АКТ КЛАССИФИКАЦИИ

по требованиям безопасности информации

2018 г.

СПИСОК СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ

Специальные категории персональных данных	Персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных
Биометрические персональные данные	Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность
Общедоступные персональные данные	Персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей 8 Федерального закона «О персональных данных»
Иные категории персональных данных	Персональные данные, не относящиеся к специальным, биометрическим или общедоступным персональным данным
АРМ	Автоматизированное рабочее место
ИСПДн	Информационная система персональных данных
ИС	Информационная система
ПДн	Персональные данные
УЗ	Уровень значимости
Угрозы 1-го типа	Угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.
Угрозы 2-го типа	Угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе
Угрозы 3-го типа	Угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе
Актуальные угрозы безопасности персональных данных	Совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия

1.ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Определение уровня защищенности персональных данных осуществляется с целью установления методов и способов защиты, необходимых для обеспечения безопасности ПДн и в соответствии с требованиями, установленными Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и Постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.2. Проведение классификации информационной системы осуществляется в соответствии с требованиями, установленными Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и защите информации» и п. 6 Приказа ФСТЭК России от 11.02.2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

2. СОСТАВ КОМИССИИ

Комиссия назначена Распоряжением от года № в составе:

Председатель комиссии:

фио - должность

Члены комиссии:

фио - должность;

фио - должность;

фио - должность;

фио - должность;

фио - должность;

фио - должность;

фио - должность;

3. ОПРЕДЕЛЕНИЕ КЛАССА ЗАЩИЩЕННОСТИ

3.1. **название системы** является государственной информационной системой (Ст. 14 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и защите информации»)

3.2. Для определения класса защищенности информационной системы принимается порядок, изложенный в Приказе ФСТЭК России от 11.02.2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (Приложение № 1. Определение класса защищенности информационной системы).

3.3. Класс защищенности информационной системы определяется в зависимости от уровня значимости информации, обрабатываемой в этой информационной системе, и масштаба информационной системы (федеральный, региональный, объектовый) – К = [УЗ; масштаб системы].

3.4. Уровень значимости информации определяется степенью возможного ущерба наносимого

от нарушения конфиденциальности (неправомерные доступ, копирование, предоставление, или распространение), целостности (неправомерные уничтожение или модифицирование) или доступности (неправомерное блокирование) защищаемой информации.

С учетом обработки в информационной системе нескольких видов информации степень возможного ущерба определена отдельно для каждого вида информации и приведена в Таблице 1.

Таблица 1. Определение степени возможного ущерба

Виды информации	**Степень возможного ущерба**		
	Нарушение конфиденциальности	Нарушение целостности	Нарушение доступности
Информация, обрабатываемая основными технологическими сервисами	средний	средний	средний
Персональные данные	средний	средний	средний
Общедоступная информация		средний	средний

Итоговый уровень значимости информации, обрабатываемой в информационной системе, установлен по наивысшим значениям степени возможного ущерба, определенным для конфиденциальности, целостности, доступности информации каждого вида информации, указанным в Таблице 1. Таким образом, уровень значимости информации обрабатываемой в информационной системе определяется как **средний уровень значимости (УЗ 2)**.

3.5. Информационная система имеет **региональный** масштаб и функционирует на территории субъекта Российской Федерации и имеет сегменты в одном или нескольких муниципальных образованиях и (или) подведомственных и иных организациях. Определение класса защищенности приведено в табл. № 2.

3.6. Согласно требованиям, утвержденным приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственной тайны, содержащейся в государственных информационных системах» и в соответствии с определенным уровнем значимости обрабатываемой информации и масштабом системы, для информационной системы определен **второй класс защищенности (К2)**.

Табл. 2. Определение класса защищенности информационной системы

Уровень значимости информации	**Масштаб информационной системы**		
	Федеральный	**Региональный**	**Объектовый**
УЗ 1 (высокая степень ущерба)	К1	К1	К1
УЗ 2 (средняя степень ущерба)	К1	К2	К2
УЗ 3 (низкая степень ущерба)	К2	К3	К3
УЗ 4 (минимальная степень ущерба)	К3	К3	К4

4. ОПРЕДЕЛЕНИЕ УРОВНЯ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. В соответствии с Постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», установлены четыре уровня защищенности персональных данных при их обработке в информационных системах. **название системы** является информационной системой персональных данных (далее - ИСПДн) и имеет следующие характеристики, с учетом которых определяется уровень защищенности персональных данных:

Категория обрабатываемых персональных данных	специальные категории персональных данных – обрабатываются персональные данные, касающиеся, состояния здоровья, субъектов ПДн.
Объем обрабатываемых персональных данных	Персональные данные более чем 100 000 субъектов персональных данных, не являющихся сотрудниками оператора.
Тип актуальных угроз	Угрозы 3-го типа – угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе

С учетом указанных характеристик в соответствии с п. 12 б) Постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» определена необходимость обеспечения **2-го уровня защищенности персональных данных (УЗ 2)** при их обработке в информационной системе.

5. ВЫВОДЫ КОМИССИИ

В соответствии с приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственной тайны, содержащейся в государственных информационных системах» определить для **название системы второй класс защищенности (К2)**.

В соответствии с постановлением Правительства № 1119 от 01.11.2012 года «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» классифицировать **название системы** как информационную систему персональных данных и установить необходимость обеспечения **2-го уровня защищенности персональных данных (УЗ 2)** при их обработке в информационной системе.

Председатель комиссии _____ фио

Члены комиссии _____ фио

_____ фио

_____ фио

_____ фио

_____ фио

_____ фио

_____ фио