасности ПД

Установлены следующие типы актуальных угроз безопасности ПД при их обработке в ИСПД:

1) угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе;

2) угрозы 2-го типа актуальны для информационной системы, если для нее актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе;

3) угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

3. Определение уровня защищенности ПД

Установление уровня защищенности ПД для каждой ИСПД осуществляется в соответствии положениями п.9-12 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных 1119-ПП. Ниже представлен пошаговый алгоритм определения уровня защищенности ПД в ИСПД.

3.1. Шаг 1. Определение категорий ПД, обрабатываемых в ИСПД

В рамках данного шага определяем категории обрабатываемых ПД:

1) **Специальные** – ПД, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов ПД.

2) **Биометрические** – сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта ПД, и не обрабатываются сведения, относящиеся к специальным категориям ПД.

3) **Общедоступные** – ПД субъектов ПД, полученные только из общедоступных источников ПД, созданных в соответствии со ст. 8 Закона о персональных данных.

4) **Иные** – ПД, не относящиеся к специальным и биометрическим и не являющиеся общедоступными данными.

3.2.Шаг 2. Определение типа субъекта ПД

На данном шаге необходимо определить тип субъектов ПД, обрабатываемых в ИСПД:

1) Субъект ПД, **являющийся сотрудником** образовательной организации.

2) Субъект ПД, **не являющийся сотрудником** образовательной организации.

Если в ИСПД одновременно обрабатываются ПД сотрудников образовательной организации и субъектов, не являющихся сотрудниками образовательной организации, то для ИСПД устанавливается тип субъекта «Субъект ПД, **не являющийся сотрудником** образовательной организации».

3.3.Шаг 3. Определение количества обрабатываемых субъектов ПД в ИСПД

В рамках данного шага необходимо проанализировать обрабатываемое количество субъектов ПД в информационной системе и по результатам анализа получить контрольное значение:

1) **менее 100 000** субъектов ПД;

2) **более 100 000** субъектов ПД.

3.4.Шаг 4. Определение типов актуальных угроз

Для выполнения данного шага в документе «Модель угроз безопасности ПД в ИСПД» определяем актуальные угрозы безопасности ПД в ИСПД, в том числе определяем актуальность угроз недекларированных возможностей в прикладном программном обеспечении и недекларированных возможностей в системном программном обеспечении.

В зависимости от их актуальности (п. 2.3) получаем одно из следующих значений:

1) **1 тип угроз**;

2) **2 тип угроз**;

3) **3 тип угроз**.

3.5.Шаг 5. Определение уровня защищенности ПД в ИСПД

По результатам, полученным в ходе шагов 1-4, определяются уровни защищенности ПД в ИСПД и фиксируются Актом установления уровня защищенности ПД в ИСПД (**Ошибка! Источник ссылки не найден.**).

Для удобства определения уровней защищенности ПД подготовлена таблица, которая сформирована на основании пп.9-12 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных 1119-ПП

Таблица 1 – Таблица определения уровня защищенности ПД в ИСПД

	Категории ПД, количество субъектов ПД, тип субъектов ПД											
	специальные			**биометрические**			**общедоступные**			**иные**		
Угрозы	**>100 000**	**<100 000**	**сотр уд**	**>100 000**	**<100 000**	**сотр уд**	**>100 000**	**<100 000**	**сотр уд**	**>100 000**	**<100 000**	**сотр уд**
1 тип	1УЗ			1УЗ			2УЗ			1УЗ		
2 тип	1УЗ	2УЗ		2УЗ			2УЗ	3УЗ		2УЗ	3УЗ	
3 тип	2УЗ	3УЗ		3УЗ			4УЗ			3УЗ	4УЗ	

Примечание: по результатам проведенных обследований ОО в информационных системах, которые используются для обработки ПД, обрабатываются иные категории ПД, биометрические и специальные ПД. При принятии мер по нейтрализации угроз[1] недекларированных возможностей в системном и прикладном программном обеспечении для информационных систем будут определены 3 уровень защищенности ПД в ИСПД или 4 уровень защищенности ПД в ИСПД.

[1] Меры по нейтрализации угроз 1 и 2 типа:

проверка системного и (или) прикладного программного обеспечения, включая программный код, на отсутствие недекларированных возможностей с использованием автоматизированных средств и (или) без использования таковых;

тестирование информационной системы на проникновения;

использование в информационной системе системного и (или) прикладного программного обеспечения, разработанного с использованием методов защищенного программирования.