О положениях постановления Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

В связи с принятием постановления Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее – ПП-1119) утратило силу постановление Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» (далее – ПП-781).

Учитывая, что ПП-1119 было принято в соответствии со статьей 19 Федерального закона от 27 июля 2006 г. 152-ФЗ «О персональных данных» (далее - 152-ФЗ) в той редакции, которая распространяется на правоотношения, возникшие с 1 июля 2011 года, требования ПП-1119 обязательны к исполнению для информационных систем персональных данных (далее – ИСПДн), созданных с 1 июля 2011 года. В отношении ИСПДн, созданных до 1 июля 2011 года, применимы как требования ПП-1119, так и требования ПП-781.

В случае, если работы по обеспечению безопасности персональных данных в ИСПДн, созданных с 1 июля 2011 года, уже были выполнены до вступления в силу ПП-1119, после принятия нормативных правовых актов ФСБ России и ФСТЭК России необходимо будет пересмотреть результаты выполненных работ на соответствие ПП-1119, а также указанным документам ФСБ России и ФСТЭК России, в соответствии с которыми будет осуществляться выбор средств защиты информации (далее – СЗИ).

Новым ПП-1119 установлены:

- требования к защите персональных данных при их обработке в ИСПДн;
- уровни защищенности таких данных.

В соответствии с ПП-1119 оператору или лицу, осуществляющему обработку персональных данных по поручению оператора на основании заключаемого с этим лицом договора, необходимо создать систему защиты персональных данных, обеспечивающую безопасность персональных данных, включающую организационные и (или) технические меры, которые определяются с учетом:

- актуальных угроз безопасности персональных данных;
- информационных технологий, используемых в ИСПДн.

При этом в ПП-1119 не содержится упоминания о СЗИ как обязательной компоненте обеспечения безопасности персональных данных, как это было определено в ПП-781.

В ПП-1119 установлены как новые требования к операторам, так и требования, ранее закрепленные в других нормативных правовых актах:

1. Необходимо включить в договор между оператором и уполномоченным лицом обязанность уполномоченного лица обеспечить безопасность персональных данных при их обработке в ИСПДн [1)].

2. СЗИ для системы защиты персональных данных должны быть выбраны оператором после принятия нормативных правовых актов ФСБ России и ФСТЭК России во исполнение ч.4 ст.19 152-ФЗ.

3. Необходимо определить, какие категории персональных данных обрабатываются в каждой ИСПДн, а также к какой из двух категорий субъектов (работники опреатора или иные лица) принадлежат эти персональные данные:

- специальные категории персональных данных;
- биометрические персональные данные;
- общедоступные персональные данные;
- иные категории персональных данных.

При этом:

- в ПП-1119 не упоминаются обезличенные персональные данные как категория персональных данных. Следовательно, для персональных данных, в отношении которых были совершены действия по обезличиванию, определение уровня защищенности не требуется[2)];
- сведения о судимости не причислены ни к одной из вышеназванных категорий персональных данных, несмотря на то, что в ст.10 152-ФЗ они отнесены к специальным категориям;
- ИСПДн признается обрабатывающей общедоступные персональные данные, если в ней обрабатываются персональные данные субъектов, полученные только из общедоступных источников персональных данных. Случаи, когда персональные данные сделаны субъектом общедоступными в соответствии с п.10 ч.1 ст.6 152-ФЗ, в ПП-1119 не рассмотрены.

4. Необходимо определить, угрозы какого типа из трех возможных актуальны для этих ИСПДн в зависимости от наличия недокументированных (недекларированных) возможностей, а также типа программного обеспечения (системное (далее - СПО) или прикладное (далее – ППО)). Определение типа актуальных угроз должно осуществляться с учетом оценки возможного вреда субъектам персональных данных и в соответствии с нормативными правовыми актами, определяющими актуальные угрозы безопасности персональных данных при их обработке в ИСПДн при осуществлении соответствующих видов деятельности[3)].

5. Необходимо разработать документ, на основании которого можно оценить возможный вред субъектам персональных данных в случае нарушения 152-ФЗ[4].

6. Необходимо установить количество субъектов, персональные данные которых обрабатываются в каждой ИСПДн (больше 100 000 или меньше 100 000).

7. Необходимо определить, какой уровень защищенности персональных данных из четырех возможных необходимо обеспечивать при их обработке в ИСПДн (см.Таблицу 1) на основании:

- типа актуальных угроз,
- категорий персональных данных, обрабатываемых в ИСПДн,
- категорий субъектов, персональные данные которых обрабатываются в ИСПДн,
- количества субъектов, персональные данные которых обрабатываются в каждой ИСПДн.

8. Выполнить требования, предусмотренные в ПП-1119, для обеспечения соответствующего уровня защищенности персональных данных (см. Таблицу 2).

9. Оператору (уполномоченному лицу) необходимо не реже 1 раза в 3 года организовывать и проводить контроль за выполнением указанных требований (самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации.

Таблица 1. Определение уровней защищенности (УЗ) персональных данных

<table>
<tr><th rowspan="2">Категории ПДн</th><th rowspan="2">Сотрудники оператора</th><th rowspan="2">Количество субъектов</th><th colspan="3">Тип актуальных угроз</th></tr>
<tr><th>I (НДВ в СПО)</th><th>II (НДВ в ППО)</th><th>III (нет НДВ)</th></tr>
<tr><td rowspan="3">Специальные</td><td>Нет</td><td>более 100 000</td><td rowspan="4">УЗ-1</td><td>УЗ-1</td><td>УЗ-2</td></tr>
<tr><td>Нет</td><td>менее 100 000</td><td rowspan="3">УЗ-2</td><td rowspan="2">УЗ-3</td></tr>
<tr><td>Да</td><td>–</td></tr>
<tr><td>Биометрические</td><td>–</td><td>–</td></tr>
<tr><td rowspan="3">Общедоступные</td><td>Нет</td><td>более 100 000</td><td rowspan="3">УЗ-2</td><td rowspan="3">УЗ-4</td></tr>
<tr><td>Нет</td><td>менее 100 000</td><td rowspan="2">УЗ-3</td></tr>
<tr><td>Да</td><td>–</td></tr>
<tr><td rowspan="3">Иные</td><td>Нет</td><td>более 100 000</td><td rowspan="3">УЗ-1</td><td>УЗ-2</td><td>УЗ-3</td></tr>
<tr><td>Нет</td><td>менее 100 000</td><td rowspan="2">УЗ-3</td><td rowspan="2">УЗ-4</td></tr>
<tr><td>Да</td><td>–</td></tr>
</table>

Таблица 2. Определение требований, выполнение которых необходимо для обеспечения соответствующих УЗ

Требования	УЗ			
	1	2	3	4
Режим обеспечения безопасности помещений, где обрабатываются персональные данные	+	+	+	+
Сохранность носителей персональных данных	+	+	+	+
Перечень лиц, допущенных к персональным данным	+	+	+	+
СЗИ, прошедшие процедуру оценки соответствия	+	+	+	+
Должностное лицо, ответственное за обеспечение безопасности персональных данных в ИСПДн	+	+	+	–
Ограничение доступа к содержанию электронного журнала сообщений	+	+	–	–
Автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным	+	–	–	–
Структурное подразделение, ответственное за обеспечение безопасности персональных данных	+	–	–	–

персональные данные, аналитика

[1] Данный пункт необходим к исполнению в случае, если соответствующие положения еще не закреплены в договорах с уполномоченными лицами во исполнение ч.3 ст.6 152-ФЗ.

[2] Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных (п.9 ст.3 152-ФЗ).

[3] Указанные нормативные правовые акты необходимо будет учитывать после их принятия во исполнение ч.5 ст.19 152-ФЗ

[4] Данный пункт необходим к исполнению в случае, если оценка вреда субъектам персональных данных еще не произведена оператором во исполнение п.5 ч.1 ст.18.1 152-ФЗ.