

УТВЕРЖДАЮ  
Президент  
Инфокоммуникационного союза

А.Е. Крупнов

«\_\_\_» \_\_\_\_\_ 2010 г.

**СОГЛАСОВАНО**

Начальник 2-го управления Федеральной  
службы по техническому и экспортному  
контролю

А.В. Куц

«30» МАРТА 2010 г



**НАУЧНО-ИССЛЕДОВАТЕЛЬСКАЯ РАБОТА  
«РАЗРАБОТКА КОНЦЕПЦИИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В  
ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ  
ОПЕРАТОРОВ СВЯЗИ»  
(шифр «ТРИТОН»)**

**ОТРАСЛЕВОЙ КЛАССИФИКАТОР  
«ИНФОРМАЦИОННЫЕ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ  
ОПЕРАТОРОВ СВЯЗИ»  
(ICU-4/2009-ОК)**

Заместитель генерального директора  
ЗАО «Рэйнвокс»



А.В. Захаркин

«01» МАРТА 2010 г.





## АННОТАЦИЯ

Отраслевой классификатор «Информационные системы персональных данных операторов связи»<sup>1</sup> разработан ЗАО «ReignVox» в рамках научно-исследовательской работы «Разработка концепции защиты персональных данных в информационных системах персональных данных операторов связи» (шифр «ТРИТОН»).

Положения настоящего Классификатора рекомендуется использовать при проведении классификации информационных систем персональных данных операторов связи<sup>2</sup>.

Целью Классификатора является установление методов и способов защиты информации, необходимых для обеспечения безопасности персональных данных обрабатываемых в информационных системах персональных данных операторов связи.

Классификатор содержит перечень информационных систем персональных данных операторов связи, исходные данные на эти системы, необходимые для проведения классификации, а также сведения о предварительной классификации.

Перечень информационных систем персональных данных операторов связи, приведенный в настоящем Классификаторе, не является конечным и может быть расширен по мере развития информационно-технологической инфраструктуры и бизнес-процессов операторов связи.

<sup>1</sup> Далее – Классификатор

<sup>2</sup> Оператор связи - юридическое лицо или индивидуальный предприниматель, оказывающие услуги связи на основании соответствующей лицензии (126-ФЗ «О связи»)

Инв. № подл.	Подп. и дата	Инв. № дубл.	Взам. инв. №	Подп. и дата					
Ли	Изм.	№ докум.	Подп.	Дат	ICU-4/2009-OK				Лист
									4

## ОГЛАВЛЕНИЕ

<b>1. КЛАССИФИКАЦИЯ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ.....</b>	<b>6</b>
1.1 Общие положения .....	6
1.2 Порядок проведения классификации .....	8
1.3 Критерии отнесения информационных систем к специальным .....	9
<b>2. ИНФОРМАЦИОННЫЕ СИСТЕМЫ ОПЕРАТОРОВ СВЯЗИ .....</b>	<b>10</b>
2.1 Общие положения .....	10
2.2 Внутренние информационные системы .....	11
2.2.1 Информационные системы услуг связи .....	11
2.2.2 Информационные системы управления предприятием .....	16
2.3 Информационные системы внешнего взаимодействия .....	19
<b>3. СУБЪЕКТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ.....</b>	<b>22</b>
3.1 Категории субъектов персональных данных. Цели обработки персональных данных ..	22
3.2 Перечни персональных данных субъектов персональных данных .....	23
3.3 Категории персональных данных субъектов персональных данных .....	25
<b>4. СБОР И АНАЛИЗ ИСХОДНЫХ ДАННЫХ.....</b>	<b>27</b>
4.1 Общие положения .....	27
4.2 Внутренние информационные системы .....	28
4.2.1 Информационные системы услуг связи .....	28
4.2.2 Информационные системы управления предприятием .....	38
4.3 Информационные системы внешнего взаимодействия .....	41
<b>5. ОТРАСЛЕВОЙ КЛАССИФИКАТОР. МЕТОДИКА КЛАССИФИКАЦИИ. ....</b>	<b>46</b>
5.1 Общие положения .....	46
5.2 Сбор и анализ исходных данных.....	46
5.3 Присвоение информационной системе соответствующего класса.....	47
5.3.1 Методика классификации типовых информационных систем .....	47
5.3.2 Методика классификации специальных информационных систем .....	47
5.4 Выбор требований по обеспечению безопасности персональных данных .....	49
<b>Приложение 1. НОРМАТИВНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ .....</b>	<b>51</b>
<b>Приложение 2. ПЕРЕЧЕНЬ СОКРАЩЕНИЙ.....</b>	<b>55</b>

Подп. и дата					
	Взам. инв. №				
Подп. и дата					
	Инв. № дубл.				
Подп. и дата					
	Инв. № подл.				
Подп. и дата					
	Инв. № инв.				
Инв. № подл.	<b>ICU-4/2009-OK</b>				
	Ли	Изм.	№ докум.	Подп.	Дата
	Разраб.	Романов В.В.			
	Пров.				
	Т. контр.				
	Н. контр.				
	Утв.				
Отраслевой классификатор «Информационные системы персональных данных операторов связи»					
			Лит	Лист	Листов
				5	55
Союз участников рынка инфокоммуникационных услуг					

# 1. КЛАССИФИКАЦИЯ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

## 1.1 Общие положения

Информационные системы классифицируются государственными органами, муниципальными органами, юридическими или физическими лицами, организующими и (или) осуществляющими обработку персональных данных, а также определяющими цели и содержание обработки персональных данных (ПДн), в зависимости от объема обрабатываемых ими персональных данных и угроз безопасности жизненно важным интересам личности, общества и государства<sup>3</sup>.

Информационные системы персональных данных классифицируются на этапе их создания или в ходе их эксплуатации (для ранее введенных в эксплуатацию и (или) модернизируемых информационных систем) с целью установления методов и способов защиты, необходимых для обеспечения безопасности персональных данных<sup>4</sup>.

Классификация информационных систем персональных данных проводится в отношении систем, позволяющих осуществлять обработку персональных данных с использованием средств автоматизации.

Состав и функциональное содержание методов и средств защиты зависит от вида и степени ущерба, возникающего вследствие реализации угроз безопасности персональных данных<sup>5</sup>.

В зависимости от объекта, причинение ущерба которому, в конечном счете, вызывается неправомерными действиями с персональными данными, рассматриваются два вида ущерба: непосредственный и опосредованный.

Непосредственный ущерб связан с причинением физического, материального, финансового или морального вреда непосредственно субъекту персональных данных. Он возникает за счет незаконного использования (в том числе распространения) персональных данных или за счет несанкционированной модификации этих данных и может проявляться в виде:

<sup>3</sup> п.6. Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных

<sup>4</sup> п.3. Порядка проведения классификации информационных систем персональных данных

<sup>5</sup> Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

Подп. и дата
Взам. инв. №
Инв. № дубл.
Подп. и дата
Инв. № подл.

Ли	Изм.	№ докум.	Подп.	Дат
----	------	----------	-------	-----



## 1.2 Порядок проведения классификации

Проведение классификации информационных систем персональных данных включает в себя два этапа<sup>6</sup>:

- сбор и анализ исходных данных по информационной системе;
- присвоение информационной системе соответствующего класса и его документальное оформление.

При проведении классификации информационной системы учитываются следующие исходные данные:

- категория обрабатываемых в информационной системе персональных данных;
- объем обрабатываемых персональных данных (количество субъектов персональных данных, персональные данные которых обрабатываются в информационной системе);
- заданные оператором характеристики безопасности персональных данных, обрабатываемых в информационной системе;
- структура информационной системы;
- наличие подключений информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена;
- режим обработки персональных данных;
- режим разграничения прав доступа пользователей информационной системы;
- местонахождение технических средств информационной системы.

<sup>6</sup> п.4. Порядка проведения классификации информационных систем персональных данных

Инв. № подл.	Подп. и дата	Инв. № дубл.	Взам. инв. №	Подп. и дата	Итого	Лист
Ли	Изм.	№ докум.	Подп.	Дат	Итого	8
ИСУ-4/2009-ОК						Лист

### 1.3 Критерии отнесения информационных систем к специальным

Информационные системы персональных данных подразделяются на типовые и специальные.

Типовые информационные системы – информационные системы, в которых требуется обеспечение только конфиденциальности персональных данных.

Критериями отнесения информационной системы к классу специальной информационной системы персональных данных являются:

- осуществление в информационной системе обработки персональных данных, касающихся состояния здоровья субъектов персональных данных;
- необходимость обеспечения в информационной системе хотя бы одной характеристики безопасности персональных данных, отличной от конфиденциальности (вне зависимости от необходимости обеспечения конфиденциальности);
- наличие в информационной системе функций, предусматривающих принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы.

Информационные системы, удовлетворяющие хотя бы одному из вышеперечисленных критериев, относятся к классу специальных информационных систем персональных данных.

Ине. № подл.	Подп. и дата	Ине. № дубл.	Взам. инв. №	Подп. и дата

Ли	Изм.	№ докум.	Подп.	Дат

## 2. ИНФОРМАЦИОННЫЕ СИСТЕМЫ ОПЕРАТОРОВ СВЯЗИ

### 2.1 Общие положения

В настоящем документе рассматриваются информационные системы операторов связи, в рамках которых осуществляется обработка персональных данных.

Под информационной системой персональных данных понимается информационная система, представляющая собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации.

Информационные системы операторов связи делятся на следующие категории:

#### 1) *Внутренние информационные системы*

К внутренним информационным системам относятся информационные системы, обеспечивающие технологический процесс оказания услуг связи:

– информационные системы услуг связи – информационные системы, обеспечивающие автоматизацию услуг связи<sup>7</sup>;

– информационные системы управления предприятием – информационные системы, обеспечивающие автоматизацию функций управления предприятием связи.

#### 2) *Информационные системы внешнего взаимодействия*

К информационным системам внешнего взаимодействия относятся информационные системы, входящие в состав информационно-технологической инфраструктуры оператора связи и обеспечивающие автоматизацию функций обмена информацией, с государственными и муниципальными органами, юридическими и физическими лицами, организующими и (или) осуществляющими обработку персональных данных, а также определяющими цели и содержание обработки персональных данных.

Ответственность за обеспечение требований по технической защите конфиденциальной информации (персональных данных)<sup>8</sup> возлагается на руководителей организаций, эксплуатирующих объекты информатизации<sup>9</sup>.

Инв. № подл.	Подп. и дата	Инв. № дубл.	Взам. инв. №	Подп. и дата	Ли	Изм.	№ докум.	Подп.	Дат	ICU-4/2009-ОК	Лист
											10





- величине задолженности абонента по оплате услуг связи;
- тарифам (тарифным планам);
- формирования массива данных с информацией по абонентам, имеющим задолженность по оплате услуг связи;
- информирования абонента, в случае использования им предварительного платежа за услуги связи, об уменьшении запаса денежных средств на его лицевом счете ниже определенного уровня, оговоренного договором об оказании услуг связи (при наличии технической возможности для реализации такой функции);
- регистрации исполнения оповещения абонентов об имеющейся задолженности по оплате услуг связи (в случае реализации функции оповещения абонентов средствами автоматизированной системы расчетов);
- настройки критериев, в соответствии с которыми абонент считается должником;
- формирования списков должников и ведомостей на временное ограничение доступа должников к услугам связи или сети связи.

К системам информационно-справочного обслуживания операторов связи относятся следующие информационные системы:

- автоматические системы самообслуживания абонентов;
- системы управления взаимоотношениями с клиентами.

***Автоматические системы самообслуживания абонентов***

Автоматические системы самообслуживания абонентов представляют собой информационные системы, предназначенные для управления набором услуг, предоставляемых абонентам, и дают возможность абоненту самостоятельно:

- получать справочную информацию;
- получать информацию о состоянии баланса;

<sup>13</sup> п. 18 Требований к функциям и техническим параметрам автоматизированной системы расчетов, предназначенной для автоматизации расчетов с абонентами

Ине. № подл	
Подп. и дата	
Ине. № дубл.	
Взам. инв. №	
Подп. и дата	

Ли	Изм.	№ докум.	Подп.	Дат	ICU-4/2009-OK

- подключать /отключать дополнительные услуги;
- изменять тарифный план;

**Системы управления взаимоотношениями с клиентами**

Системы управления взаимоотношениями с клиентами предназначены для автоматизации функций анализа данных о клиентах оператора связи (в том числе абонентах), экспорта информации (в том числе персональных данных) во взаимодействующие информационные системы, функций поддержки отношений с клиентами, и позволяют отслеживать развитие взаимоотношений с клиентами, координировать эти отношения, осуществлять централизованное управление предоставлением услуг связи.

**5) Системы интеграции**

Системы интеграции представляют собой технологии, позволяющие интегрировать корпоративную информацию, данные (включая персональные) и приложения, и охватывают все уровни корпоративной информационной системы – архитектуру, программное и аппаратное обеспечение, процессы.

Системы интеграции предназначены для решения широкого круга задач:

- Enterprise Application Integration (EAI) – технология, позволяющая решать задачи интеграции корпоративных приложений;
- Extract, Transform and Load (ETL) – технология, позволяющая преобразовывать данные (обычно с помощью их пакетной обработки) из операционной среды, включающей гетерогенные технологии, в интегрированные, согласующиеся между собой данные, пригодные для использования в процессе поддержки принятия решений. ETL-технология ориентирована на базы данных;
- Enterprise Information Integration (EII) – технология предназначенные для интеграции в режиме реального времени несопоставимых типов данных из многочисленных источников как внутри, так и за пределами предприятия.

**6) Системы записи вызовов**

Информационные системы записи вызовов представляют собой программно-аппаратные решения, предназначенные для выполнения функций записи, хранения, воспроизведения и анализа аудио и видео информации, получаемой, в основном, с автоматизированных рабочих мест операторов Call-центров.

Ине. № подл.	Подп. и дата
Ине. № дубл.	Взам. инв. №
Подп. и дата	Подп. и дата

Ли	Изм.	№ докум.	Подп.	Дат	ICU-4/2009-OK	Лист
						14

Информационные системы записи вызовов создаются операторами связи в целях осуществления контроля качества обслуживания абонентов.

**7) Автоматизированные рабочие места**

Автоматизированное рабочее место – программно-технический комплекс автоматизированной системы, предназначенный для автоматизации деятельности определенного вида<sup>14</sup>.

В целях обеспечения автоматизации деятельности предприятия связи, в части проведения расчетов с абонентами, приема и обработки платежей за услуги связи, информационно-справочного обслуживания, генерации выходных документов в соответствии с нормативно-правовыми и ведомственными актами по вопросам оказания услуг связи, администрирования информационных систем, операторами связи создаются автоматизированные рабочие места.

Автоматизированные рабочие места выделяются по функционально-технологическому принципу:

– автоматизированные рабочие места администраторов – программно-технические комплексы, предназначенные для автоматизации функций администрирования информационных систем персональных данных операторов связи;

– автоматизированные рабочие места пользователей – программно-технические комплексы, предназначенные для автоматизации деятельности сотрудников оператора связи, доступ которых к персональным данным, обрабатываемым в информационных системах, необходим для выполнения служебных (трудовых) обязанностей.

**8) Сети связи**

Сеть связи - технологическая система, включающая в себя средства и линии связи и предназначенная для электросвязи или почтовой связи<sup>15</sup>.

Средства связи представляют собой технические и программные средства, используемые для формирования, приема, обработки, хранения, передачи, доставки сообщений электросвязи или почтовых отправлений, а также иные технические и

<sup>14</sup> ГОСТ 34.003-90.

<sup>15</sup> Ст.2, п.24, 126-ФЗ «О связи»

Ине. № подл.	Подп. и дата
Ине. № дубл.	Взам. инв. №
Подп. и дата	Подп. и дата

Ли	Изм.	№ докум.	Подп.	Дат
----	------	----------	-------	-----

ICU-4/2009-OK				
---------------	--	--	--	--

программные средства, используемые при оказании услуг связи или обеспечении функционирования сетей связи<sup>16</sup>.

Линии связи - линии передачи, физические цепи и линейно-кабельные сооружения связи<sup>17</sup>.

В настоящем Классификаторе, под сетью связи понимается технологическая система, включающая в себя линии связи и технические и программные средства, используемые для формирования, приема, обработки, хранения, передачи, доставки сообщений электросвязи.

Электросвязь - любое излучение, передача или прием знаков, сигналов, голосовой информации, письменного текста, изображений, звуков или сообщений любого рода по радиосистеме, проводной, оптической и другим электромагнитным системам<sup>18</sup>.

Требования по защите сетей связи от несанкционированного доступа к ним и передаваемой посредством их информации утверждены приказом Министерства информационных технологий и связи Российской Федерации от 09.01.2008 №1.

Цели, задачи, принципы и основные положения обеспечения безопасности сетей электросвязи определены ГОСТ Р 52448-2005. Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения.

## 2.2.2 Информационные системы управления предприятием

### 1) Системы управления персоналом организации связи

Организацией связи является юридическое лицо, осуществляющее деятельность в области связи в качестве основного вида деятельности<sup>19</sup>.

Информационные системы управления персоналом организации связи, предназначены для автоматизации функций управления, основными из которых являются подбор, оценка, развитие и стимулирование работников.

В рамках функционирования данных систем осуществляется обработка персональных данных работников организации связи<sup>20</sup>.

<sup>16</sup> Ст.2, п.28, 126-ФЗ «О связи»

<sup>17</sup> Ст.2, п.7, 126-ФЗ «О связи»

<sup>18</sup> Ст.2, п.35, 126-ФЗ «О связи»

<sup>19</sup> Ст.2, п.14, 126-ФЗ «О связи»

<sup>20</sup> Обработка персональных данных работника - получение, хранение, комбинирование, передача или любое другое использование персональных данных работника (ст. 85. ТК РФ).

Ине. № подл.	Подп. и дата	Ине. № дубл.	Взам. инв. №	Подп. и дата	Ли	Изм.	№ докум.	Подп.	Дат	ИСУ-4/2009-ОК	Лист
											16

Защита персональных данных работников регламентируется гл. 14 Трудового кодекса Российской Федерации.

**2) Системы финансового учета**

Системы финансового учета представляют собой инструмент контроля и управления финансовыми данными организации связи.

В настоящем документе системы финансового учета рассматриваются как информационные системы, в рамках которых осуществляется обработка персональных данных работников организации связи – системы, выполняющие функции автоматизации расчета заработной платы.

**3) Системы контроля и управления доступом**

В целях защиты от несанкционированного доступа к сетям связи и передаваемой посредством их информации операторы связи принимают организационные и технические меры, направленные на предотвращение доступа к линиям связи, сооружениям связи, средствам связи, находящимся как внутри, так и вне сооружений связи, и передаваемой по сетям связи информации, осуществляемого с нарушением установленного этими операторами связи порядка доступа<sup>21</sup>.

Сооружениями связи являются объекты инженерной инфраструктуры, в том числе здания, строения, созданные или приспособленные для размещения средств связи и кабелей электросвязи<sup>22</sup>.

В целях выполнения Требований по защите сетей связи от несанкционированного доступа к ним и передаваемой посредством их информации, утвержденных приказом Министерства информационных технологий и связи Российской Федерации от 09.01.2008 №1, операторы связи оснащают сооружения связи средствами контроля доступа (системами контроля и управления доступом).

Системы контроля и управления доступом представляют собой совокупность средств контроля и управления доступом, обладающих технической, информационной, программной и эксплуатационной совместимостью<sup>23</sup>.

Средства управления – аппаратные средства (устройства) и программные средства, обеспечивающие установку режимов доступа, прием и обработку

<sup>21</sup> п.2. Требований по защите сетей связи от несанкционированного доступа к ним и передаваемой посредством их информации.  
<sup>22</sup> ст.2, п.27, 126-ФЗ «О связи»

Ине. № подл.	Подп. и дата
Ине. № дубл.	Взам. инв. №
Подп. и дата	Подп. и дата

Ли	Изм.	№ докум.	Подп.	Дат	ИСУ-4/2009-ОК	Лист
						17

информации со считывателей, проведение идентификации и аутентификации, управление исполнительными и преграждающими устройствами, отображение и регистрацию информации<sup>24</sup>.

В состав систем контроля и управления доступом могут входить дополнительные средства<sup>25</sup>:

– источники электропитания: датчики (извещатели) состояния преграждающих устройств, дверные доводчики, световые и звуковые оповещатели, кнопки ручного управления преграждающих устройств, устройства преобразования интерфейсов сетей связи: аппаратура передачи данных по различным каналам связи и другие устройства, предназначенные для обеспечения работы систем контроля и управления доступом;

– аппаратно-программные средства: средства вычислительной техники общего назначения (компьютерное оборудование, оборудование для компьютерных сетей, общее программное обеспечение).

#### **4) Системы обнаружения мошенничества**

В каждой организации связи должна создаваться система обеспечения информационной безопасности для осуществления мероприятий и действий по снижению потенциального ущерба от реализации угроз безопасности до приемлемого уровня за счет устранения уязвимостей в сетях и средствах связи или существенного затруднения использования этих уязвимостей нарушителями безопасности<sup>26</sup>.

Мошенничество является одной из основных возможных угроз безопасности сетей электросвязи<sup>27</sup>.

Система обеспечения информационной безопасности сети (сетей) электросвязи предусматривает<sup>28</sup>:

– обеспечение безопасности персональных данных, сведений об абонентах и предоставляемых им услугах связи;

<sup>23</sup> ГОСТ Р 51241-2008

<sup>24</sup> ГОСТ Р 51241-2008

<sup>25</sup> ГОСТ Р 51241-2008

<sup>26</sup> ГОСТ Р 53110-2008

<sup>27</sup> ГОСТ Р 52448-2005

<sup>28</sup> ГОСТ Р 53110-2008

Ине. № подл.	Подп. и дата	Ине. № дубл.	Взам. инв. №	Подп. и дата

Ли	Изм.	№ докум.	Подп.	Дат	ИСУ-4/2009-ОК	Лист
						18

- разработка политики борьбы с мошенничеством (фрод менеджмент), как со стороны внешних злоумышленников, так и со стороны собственного персонала;
- развертывание на сети связи системы обнаружения мошенничества, направленной на защиту доходов оператора и мониторинг незапланированных потерь;
- мониторинг деятельности и событий, связанных со счетами клиентов и с оплатами счетов.

Использование автоматизированных систем обнаружения мошенничества позволяют операторам связи обнаруживать случаи мошенничества и успешно бороться с ними.

#### **5) Внутренние информационно-справочные системы**

Операторами связи создаются внутренние информационно-справочные системы (корпоративные справочники, адресные книги), содержащие данные, предназначенные для общего доступа в рамках организации (предприятия) связи.

Создание таких информационных систем обусловлено необходимостью информационного обеспечения организации (предприятия) связи.

### **2.3 Информационные системы внешнего взаимодействия**

#### **1) Системы взаимодействия с бюро кредитных историй**

Взаимодействие с бюро кредитных историй осуществляется в соответствии с Федеральным законом от 30.12.2004 г. №218-ФЗ «О кредитных историях».

Бюро кредитных историй обеспечивает защиту информации при ее обработке, хранении и передаче сертифицированными средствами защиты в соответствии с законодательством Российской Федерации<sup>29</sup>.

Источники формирования кредитной истории представляют информацию, в бюро кредитных историй на основании заключенного договора об оказании информационных услуг. Допускается заключение договора об оказании информационных услуг с несколькими бюро кредитных историй<sup>30</sup>.

<sup>29</sup> Ст. 7, ч.2. 218-ФЗ «О кредитных историях»

<sup>30</sup> Ст. 5, ч.1. 218-ФЗ «О кредитных историях»

Инв. № подл.	Подп. и дата				Инв. № дубл.	Взам. инв. №	Подп. и дата	Инв. № подл.	Подп. и дата	ИСУ-4/2009-ОК	Лист
	19										
Ли	Изм.	№ докум.	Подп.	Дат							



Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

Изм.	
Лист	
№ докум.	
Подп.	
Дата	

Таблица 2.1 – Информационные системы персональных данных операторов связи

Русское наименование	Английское наименование	Сокращение
<b>1. Внутренние информационные системы</b>		
<b>1.1. Информационные системы услуг связи</b>		
1.1.1. Автоматизированные системы расчетов	Billing Systems	ACP
1.1.2. Системы управления взаимоотношениями с дилерами	Dealer Management Systems	DMS
1.1.3. Системы печати счетов	Enterprise Printing Systems	EPS
<b>1.1.4. Системы информационно-справочного обслуживания</b>		
1.1.4.1. Автоматические системы самообслуживания абонентов	Automatic Customer Care Systems	ACCS
1.1.4.2. Системы управления взаимоотношениями с клиентами	Customer Relationship Management Systems	CRM
1.1.5. Системы интеграции	Integration Systems	IntS
1.1.6. Системы записи вызовов	Call Recording Systems	CRS
<b>1.1.7. Автоматизированные рабочие места</b>		
1.1.7.1. Автоматизированные рабочие места администраторов	Automated Workplaces <sup>32</sup> of Administrators	APM.A
1.1.7.2. Автоматизированные рабочие места пользователей	Automated Workplaces of Users	APM.П
1.1.8. Сети связи	Networks Communications	NetComm
<b>1.2. Информационные системы управления предприятием</b>		
1.2.1. Системы управления персоналом организации связи	Human Resource Management Systems	HRMS
1.2.2. Системы финансового учета	Financial Management Systems	FinMS
1.2.3. Системы контроля и управления доступом	Access Control Systems	СКУД
1.2.4. Системы обнаружения мошенничества	Fraud Management Systems	FMS
1.2.5. Внутренние информационно-справочные системы	Information Resource Dictionary Systems <sup>33</sup>	IRDS
<b>2. Информационные системы внешнего взаимодействия</b>		
2.1. Системы взаимодействия с бюро кредитных историй	Credit History Agency Systems	СБКИ
2.2. Системы оперативно-розыскных мероприятий	Lawful Interception Systems	COPM

ISU-4/2009-OK

<sup>32</sup> Рекомендации по стандартизации. Р50.1.053-2005

<sup>33</sup> ГОСТ Р ИСО/МЭК 10027-93

### 3. СУБЪЕКТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

#### 3.1 Категории субъектов персональных данных. Цели обработки персональных данных

Субъектами персональных данных являются физические лица<sup>34</sup>.

Операторами связи являются юридические лица или индивидуальные предприниматели, оказывающие услуги связи на основании соответствующих лицензий<sup>35</sup>.

Субъекты, персональные данные которых обрабатываются в информационных системах операторов связи, делятся на две категории (Таблица 3.1):

**1) Пользователи услугами связи – физические лица, заказывающее и (или) использующее услуги связи<sup>36</sup>**

К данной категории относятся абоненты – пользователи услугами связи, с которыми заключены договоры об оказании таких услуг при выделении для этих целей абонентского номера или уникального кода идентификации<sup>37</sup>.

**2) Физические лица, обработка персональных данных которых осуществляется в рамках технологического процесса оказания услуг связи**

К данной категории относятся:

– *работники* – физические лица, вступившие в трудовые отношения с работодателем<sup>38</sup> (оператором связи);

– *пользователи систем контроля и управления доступом* – физические лица, в отношении которых осуществляются мероприятия по контролю доступа на защищаемые объекты оператора связи<sup>39</sup>.

<sup>34</sup> 152-ФЗ «О персональных данных»

<sup>35</sup> Ст.2, п.12, 126-ФЗ «О связи»

<sup>36</sup> Ст.2, п.16, 126-ФЗ «О связи»

<sup>37</sup> Ст.2, п.1, 126-ФЗ «О связи»

<sup>38</sup> Ст. 20, ТК РФ

<sup>39</sup> П.3.20. ГОСТ Р 53110-2008

Ине. № подл	Подп. и дата	Ине. № дубл.	Взам. инв. №	Подп. и дата

Таблица 3.1 – Категории субъектов, персональные данные которых обрабатываются в информационных системах операторов связи. Цели обработки персональных данных.

Категория субъекта ПДн	Цели обработки ПДн
<b>1. Пользователи услугами связи</b>	
1.1. Абоненты	Исполнение договоров об оказании услуг связи <sup>40</sup>
<b>2. Физические лица, обработка персональных данных которых осуществляется в рамках технологического процесса оказания услуг связи</b>	
2.1. Работники	Обеспечение соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества <sup>41</sup>
2.2. Пользователи систем контроля и управления доступом	Предоставление однократного и (или) неоднократного пропуска субъектов персональных данных на территорию, на которой находится Оператор связи или в иных аналогичных целях <sup>42</sup>

*Примечание.* Настоящий перечень субъектов персональных данных не является конечным и может быть расширен по мере развития бизнес-процессов операторов связи и предоставляемых услуг.

### 3.2 Перечни персональных данных субъектов персональных данных

Субъект персональных данных имеет право на получение сведений, о наличии у оператора, персональных данных, относящихся к соответствующему субъекту персональных данных, а также на ознакомление с такими персональными данными<sup>43</sup>.

Настоящий раздел содержит сведения о составе персональных данных для каждой из категорий субъектов, персональные данные которых обрабатываются в информационных системах операторов связи.

#### **Абоненты**

К сведениям об абонентах относятся фамилия, имя, отчество или псевдоним абонента-гражданина, наименование (фирменное наименование) абонента - юридического лица, фамилия, имя, отчество руководителя и работников этого юридического лица, а также адрес абонента или адрес установки окончного оборудования, абонентские номера и другие данные, позволяющие идентифицировать абонента или его окончное оборудование, сведения баз данных

<sup>40</sup> Ст. 53, 126-ФЗ «О связи»

<sup>41</sup> Ст. 86, ТК РФ

<sup>42</sup> Ст. 22, ч.2, п. 6, 152-ФЗ «О персональных данных»

Ине. № подл	Подп. и дата	Ине. № дубл.	Взам. инв. №	Подп. и дата

Ли	Изм.	№ докум.	Подп.	Дат	ИСУ-4/2009-ОК	Лист 23

систем расчета за оказанные услуги связи, в том числе о соединениях, трафике и платежах абонента<sup>44</sup>.

### **Работники**

Персональные данные работника - информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника<sup>45</sup>.

Персональные данные работников обрабатываются операторами связи, в объеме, установленном ст. 65 Трудового кодекса Российской Федерации – при заключении трудового договора лицо, поступающее на работу, предъявляет работодателю:

- паспорт или иной документ, удостоверяющий личность;
- трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или работник поступает на работу на условиях совместительства;
- страховое свидетельство государственного пенсионного страхования;
- документы воинского учета - для военнообязанных и лиц, подлежащих призыву на военную службу;
- документ об образовании, о квалификации или наличии специальных знаний - при поступлении на работу, требующую специальных знаний или специальной подготовки.

Запрещается требовать от лица, поступающего на работу, документы помимо предусмотренных Трудовым кодексом, иными федеральными законами, указами Президента Российской Федерации и постановлениями Правительства Российской Федерации.

### **Пользователи систем контроля и управления доступом**

В состав персональных данных пользователей систем контроля и управления доступом входят:

- сведения о личности владельца паспорта<sup>46</sup>:

<sup>43</sup> Ст. 14, ч.1, 152-ФЗ «О персональных данных»

Инва. № подл.	Подп. и дата
Инва. № дубл.	Взам. инв. №
Подп. и дата	Подп. и дата

- фамилия;
  - имя;
  - отчество;
  - пол;
  - дата рождения;
  - место рождения.
- цифровая фотография владельца паспорта.

### 3.3 Категории персональных данных субъектов персональных данных

В соответствии с порядком проведения классификации информационных систем персональных данных, утвержденным приказом Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации, Министерства информационных технологий и связи Российской Федерации от 13.02.2008 г. №55/86/20, определяются следующие категории обрабатываемых в информационных системах персональных данных:

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 персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1;

категория 3 - персональные данные, позволяющие идентифицировать субъекта персональных данных;

категория 4 - обезличенные и (или) общедоступные персональные данные.

<sup>44</sup> Ст. 53, п.1. 126-ФЗ «О связи»  
<sup>45</sup> Ст. 85. ТК РФ  
<sup>46</sup> «Описание бланка паспорта гражданина Российской Федерации»

Подп. и дата	
Взам. инв. №	
Инв. № дубл.	
Подп. и дата	
Инв. № подл.	

Обработка персональных данных осуществляться операторами связи на основе принципов, изложенных в 152-ФЗ «О персональных данных», определяющих соответствие объема и характера обрабатываемых персональных данных целям обработки персональных данных.

В соответствии с целями обработки персональных данных субъектов персональных данных (Таблица 3.1), операторами связи не осуществляется обработка специальных категорий персональных данных касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, судимости<sup>47</sup>;

В информационных системах операторов связи может осуществляться обработка персональных данных субъектов персональных данных 2-ой, 3-ей и 4-ой категорий.

Инв. № подл.	Подп. и дата	Инв. № дубл.	Взам. инв. №	Подп. и дата

<sup>47</sup> В соответствии со ст.10, ч.4, 152-ФЗ «О персональных данных»: обработка специальных категорий персональных данных должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась обработка.

Инв. № подл.	Подп. и дата	Инв. № дубл.	Взам. инв. №	Подп. и дата	ICU-4/2009-OK	Лист 26
Ли	Изм.	№ докум.	Подп.	Дат		

## 4. СБОР И АНАЛИЗ ИСХОДНЫХ ДАННЫХ

### 4.1 Общие положения

Исходные данные на информационные системы собираются в объеме, установленном порядком проведения классификации информационных систем персональных данных (см. п. 1.2 настоящего документа).

Исходные данные на информационные системы персональных данных операторов связи, приведенные в настоящем разделе, являются результатом обобщения сведений, полученных в ходе комплексного обследования информационных систем трех операторов сотовой подвижной связи: ОАО «ВымпелКом», ОАО «Мобильные ТелеСистемы», ОАО «МегаФон».

В настоящем Классификаторе (разделы 4.2 и 4.3) детально рассматриваются следующие исходные данные на информационные системы персональных данных операторов связи: категории обрабатываемых в информационных системах персональных данных; объем обрабатываемых персональных данных; характеристики безопасности персональных данных (Таблица 4.1 настоящего документа).

Исходные данные, такие как: структура информационных систем; наличие подключений к сетям связи общего пользования и (или) сетям международного информационного обмена; режим обработки персональных данных; режим разграничения прав доступа пользователей, местонахождение технических средств, являются идентичными для всех рассматриваемых информационных систем персональных данных операторов связи и имеют следующие значения:

- по структуре информационные системы персональных данных операторов связи являются локальными информационными системами, состоящими из комплекса технических и программных средств, предназначенных для обработки персональных данных, и функционирующих в доверенной среде эксплуатации (среде, в которой приняты необходимые организационно-технические меры, направленные на поддержание заданного уровня безопасности);
- информационные системы персональных данных операторов связи не имеют подключений к сетям связи общего пользования и (или) сетям международного информационного обмена;

Исх. № подл.	Подп. и дата	Исх. № дубл.	Взам. исх. №	Подп. и дата	Исх. № подл.	Лист
	Исх. № подл.					
Ли	Изм.	№ докум.	Подп.	Дат	Исх. № подл.	Исх. № подл.
ИСУ-4/2009-ОК						27

- информационные системы персональных данных операторов связи являются многопользовательскими информационными системами;
- информационные системы персональных данных операторов связи являются системами с разграничением прав доступа;
- все технические средства информационных систем персональных данных операторов связи находятся в пределах Российской Федерации.

Далее рассматриваются категории обрабатываемых в информационных системах персональных данных; объем обрабатываемых персональных данных; характеристики безопасности персональных данных.

## 4.2 Внутренние информационные системы

### 4.2.1 Информационные системы услуг связи

#### *Автоматизированные системы расчетов (1.1.1)*

#### Категория персональных данных

Автоматизированные системы расчетов обеспечивают выполнение учета и хранения сведений об абонентах, необходимых и достаточных для однозначной идентификации абонентов, тарификации и расчета стоимости оказанных им услуг связи, расчета неустойки (пени), формирования платежных документов, контроля доставки абонентам платежных документов, регистрации и контроля платежей, информационно-справочного обслуживания абонентов, регистрации и обработки претензий по расчетам за услуги связи<sup>48</sup>.

Автоматизированная система расчетов обеспечивает возможность регистрации (формирования) и хранения для каждого абонента следующей информации<sup>49</sup>:

- не менее двух идентификационных признаков лицевого счета (по отдельности или в совокупности), являющихся уникальными;
- регистрационных данных договора (договоров) об оказании услуг связи: уникального номера (номеров), начала действия, срока окончания действия или условий прекращения оказания услуг, тарифного плана;

<sup>48</sup> п.6, Требований к функциям и техническим параметрам автоматизированных систем расчетов, предназначенных для автоматизации расчетов с абонентами.

<sup>49</sup> п.1, Требований к функциям и техническим параметрам автоматизированных систем расчетов, предназначенных для автоматизации расчетов с абонентами.

Инв. № подл.	
Подп. и дата	
Инв. № дубл.	
Взам. инв. №	
Подп. и дата	

Ли	Изм.	№ докум.	Подп.	Дат	ICU-4/2009-OK

- перечня назначенных абоненту абонентских номеров и (или) уникальных кодов идентификации;
- номеров SIM-карт (при их наличии);
- вида (типа) пользовательского (оконечного) оборудования (при наличии);
- сведений об абоненте (фамилия, имя, отчество, дата и место рождения, место жительства и реквизиты основного документа, удостоверяющего личность, – для гражданина, наименование (фирменное наименование) юридического лица, его место нахождения (место государственной регистрации) – для юридического лица);
- признака, отражающего согласие абонента на доступ к услугам междугородной и международной телефонной связи;
- признака, отражающего способ выбора операторов сетей междугородной и международной телефонной связи, определенного абонентом при заключении договора об оказании услуг связи;
- идентификационного признака оператора междугородной и международной телефонной связи, который определен абонентом для получения услуг междугородной и международной телефонной связи (в случае предварительного выбора оператора связи);
- признака, отражающего выбор тарифного плана;
- данных для начисления налогов (при необходимости);
- уникальных номеров или номеров лицевого счета (при отдельных начислениях за оказываемые услуги) абонента;
- сведений, необходимых для доставки счетов абоненту.

Категория персональных данных – 2. Дополнительной информацией, неправомерный доступ к которой может привести к непосредственному ущербу субъекту персональных данных, является детализация счета с указанием даты и времени состоявшихся соединений, их продолжительности и абонентских номеров.

Инд. № подл.	
Подп. и дата	
Инд. № дубл.	
Взам. инв. №	
Подп. и дата	

Ли	Изм.	№ докум.	Подп.	Дат	ICU-4/2009-OK

Автоматизированная система расчетов обеспечивает формирование платежных документов для наличной и безналичной оплаты в соответствии с действующим законодательством<sup>50</sup>.

Автоматизированная система расчетов обеспечивает целостность и доступность хранимой, обрабатываемой и передаваемой информации<sup>51</sup>.

Автоматизированная система расчетов обеспечивает достоверность расчетов на не менее чем 99,99%<sup>52</sup>.

В соответствии со ст.7, 152-ФЗ от 27.07.2006 г. «О персональных данных», операторами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных, за исключением обезличенных и общедоступных персональных данных.

Необходимость обеспечения целостности, доступности и достоверности персональных данных, а также наличие в информационной системе функций, предусматривающих принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных (формирование платежных документов), соответствует критериям отнесения информационной системы к специальной (см. раздел 1.3 настоящего документа).

**Системы управления взаимоотношениями с дилерами (1.1.2)**

*Категория персональных данных*

Перечень персональных данных, определяется содержанием договоров об оказании услуг связи.

Гражданин представляет оператору связи документ, удостоверяющий личность<sup>53</sup>.

В договоре должны быть указаны следующие данные<sup>54</sup>:

<sup>50</sup> п.12, Требований к функциям и техническим параметрам автоматизированных систем расчетов, предназначенных для автоматизации расчетов с абонентами.

<sup>51</sup> п.21, Требований к функциям и техническим параметрам автоматизированных систем расчетов, предназначенных для автоматизации расчетов с абонентами.

<sup>52</sup> п.29, Требований к функциям и техническим параметрам автоматизированных систем расчетов, предназначенных для автоматизации расчетов с абонентами.

<sup>53</sup> п.18, Правил оказания услуг подвижной связи

<sup>54</sup> п.19, Правил оказания услуг подвижной связи

Ине. № подл.	Подп. и дата
Ине. № дубл.	Взам. инв. №
Подп. и дата	
Ине. № подл.	

- сведения об абоненте (фамилия, имя, отчество, место жительства, реквизиты документа, удостоверяющего личность);
- согласие (отказ) абонента на предоставление доступа к услугам связи, оказываемым другим оператором связи, и предоставление сведений о нем для оказания таких услуг;
- номер SIM-карты;
- согласие (отказ) абонента на использование сведений о нем в системе информационно-справочного обслуживания;
- способ доставки счета.

В договоре должны быть указаны следующие существенные условия<sup>55</sup>:

- назначенный абоненту абонентский номер из выделенного оператору связи ресурса нумерации географически не определяемой зоны нумерации или уникальный код идентификации;
- оказываемые услуги подвижной связи;
- порядок, сроки и форма расчетов;
- система оплаты услуг подвижной связи.

Категория персональных данных – 3. Данные, содержащиеся в договоре об оказании услуг связи, позволяют однозначно идентифицировать субъекта персональных данных и не содержат дополнительной информации о нем.

Характеристики безопасности ПДн

В соответствии со ст.7, 152-ФЗ от 27.07.2006 г. «О персональных данных», операторами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных, за исключением обезличенных и общедоступных персональных данных.

При заключении договоров об оказании услуг связи (сбор персональных данных), операторами связи и третьими лицами, которым оператор вправе поручить

<sup>55</sup> п.20, Правил оказания услуг подвижной связи

Ине. № подл	Подп. и дата
Ине. № дубл.	Взам. инв. №
Подп. и дата	Подп. и дата

Ли	Изм.	№ докум.	Подп.	Дат	ICU-4/2009-OK	Лист 31

заключение договоров от своего имени, проверяется достоверность предоставляемых персональных данных.

При передаче данных, содержащихся в договорах об оказании услуг связи (в том числе персональных данных), для их последующей регистрации в автоматизированных системах расчетов, необходимо обеспечить целостность этих данных.

### **Системы печати счетов (1.1.3)**

#### Категория персональных данных

Перечень персональных данных, обрабатываемых в системах печати счетов, определяется требованиями к содержанию счета.

Для проведения расчетов за оказанные услуги подвижной связи абоненту выставляется счет, который должен содержать следующие сведения<sup>56</sup>:

- реквизиты оператора связи;
- сведения об абоненте;
- расчетный период, за который выставляется счет;
- номер лицевого счета абонента (при авансовой системе оплаты);
- виды оказанных услуг подвижной связи с указанием объема услуг подвижной связи по каждому виду;
- сумма, предъявляемая к оплате, по каждому виду услуг подвижной связи и каждому абонентскому номеру абонента;
- общая сумма, предъявляемая к оплате;
- сумма остатка на лицевом счете (при авансовой системе оплаты);
- дата выставления счета;
- срок оплаты счета (если для этого платежа он установлен оператором связи).

<sup>56</sup> п.42, Правил оказания услуг подвижной связи

Ине. № подл.	Подп. и дата
Ине. № дубл.	Взам. инв. №
Подп. и дата	Ине. № дубл.
Ине. № подл.	Подп. и дата

Ли	Изм.	№ докум.	Подп.	Дат
----	------	----------	-------	-----

Основанием для выставления счета абоненту за предоставленные соединения по сети подвижной связи являются данные, полученные с помощью оборудования учета объема оказанных услуг подвижной связи<sup>57</sup>.

Категория персональных данных – 2. Дополнительной информацией, неправомерный доступ к которой может привести к непосредственному ущербу субъекту персональных данных, является детализация счета.

Характеристики безопасности ПДн

В соответствии со ст.7, 152-ФЗ от 27.07.2006 г. «О персональных данных», операторами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных, за исключением обезличенных и общедоступных персональных данных.

Данные, содержащиеся в счетах за оказанные услуги связи, должны удовлетворять условию целостности.

**Автоматические системы самообслуживания абонентов (1.1.4.1)**

Категория персональных данных

Автоматические системы самообслуживания абонентов создаются операторами связи в целях оказания информационно-справочных услуг и управления набором услуг, предоставляемых абонентам.

Оператор связи оказывает бесплатно и круглосуточно следующие информационно-справочные услуги<sup>58</sup>:

- выдает информацию о тарифах на услуги, о зоне обслуживания сети подвижной связи;
- выдает информацию абоненту о состоянии его лицевого счета и о задолженности по оплате услуг подвижной связи;
- осуществляет прием информации от абонента о технических неисправностях, препятствующих пользованию услугами подвижной связи.

Перечень бесплатных информационно-справочных услуг не может быть сокращен.

<sup>57</sup> п.37, Правил оказания услуг подвижной связи  
<sup>58</sup> п.12, Правил оказания услуг подвижной связи

Инва. № подл	
Подп. и дата	
Инва. № дубл.	
Взам. инв. №	
Подп. и дата	

Ли	Изм.	№ докум.	Подп.	Дат	ICU-4/2009-ОК

Персональные данные, обрабатываемые в автоматических системах самообслуживания абонентов являются обезличенными и не позволяют идентифицировать субъекта персональных данных.

Характеристики безопасности ПДн

Предоставление возможности удаленного управления услугами, требует соблюдения условий конфиденциальности.

Круглосуточное предоставление информационно-справочных услуг, требует выполнение условий доступности автоматических систем самообслуживания абонентов и данных, обрабатываемых в этих системах.

**Системы управления взаимоотношениями с клиентами (1.1.4.2)**

Категория персональных данных

Информационные системы управления взаимоотношениями с клиентами, являются системами аккумулирующими данные (в том числе персональные) из взаимодействующих информационных систем персональных данных, предназначенных для обеспечения технологического процесса оказания услуг связи (внутренних информационных систем операторов связи).

В информационных системах управления взаимоотношениями с клиентами могут обрабатываться персональные данные любой из категорий персональных данных, обрабатываемых операторами связи. Такими категориями являются 2, 3 и 4. (см. раздел «[Категории персональных данных субъектов персональных данных](#)» настоящего документа).

Характеристики безопасности ПДн

В соответствии со ст.7, 152-ФЗ от 27.07.2006 г. «О персональных данных», операторами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных, за исключением обезличенных и общедоступных персональных данных.

В целях поддержания доступности и качества оказываемых операторами связи услуг, информационные системы управления взаимоотношениями с клиентами, предназначенные для централизованного управления предоставляемыми услугами связи, должны обеспечивать целостность и доступность обрабатываемых персональных данных.

Инва. № подл.	
Подп. и дата	
Инва. № дубл.	
Взам. инв. №	
Подп. и дата	

Ли	Изм.	№ докум.	Подп.	Дат	ICU-4/2009-ОК

### **Системы интеграции (1.1.5)**

#### Категория персональных данных

Системы интеграции представляют собой технологии, позволяющие интегрировать данные (включая персональные) и могут содержать (обрабатывать) персональные данные любой из категорий персональных данных, обрабатываемых операторами связи. Такими категориями являются 2, 3 и 4. (см. раздел «[Категории персональных данных субъектов персональных данных](#)» настоящего документа).

#### Характеристики безопасности ПДн

В целях обеспечения конфиденциальности, целостности и доступности персональных данных, обрабатываемых в других информационных системах персональных данных операторов связи, системы интеграции также должны обеспечивать конфиденциальность, целостность и доступность таких данных.

### **Системы записи вызовов (1.1.6)**

#### Категория персональных данных

В информационных системах записи вызовов обрабатывается аудио и видео информация, получаемая, с автоматизированных рабочих мест пользователей (в основном операторов Call-центров).

В информационных системах записи вызовов могут обрабатываться персональные данные любой из категорий персональных данных, обрабатываемых операторами связи. Такими категориями являются 2, 3 и 4. (см. раздел «[Категории персональных данных субъектов персональных данных](#)» настоящего документа).

#### Характеристики безопасности ПДн

В соответствии со ст.7, 152-ФЗ от 27.07.2006 г. «О персональных данных», операторами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных, за исключением обезличенных и общедоступных персональных данных.

Информационные системы записи вызовов создаются в целях осуществления контроля качества обслуживания абонентов и не требуют обеспечения характеристик безопасности персональных данных, отличных от конфиденциальности.

Ине. № подл.	Подп. и дата
Ине. № дубл.	Взам. инв. №
Подп. и дата	

Ли	Изм.	№ докум.	Подп.	Дат	ICU-4/2009-ОК

## **Автоматизированные рабочие места (1.1.7.1, 1.1.7.2)**

### Категория персональных данных

Автоматизированные рабочие места, предназначенные для взаимодействия с другими информационными системами персональных данных операторов связи, могут содержать (обрабатывать) персональные данные любой из категорий персональных данных, обрабатываемых операторами связи. Такими категориями являются 2, 3 и 4. (см. раздел «[Категории персональных данных субъектов персональных данных](#)» настоящего документа).

### Характеристики безопасности ПДн

В соответствии со ст.7, 152-ФЗ от 27.07.2006 г. «О персональных данных», операторами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных, за исключением обезличенных и общедоступных персональных данных.

В целях поддержания доступности оказываемых операторами связи услуг, автоматизированные рабочие места, предназначенные для автоматизации функций администрирования информационных систем персональных данных операторов связи, должны отвечать требованиям доступности.

Автоматизированные рабочие места пользователей, должны обеспечивать целостность обрабатываемых персональных данных.

## **Сети связи (1.1.8)**

### Категория персональных данных

К информационным ресурсам сетей электросвязи, требующим защиты со стороны оператора связи, могут быть отнесены<sup>59</sup>:

- информация управления;
- данные, содержащие информацию пользователей (обеспечение доступности и целостности);
- программное обеспечение систем управления сетями электросвязи;
- сведения о прохождении, параметрах, загрузке (использовании) линий связи магистральных сетей;

<sup>59</sup> п. 5.1, ГОСТ Р 52448-2005

Ине. № подл	Подп. и дата
Ине. № дубл.	Взам. инв. №
Подп. и дата	Подп. и дата

Ли	Изм.	№ докум.	Подп.	Дат	ИСУ-4/2009-ОК	Лист
						36

- обобщенные сведения о местах дислокации узлов связи и установленном сетевом оборудовании;
- сведения, раскрывающие структуру используемых механизмов обеспечения безопасности сети электросвязи.

К персональным данным, обрабатываемым в сети электросвязи, относятся данные о совершенных и принятых субъектами персональных данных вызовах.

Категория персональных данных – 4. Данные, не позволяющие определить принадлежность персональных данных конкретному субъекту персональных данных (обезличенные персональные данные).

*Характеристики безопасности ПДн*

Открытость сетей электросвязи не должна означать полную доступность ко всем ее информационным ресурсам и отсутствие контроля их использования. В сети электросвязи должна быть обеспечена защита собственной, служебной информации, предназначенной для управления работой сети или служб сети<sup>60</sup>.

Безопасность сети электросвязи характеризуется основными ее критериями<sup>61</sup>:

- конфиденциальностью инфокоммуникационной структуры сети электросвязи;
- целостностью информации и услуг связи;
- доступностью информации и услуг связи;
- подотчетностью действий в сети.

Под конфиденциальностью инфокоммуникационной структуры сети электросвязи понимают свойство, позволяющее ограничить несанкционированный доступ к инфокоммуникационной структуре сети электросвязи и/или не раскрывать содержания информационных ресурсов сети неуполномоченным лицам, объектам или процессам.

Нарушение конфиденциальности - несанкционированное раскрытие информации управления, персональных данных пользователей и др.

<sup>60</sup> п. 5.1, ГОСТ Р 52448-2005  
<sup>61</sup> п. 5.12, ГОСТ Р 52448-2005

Ине. № подл	Подп. и дата	Ине. № дубл.	Взам. инв. №	Подп. и дата

Под целостностью информации и услуг связи понимают состояние сети электросвязи, при котором обеспечивается неизменность информации и доступность услуг связи для пользователей, независимо от преднамеренного или случайного несанкционированного воздействия нарушителей на инфокоммуникационную структуру сети, в том числе в чрезвычайных ситуациях.

Нарушение целостности – несанкционированная модификация или разрушение информационных ресурсов и инфраструктуры сети электросвязи.

Под доступностью информации и услуг понимается способность сети электросвязи обеспечить пользователям согласованные условия доступа к предоставляемым услугам связи и их получение, в том числе в условиях возможных воздействий нарушителей на инфокоммуникационную структуру сети электросвязи.

Нарушение доступности – нарушение доступа к использованию информации или услуг связи.

Под подотчетностью понимают свойство, которое обеспечивает однозначное отслеживание действий в сети любого объекта.

Нарушение подотчетности – отрицание действий в сети (например, участие в совершенном сеансе связи) или подделка (например, создание информации и претензии, которые якобы были получены от другого объекта или посланы другому объекту).

#### 4.2.2 Информационные системы управления предприятием

*Системы управления персоналом организации связи и системы финансового учета (1.2.1, 1.2.2)*

##### Категория персональных данных

В информационных системах управления персоналом организации связи и системах финансового учета обрабатываются персональные данные сотрудников (работников) операторов связи.

Перечень персональных данных работников приведен в разделе [3.2](#) настоящего документа.

Категория персональных данных – 2. Данные, позволяют однозначно идентифицировать субъекта персональных данных (работника оператора связи) и получить о нем дополнительную информацию.

Ине. № подл	Подп. и дата	Ине. № дубл.	Взам. инв. №	Подп. и дата

В соответствии со ст.7, 152-ФЗ от 27.07.2006 г. «О персональных данных», операторами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных, за исключением обезличенных и общедоступных персональных данных.

Информационные системы управления персоналом и системы финансового учета должны обеспечивать целостность обрабатываемых данных.

**Системы контроля и управления доступом (1.2.3)**

Категория персональных данных

Перечень персональных данных, обрабатываемых в информационных системах контроля и управления доступом, приведен в разделе [3.2](#) настоящего документа.

Категория персональных данных – 3. Данные, позволяют однозначно идентифицировать субъекта персональных данных (пользователя системы контроля и управления доступом) и не содержат дополнительной информации о нем.

Характеристики безопасности ПДн

В соответствии со ст.7, 152-ФЗ от 27.07.2006 г. «О персональных данных», операторами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных, за исключением обезличенных и общедоступных персональных данных.

В целях обеспечения постоянного (круглосуточного) контроля доступа на защищаемые объекты операторов связи, информационные системы контроля и управления доступом (включая обрабатываемые персональные данные), должны отвечать требованиям доступности.

Ине. № подл	Подп. и дата
Ине. № дубл.	Взам. инв. №
Подп. и дата	Подп. и дата

Ли	Изм.	№ докум.	Подп.	Дат
----	------	----------	-------	-----

#### **Системы обнаружения мошенничества (1.2.4)**

##### Категория персональных данных

Основной функцией информационных систем обнаружения мошенничества, является обнаружение (предупреждение/предотвращение) мошенничества и идентификация субъекта совершившего/совершающего мошеннические действия.

Категория персональных данных – 2.

##### Характеристики безопасности ПДн

В соответствии со ст.7, 152-ФЗ от 27.07.2006 г. «О персональных данных», операторами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных, за исключением обезличенных и общедоступных персональных данных.

Информационные системы обнаружения мошенничества создаются в целях защиты доходов операторов связи, мониторинга незапланированных потерь и требуют обеспечения таких характеристик безопасности персональных данных, как конфиденциальность и достоверность.

#### **Внутренние информационно-справочные системы (1.2.5)**

##### Категория персональных данных

Во внутренние информационно-справочные системы могут быть включены следующие данные: фамилия, имя, отчество, год и место рождения субъекта ПДн, адрес, абонентский номер, сведения о профессии, цифровая фотография, иные персональные данные, позволяющие идентифицировать субъекта персональных данных.

Персональные данные, обрабатываемые в информационно-справочных системах операторов связи относятся к 3-ей категории.

##### Характеристики безопасности ПДн

В соответствии со ст.7, 152-ФЗ от 27.07.2006 г. «О персональных данных», операторами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных, за исключением обезличенных и общедоступных персональных данных.

Ине. № подл	Подп. и дата
Ине. № дубл.	Взам. инв. №
Подп. и дата	Подп. и дата

Ли	Изм.	№ докум.	Подп.	Дат
----	------	----------	-------	-----

### 4.3 Информационные системы внешнего взаимодействия

#### Системы взаимодействия с бюро кредитных историй (2.1)

Категория персональных данных

Перечень персональных данных определяется ст. 4, ФЗ-218 от 30.12.2004 г. «О кредитных историях».

В титульной части кредитной истории физического лица содержится следующая информация о субъекте кредитной истории:

– фамилия, имя, отчество (если последнее имеется) на русском языке (для иностранных граждан и лиц без гражданства написанные буквами латинского алфавита на основании сведений, содержащихся в документе, удостоверяющем личность в соответствии с законодательством Российской Федерации), дата и место рождения;

– данные паспорта гражданина Российской Федерации или при его отсутствии иного документа, удостоверяющего личность в соответствии с законодательством Российской Федерации (серия, номер, дата и место выдачи, наименование и код органа, выдавшего паспорт или иной документ, удостоверяющий личность);

– идентификационный номер налогоплательщика (если лицо его указало);

– страховой номер индивидуального лицевого счета, указанный в страховом свидетельстве обязательного пенсионного страхования (если лицо его указало).

В основной части кредитной истории физического лица содержатся следующие сведения (если таковые имеются):

– в отношении субъекта кредитной истории:

- указание места регистрации и фактического места жительства;
- сведения о государственной регистрации физического лица в качестве индивидуального предпринимателя;

– в отношении обязательства заемщика (для каждой записи кредитной истории):

Ине. № подл	Подп. и дата	Ине. № дубл.	Взам. инв. №	Подп. и дата
-------------	--------------	--------------	--------------	--------------

Ли	Изм.	№ докум.	Подп.	Дат
----	------	----------	-------	-----



Совокупность информации, содержащейся в кредитной истории, полученной бюро кредитных историй, является ограниченно оборотоспособным объектом<sup>62</sup> (требование конфиденциальности).

При обмене информацией (персональными данными) с бюро кредитных историй, необходимо обеспечить целостность этих данных.

### **Системы оперативно-розыскных мероприятий (2.2)**

#### Категория персональных данных

Перечень персональных данных, обрабатываемых в информационных системах оперативно-розыскных мероприятий, устанавливается п. 14 Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность, утвержденных Постановлением Правительства Российской Федерации от 17.08.2005 г. № 538.

Базы данных должны содержать следующую информацию об абонентах оператора связи:

– фамилия, имя, отчество, место жительства и реквизиты основного документа, удостоверяющего личность, представленные при личном предъявлении абонентом указанного документа, - для абонента-гражданина;

– наименование (фирменное наименование) юридического лица, его место нахождения, а также список лиц, использующих оконечное оборудование юридического лица, заверенный уполномоченным представителем юридического лица, в котором указаны их фамилии, имена, отчества, места жительства и реквизиты основного документа, удостоверяющего личность, - для абонента - юридического лица;

– сведения баз данных о расчетах за оказанные услуги связи, в том числе о соединениях, трафике и платежах абонентов.

Категория персональных данных – 2. Дополнительной информацией, неправомерный доступ к которой может привести к непосредственному ущербу субъекту персональных данных, являются сведения баз данных о расчетах за оказанные услуги связи, в том числе о соединениях, трафике и платежах абонентов.

<sup>62</sup> ст.7, ч.4, 218-ФЗ «О кредитных историях»

Ине. № подл.	Подп. и дата
Ине. № дубл.	Взам. инв. №
Подп. и дата	
Ине. № подл.	

Ли	Изм.	№ докум.	Подп.	Дат	ИСУ-4/2009-ОК	Лист
						43

Характеристики безопасности персональных данных, обрабатываемых в системах оперативно-розыскных мероприятий, определяются требованиями нормативно-правовых актов.

*Конфиденциальность*

Должна быть исключена возможность несанкционированного доступа к данным и программному обеспечению системы оперативно-розыскных мероприятий<sup>63</sup>.

В сетях связи обеспечивается защита от несанкционированного доступа персонала, обслуживающего сеть связи, к информации, относящейся к проведению оперативно-розыскных мероприятий<sup>64</sup>.

*Целостность*

При аварийной остановке оборудования сети связи и последующем рестарте, данные об объектах контроля не должны восстанавливаться, а должны вновь передаваться на станции и пункт управления<sup>65</sup>.

*Доступность*

Информация, передаваемая в контролируемом соединении и (или) сообщении электросвязи передается на пункт управления ОРМ во время установленного соединения и (или) передачи сообщения электросвязи<sup>66</sup> (требование доступности).

Оператор связи обязан своевременно обновлять информацию, содержащуюся в базах данных об абонентах оператора связи и оказанных им услугах связи. Указанная информация должна храниться оператором связи в течение 3 лет и предоставляться органам федеральной службы безопасности, органам внутренних дел путем осуществления круглосуточного удаленного доступа к базам данных<sup>67</sup>.

<sup>63</sup> п. 5.1, Технических требований СОРМ СПРС

<sup>64</sup> п.9, Требований к сетям электросвязи для проведения оперативно-розыскных мероприятий. Часть I. Общие требования.

<sup>65</sup> п. 6.1, Технических требований СОРМ СПРС

<sup>66</sup> п.2, Требований к сетям электросвязи для проведения оперативно-розыскных мероприятий. Часть I. Общие требования.

<sup>67</sup> п.12, Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность

Ине. № подл.	Подп. и дата
Ине. № дубл.	Взам. инв. №
Подп. и дата	
Ине. № подл.	

Ли	Изм.	№ докум.	Подп.	Дат	ИСУ-4/2009-ОК	Лист 44

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

Таблица 4.1 – Исходные данные на информационные системы персональных данных операторов связи. Классификация<sup>68</sup>.

Исходные данные	Категория ПДн				Объем ПДн			Тип		Характеристики безопасности					Класс информационной системы
	Категория 1	Категория 2	Категория 3	Категория 4	Менее 1000, или ПДн в пределах организации	от 1000 до 100 000	более 100 000	Типовая	Специальная	Конфиденциальность	Целостность	Доступность	Достоверность	Подотчетность	
Информационные системы персональных данных															
<b>1. Внутренние информационные системы</b>															
<b>1.1. Информационные системы услуг связи</b>															
1.1.1. Автоматизированные системы расчетов		✓					✓		✓	✓	✓	✓	✓		ИСПДНОС2 (специальная, К2-1,2,5)
1.1.2. Системы управления взаимоотношениями с дилерами			✓				✓		✓	✓	✓				ИСПДНОС2 (специальная, К2-1)
1.1.3. Системы печати счетов		✓					✓		✓	✓					ИСПДНОС2 (специальная, К2-1)
<b>1.1.4. Системы информационно-справочного обслуживания</b>															
1.1.4.1. Автоматические системы самообслуживания абонентов				✓			✓		✓	✓		✓			ИСПДНОС4 (специальная, К4-2)
1.1.4.2. Системы управления взаимоотношениями с клиентами		✓					✓		✓	✓	✓	✓			ИСПДНОС2 (специальная, К2-1,2)
1.1.5. Системы интеграции		✓					✓		✓	✓	✓	✓			ИСПДНОС2 (специальная, К2-1,2)
1.1.6. Системы записи вызовов		✓				✓		✓		✓					К2
<b>1.1.7. Автоматизированные рабочие места</b>															
1.1.7.1. Автоматизированные рабочие места администраторов		✓			✓				✓	✓		✓			АРМ.А (специальная, К2-2)
1.1.7.2. Автоматизированные рабочие места пользователей		✓			✓				✓	✓	✓				АРМ.П (специальная, К3-1)
1.1.8. Сети связи				✓			✓		✓	✓	✓	✓		✓	не классифицируются
<b>1.2. Информационные системы управления предприятием</b>															
1.2.1. Системы управления персоналом организации связи		✓			✓				✓	✓	✓				ИСПДНОС3 (специальная, К3-1)
1.2.2. Системы финансового учета		✓			✓				✓	✓	✓				ИСПДНОС3 (специальная, К3-1)
1.2.3. Системы контроля и управления доступом			✓				✓		✓	✓		✓			ИСПДНОС2 (специальная, К2-2)
1.2.4. Системы обнаружения мошенничества		✓					✓		✓	✓			✓		ИСПДНОС2 (специальная, К2-5)
1.2.5. Внутренние информационно-справочные системы				✓	✓			✓		✓					К3
<b>2. Информационные системы внешнего взаимодействия</b>															
2.1. Системы взаимодействия с бюро кредитных историй		✓			✓				✓	✓	✓				ИСПДНОС3 (специальная, К3-1)
2.2. Системы оперативно-розыскных мероприятий		✓				✓			✓	✓	✓	✓			не классифицируются

<sup>68</sup> Класс информационной системы определяется в соответствии с Методикой, приведенной в разделе 5 настоящего документа.

Изм.	
Лист	
№ докум.	
Подп.	
Дата	
ИСУ-4/2009-ОК	
Лист	45

## 5. ОТРАСЛЕВОЙ КЛАССИФИКАТОР. МЕТОДИКА КЛАССИФИКАЦИИ.

### 5.1 Общие положения

Проведение классификации информационных систем персональных данных операторов связи включает в себя следующие этапы (Рисунок 5.1):

- 1) Сбор и анализ исходных данных по информационной системе.
- 2) Присвоение информационной системе соответствующего класса и его документальное оформление.
- 3) Выбор требований по обеспечению безопасности персональных данных.

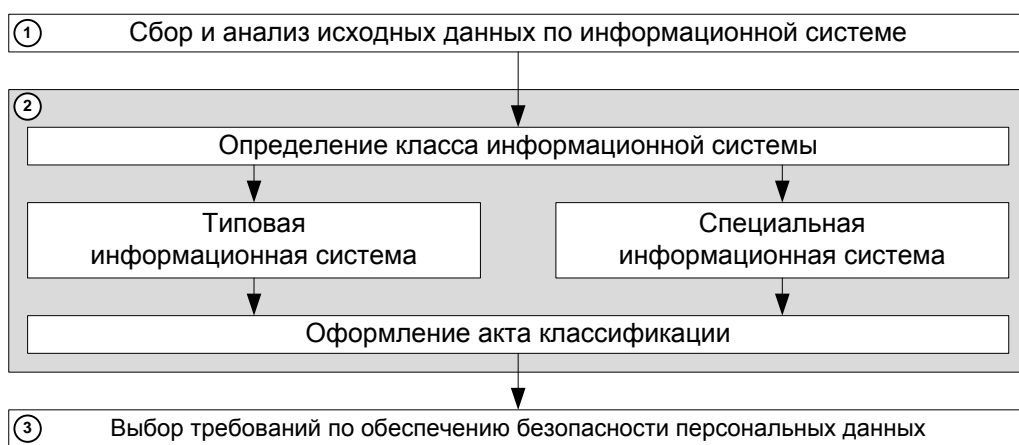


Рисунок 5.1 – Порядок проведения классификации информационных систем персональных данных операторов связи.

### 5.2 Сбор и анализ исходных данных

При сборе и анализе исходных данных по информационным системам персональных данных операторов связи необходимо определить (см. раздел 4 настоящего документа):

- категорию обрабатываемых в информационной системе персональных данных;
- объем обрабатываемых персональных данных (количество субъектов персональных данных, персональные данные которых обрабатываются в информационной системе);
- характеристики безопасности персональных данных, обрабатываемых в информационной системе;

Ине. № подл.	Подп. и дата
Ине. № дубл.	Взам. инв. №
Ине. № инв.	Подп. и дата
Ине. № инв.	Подп. и дата

Ли	Изм.	№ докум.	Подп.	Дат
----	------	----------	-------	-----

- структуру информационной системы;
- наличие подключений информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена;
- режим обработки персональных данных;
- режим разграничения прав доступа пользователей информационной системы;
- местонахождение технических средств информационной системы.

### 5.3 Присвоение информационной системе соответствующего класса

Информационные системы персональных данных операторов связи подразделяются на типовые и специальные. Критерии отнесения информационных систем к специальным информационным системам персональных данных приведены в разделе 1.3 настоящего документа.

#### 5.3.1 Методика классификации типовых информационных систем

Класс типовой информационной системы определяется в соответствии с таблицей<sup>69</sup>.

Таблица 5.1 – Классы типовых информационных систем персональных данных операторов связи

Объем ПДн	Менее 1.000 (или ПДн в пределах организации связи)	От 1.000 до 100.000	Более 100.000
Категория ПДн <sup>70</sup>			
Категория 4	K4	K4	K4
Категория 3	K3	K3	K2
Категория 2	K3	K2	K1

#### 5.3.2 Методика классификации специальных информационных систем

По результатам анализа исходных данных, специальные информационные системы персональных данных операторов связи подразделяются на два типа:

- **к первому типу** относятся автоматизированные рабочие места, являющиеся локальными информационными системами, не имеющими подключений к сетям связи общего пользования и (или) сетям международного информационного обмена;

<sup>69</sup> п. 15, Порядка проведения классификации информационных систем персональных данных

<sup>70</sup> Операторами связи не осуществляется обработки ПДн первой категории (см. раздел 3.3 настоящего документа)

Ине. № подл.	Подп. и дата	Ине. № дубл.	Взам. инв. №	Подп. и дата	Ине. № подл.	Ли	Изм.	№ докум.	Подп.	Дат	ИСУ-4/2009-ОК	Лист
												47

– **ко второму типу** относятся локальные информационные системы и (или) комплексы локальных информационных систем, объединенных в единую информационную систему средствами связи, не имеющими подключений к сетям связи общего пользования и (или) сетям международного информационного обмена.

Класс автоматизированного рабочего места определяется по его функционально-технологическому принципу:

*АРМ.А* – автоматизированное рабочее место администратора;

*АРМ.П* – автоматизированное рабочее место пользователя.

Локальной информационной системе и (или) комплексу локальных информационных систем, объединенных в единую информационную систему средствами связи, присваивается один из следующих классов:

*ИСПДНОС2с* – специальная информационная система персональных данных оператора связи, для которой нарушение заданных характеристик безопасности персональных данных, обрабатываемых в ней, может привести к **негативным последствиям** для субъектов персональных данных;

*ИСПДНОС3с* – специальная информационная система персональных данных оператора связи, для которой нарушение заданных характеристик безопасности персональных данных, обрабатываемых в ней, может привести к **незначительным негативным последствиям** для субъектов персональных данных;

*ИСПДНОС4с* – специальная информационная система персональных данных оператора связи, для которой нарушение заданных характеристик безопасности персональных данных, обрабатываемых в ней, **не приводит к негативным последствиям** для субъектов персональных данных.

Каждый класс характеризуется определенной минимальной совокупностью требований по защите персональных данных.

Ине. № подл.	Подп. и дата
Ине. № дубл.	Взам. инв. №
Подп. и дата	Подп. и дата

Ли	Изм.	№ докум.	Подп.	Дат	ИСУ-4/2009-ОК	Лист
						48

Таблица 5.2 – Классификация локальных информационных систем и (или) комплексов локальных информационных систем, объединенных в единую информационную систему средствами связи.

Объем ПДн Категория ПДн <sup>71</sup>	Менее 1.000 (или ПДн в пределах организации связи)	От 1.000 до 100.000	Более 100.000
Категория 4	ИСПДнОС4с	ИСПДнОС4с	ИСПДнОС4с
Категория 3	ИСПДнОС3с	ИСПДнОС3с	ИСПДнОС2с
Категория 2	ИСПДнОС3с	ИСПДнОС2с	ИСПДнОС2с

В случае, объединения локальных информационных систем и (или) комплекса локальных информационных систем в единую информационную систему, информационной системе в целом присваивается класс, соответствующий наиболее высокому классу входящих в нее подсистем.

Результаты классификации информационных систем оформляются соответствующим актом оператора связи.

#### 5.4 Выбор требований по обеспечению безопасности персональных данных

Для типовых информационных систем персональных данных, необходимо обеспечить мероприятия по организации и техническому обеспечению безопасности персональных данных имеющих локальную структуру, не имеющих подключений к сетям связи общего пользования и (или) сетям международного информационного обмена, при многопользовательском режиме обработке персональных данных, с разграничением прав доступа пользователей в соответствии с нормативно методическими документами ФСТЭК России.

Для специальных информационных систем персональных данных, выбор требований по обеспечению безопасности персональных данных осуществляется в соответствии со следующей таблицей.

<sup>71</sup> Операторами связи не осуществляется обработки ПДн первой категории (см. раздел 3.3 настоящего документа)

Ине. № подл.	Подп. и дата	Ине. № дубл.	Взам. инв. №	Подп. и дата	Ли	Изм.	№ докум.	Подп.	Дат	ИСУ-4/2009-ОК	Лист
											49

Таблица 5.3 – Выбор требований по обеспечению безопасности персональных данных, при их обработке в специальных информационных системах персональных данных операторов связи

№ п/п	Класс специальной информационной системы персональных данных	Требования по обеспечению безопасности персональных данных
1.	АРМ.А	Определяются профилем защиты ISU-12/2009-ПЗ1
2.	АРМ.П	Определяются профилем защиты ISU-12/2009-ПЗ1
3.	ИСПДНОС2с	Определяются профилем защиты ISU-13/2009-ПЗ2
4.	ИСПДНОС3с	Определяются профилем защиты ISU-14/2009-ПЗ3
5.	ИСПДНОС4с	Определяется оператором связи в зависимости от ущерба, который может быть нанесен в следствии несанкционированного или непреднамеренного доступа к персональным данным

Сведения о предварительной классификации информационных систем персональных данных приведены в таблице 4.1 настоящего документа.

Таблица 5.4 – Соотношение классов типовых ИСПДн и специальных ИСПДн операторов связи

Типовые ИСПДн	K1	K2	K3	K4
	Специальные ИСПДн оператора связи			
ИСПДНОС2с		✓		
ИСПДНОС3с			✓	
ИСПДНОС4с				✓
АРМ.А		✓		
АРМ.П			✓	

Применительно к специальным информационным системам после определения класса системы, оператором связи должна быть разработана модель угроз безопасности персональных данных с использованием «Отраслевой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных операторов связи» и проведена оценка актуальности угроз.

По результатам оценки требования по защите ИСПДн от различных угроз могут быть скорректированы по сравнению с типовыми. Решение об этом принимает оператор связи.

Ине. № подл. Подп. и дата

Ине. № дубл. Подп. и дата

Взам. инв. №

Ине. № подл. Подп. и дата



12. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена Заместителем директора ФСТЭК России 14.02.2008 г.

13. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации. Утверждены руководством 8 Центра ФСБ России 21.02.2008 г. №149/5-144.

14. Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при обработке в информационных системах персональных данных. Утверждены руководством 8 Центра ФСБ России 21.02.2008 г. №149/6/6-622.

15. Автоматизированные системы расчетов с пользователями за услуги электросвязи. Общие технические требования. Утверждены Госкомсвязи России 16.06.1998 г.

16. Нормативно-методический документ. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утвержден приказом Гостехкомиссии России от 30.08.2002 г. №282.

17. Приказ Министерства информационных технологий и связи Российской Федерации от 02.07.2007 №73 «Об утверждении правил применения автоматизированных систем расчетов»

18. Постановление Правительства Российской Федерации от 15.04.2005 г. №222 «Об утверждении правил оказания услуг телеграфной связи»

19. Постановление Правительства Российской Федерации от 18.05.2005 г. №310 «Об утверждении правил оказания услуг местной, внутризоновой, междугородной и международной телефонной связи»

20. Постановление Правительства Российской Федерации от 25.05.2005 г. №328 «Об утверждении правил оказания услуг подвижной связи»

Подп. и дата
Взам. инв. №
Инв. № дубл.
Подп. и дата
Инв. № подл.

Ли	Изм.	№ докум.	Подп.	Дат	ICU-4/2009-OK

21. Постановление Правительства Российской Федерации от 06.07.2005 г. №353 «Об утверждении правил оказания услуг связи проводного радиовещания»

22. Постановление Правительства Российской Федерации от 23.01.2006 г. №32 «Об утверждении правил оказания услуг связи по передаче данных»

23. Постановление Правительства Российской Федерации от 22.12.2006 г. №785 «Об утверждении правил оказания услуг связи для целей телевизионного вещания и (или) радиовещания»

24. Постановление Правительства Российской Федерации от 10.09.2007 г. №575 «Об утверждении правил оказания телематических услуг связи»

25. Постановление Правительства Российской Федерации от 25.06.2009 г. №532 «Об утверждении перечня средств связи, подлежащих обязательной сертификации»

26. Постановление Правительства Российской Федерации от 13.04.2005 г. №214 «Об утверждении правил организации и проведения работ по обязательному подтверждению соответствия средств связи»

27. Постановление Правительства Российской Федерации от 27.08.2005. №538 «Об утверждении правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-разыскную деятельность»

28. Постановление Правительства Российской Федерации от 08.07.1997 г. №828 «Об утверждении положения о паспорте гражданина Российской Федерации, образца бланка и описания паспорта гражданина Российской Федерации»

29. Приказ Министерства информационных технологий и связи Российской Федерации от 09.01.2008 №1 «Об утверждении требований по защите сетей связи от несанкционированного доступа к ним и передаваемой посредством их информации»

30. Рекомендации по стандартизации. Р50.1.053-2005. Информационные технологии. Основные термины и определения в области технической защиты информации. Разработаны Государственным научно-исследовательским испытательным институтом проблем технической защиты информации Гостехкомиссии России.

31. ГОСТ Р 52448-2005. Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения.

Ине. № подл.	Подп. и дата
Ине. № дубл.	Взам. инв. №
Подп. и дата	Подп. и дата
Ине. № подл.	Ине. № дубл.
Ине. № подл.	Ине. № дубл.

Ли	Изм.	№ докум.	Подп.	Дат	ICU-4/2009-OK	Лист 53

32. ГОСТ Р 53110 – 2008. Система обеспечения информационной безопасности сети связи общего пользования. Общие положения.

33. ГОСТ 34.003-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения

34. ГОСТ Р 51241 – 2008. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний.

35. ГОСТ Р ИСО/МЭК 10027-93. Информационная технология. Структура словаря информационных ресурсов (IRDS).

*Примечание.* При пользовании настоящим Классификатором целесообразно проверить действие ссылочных документов. Если ссылочный документ заменен (изменен), то при пользовании Классификатором следует руководствоваться заменяющим (измененным) документом. Если ссылочный документ отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

Ине. № подп	Подп. и дата				Ине. № дубл.	Взам. инв. №	Подп. и дата	Ине. № подп	Лист
Ли	Изм.	№ докум.	Подп.	Дат	ICU-4/2009-ОК				54

