Проект

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ

от ___ _____ 201_ г. №_____

г. Москва

Об установлении уровней защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных

В соответствии со статьей 19 Федерального закона «О персональных данных» Правительство Российской Федерации **постановляет:**

1. Установить следующие уровни защищенности персональных данных:

УЗ-1 – максимальный уровень защищенности персональных данных;

УЗ-2 – высокий уровень защищенности персональных данных;

УЗ-3 – средний уровень защищенности персональных данных;

УЗ-4 – низкий уровень защищенности персональных данных.

2. Установить, что уровни защищенности персональных данных определяются оператором или лицом, осуществляющим обработку персональных данных по поручению оператора, в зависимости от угроз безопасности персональных данных с учетом возможного вреда субъекту персональных данных, объема и содержания обрабатываемых персональных данных, вида деятельности, при осуществлении которого обрабатываются персональные данные, актуальности угроз безопасности персональных данных.

3. Утвердить прилагаемое Положение о порядке определения уровней защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных.

Председатель Правительства
Российской Федерации В. Путин

Утверждено
постановлением Правительства
Российской Федерации
от _____ 201_ г. № ____

ПОЛОЖЕНИЕ О ПОРЯДКЕ ОПРЕДЕЛЕНИЯ УРОВНЕЙ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ В ЗАВИСИМОСТИ ОТ УГРОЗ БЕЗОПАСНОСТИ ЭТИХ ДАННЫХ

I. Общие положения

1. Настоящее Положение устанавливает порядок определения уровней защищенности персональных данных при их обработке в информационных системах персональных данных (далее – информационная система) в зависимости от угроз безопасности этих данных с учетом возможного вреда субъекту персональных данных, объема и содержания обрабатываемых персональных данных, вида деятельности, при осуществлении которого обрабатываются персональные данные, актуальности угроз безопасности персональных данных.

2. Под уровнем защищенности персональных данных понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах.

3. Под угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе.

4. Определение уровня защищенности персональных данных при их обработке в информационной системе проводится с целью установления методов и способов защиты информации, необходимых для обеспечения безопасности персональных данных.

5. Определение уровня защищенности персональных данных проводится на этапе создания информационной системы, ее эксплуатации (при необходимости) или модернизации.

6. Уровень защищенности персональных данных при их обработке в информационной системе пересматривается оператором или лицом, осуществляющим обработку персональных данных по поручению оператора (далее – оператор):

по решению оператора, на основе проведенных им анализа и оценки угроз безопасности персональных данных с учетом особенностей и (или) изменений конкретной информационной системы;

по результатам мероприятий по контролю за выполнением организационных и технических мер, необходимых для выполнения установленных требований к защите персональных данных для каждого из уровней защищенности.

7. Определение уровня защищенности персональных данных включает в себя следующие этапы:

сбор и анализ исходных данных по информационной системе;

классификацию информационной системы;

формирование модели угроз и определение категории нарушителя;

установление уровня защищенности персональных данных и его документальное оформление.

II. Сбор и анализ исходных данных по информационной системе, классификация информационной системы

8. Оператор на основе своего вида деятельности, при осуществлении которого обрабатываются персональные данные, определяет следующие исходные данные:

содержание обрабатываемых персональных данных – $X_{ПД}$;

объем обрабатываемых персональных данных – $X_{НПД}$.

9. Определяются следующие типы $X_{ПД}$:

тип 1 – специальные категории персональных данных, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, а также биометрические персональные данные;

тип 2 – фамилия, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, или любая

совокупность таких персональных данных, позволяющая однозначно определить субъекта персональных данных, а также дополнительные персональные данные, за исключением персональных данных типа 1;

тип 3 – фамилия, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, или любая совокупность таких персональных данных, позволяющая однозначно определить субъекта персональных данных;

тип 4 – результат обезличивания персональных данных, представляющего действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных (далее – обезличенные персональные данные). В случае, если имеется возможность получения оператором такой дополнительной информации, информационная система считается обрабатывающей персональные данные того типа содержания, который был определен до прохождения процедуры обезличивания.

10. $X_{НПД}$ может принимать следующие значения:

1 – в информационной системе одновременно обрабатываются персональные данные более чем 100 000 субъектов персональных данных;

2 – в информационной системе одновременно обрабатываются персональные данные от 1000 до 100 000 субъектов персональных данных;

3 – в информационной системе одновременно обрабатываются данные менее чем 1000 субъектов персональных данных;

11. Оператор на основе исходных данных определяет класс информационной системы (Ki) в соответствии с таблицей.

$X_{НПД}$ / $X_{ПД}$	1	2	3
тип 1	К1	К1	К2
тип 2	К1	К2	К2
тип 3	К2	К3	К3
тип 4	К4	К4	К4

12. Оператор в зависимости от возможного вреда субъекту персональных данных вправе своим решением определить для своей информационной системы класс выше, чем требуется в соответствии с настоящим Положением.

III. Формирование модели угроз и определение категории нарушителя

13. Оператор на основе угроз безопасности персональных данных формирует модель угроз, включающую модель нарушителя.

Модель угроз формируется в соответствии с нормативными правовыми актами ФСТЭК России и ФСБ России.

В случаях, предусмотренных федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами, а также соглашениями между ФСТЭК России и ФСБ России модель угроз формируется только в соответствии с нормативными правовыми актами ФСБ России.

При формировании модели угроз проводится анализ актуальности угроз безопасности персональных данных в соответствии с нормативными правовыми актами ФСТЭК России. При этом все угрозы, определенные в модели нарушителя, считаются актуальными.

14. Оператор на основе модели угроз определяет категорию нарушителя.

Устанавливаются три категории нарушителей (KHj):

КН1 – нарушитель (группа нарушителей), самостоятельно осуществляющий (осуществляющая) создание методов и средств реализации атак и реализацию атак на информационную систему (нарушитель с низким потенциалом);

КН2 – группа нарушителей, осуществляющая создание методов и средств реализации атак и реализацию атак на информационную систему с привлечением специалистов в области разработки и анализа средств защиты информации, включая специалистов в области защиты информации от утечки по техническим каналам и (или) специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного программного обеспечения (нарушитель со средним потенциалом);

КН3 – нарушитель или группа нарушителей, осуществляющая создание методов и средств реализации атак и реализацию атак на информационную систему с привлечением специалистов в области разработки и анализа средств защиты информации, включая специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного программного обеспечения (нарушитель с высоким потенциалом).

Возможности нарушителя категории КН2 включают в себя возможности нарушителя категории КН1.

Возможности нарушителя категории КН3 включают в себя возможности нарушителя категорий КН1 и КН2.

15. Нарушители в зависимости от возможностей доступа к средствам вычислительной техники, с использованием которых реализована информационная система, подразделяются на внешних и внутренних.

Внешний нарушитель осуществляет атаки из-за пределов контролируемой зоны оператора.

Внутренний нарушитель осуществляет атаки, находясь в пределах контролируемой зоны оператора.

Контролируемая зона – это пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств.

IV. Установление уровня защищенности персональных данных и его документальное оформление

16. Оператор на основе исходных данных определяет уровень защищенности персональных данных при их обработке в информационной системе в соответствии с таблицей.

Ki \ KHj	КН1	КН2	КН3
К1	УЗ-2	УЗ-1	УЗ-1
К2	УЗ-3	УЗ-2	УЗ-1
К3	УЗ-3	УЗ-3	УЗ-2
К4	УЗ-4	УЗ-4	УЗ-4

Определенный уровень защищенности персональных данных при их обработке в информационной системе документально оформляется в виде акта оператора, содержащего описание исходных данных по информационной системе, результаты их анализа и обоснование выбранного уровня защищенности персональных данных.

17. Оператор вправе своим решением определить для своей информационной системы уровень защищенности персональных данных выше, чем требуется в соответствии с настоящим Положением.

Определение оператором для своей информационной системы уровня защищенности персональных данных ниже требуемого в соответствии с настоящим Положением возможно только с письменного разрешения ФСТЭК России и ФСБ России.