

**Российская Федерация**

**Администрация  
Тамбовской области**

**ФИНАНСОВОЕ УПРАВЛЕНИЕ  
ТАМБОВСКОЙ ОБЛАСТИ**

## **П Р И К А З**

«22» мая 2014 г.

№ 56

г. Тамбов

Об утверждении Правил обработки персональных данных в финансовом управлении Тамбовской области

В соответствии с Федеральным законом от 27.06.2006 № 152-ФЗ «О персональных данных» и Постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными и муниципальными органами» приказываю:

утвердить Правила обработки персональных данных в финансовом управлении Тамбовской области согласно приложению.

Заместитель главы администрации области,  
начальник финансового управления области

Л.П. Третьякова

УТВЕРЖДЕНЫ  
приказом финансового  
управления области  
от 22.05.2014 № 56

## Правила обработки персональных данных в финансовом управлении Тамбовской области

### 1. Общие положения

Настоящие Правила обработки персональных данных в финансовом управлении Тамбовской области (далее – Правила, Управление) устанавливают процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных (далее - ПДн), а также определяющие для каждой цели обработки ПДн содержание обрабатываемых ПДн, категории субъектов, ПДн которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований.

### 2. Категории субъектов персональных данных

В Управлении осуществляется обработка ПДн следующих категорий лиц (далее - субъект персональных данных):

- государственных гражданских служащих (далее - Служащие);
- лиц, замещающие должности, не относящиеся к должностям государственной гражданской службы;
- кандидатов на замещение вакантных должностей;
- лиц, в отношении которых осуществляется производство по делам об административных правонарушениях;
- граждан, чьи персональные данные внесены в государственную информационную систему «Государственные и муниципальные платежи».

### 3. Принципы обработки персональных данных

Обработка ПДн в Управлении должна осуществляться на основе следующих принципов:

- обработки ПДн на законной и справедливой основе;
- ограничения обработки ПДн при достижении конкретных, заранее определенных и законных целей;
- недопущения объединения баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой;
- обработки ПДн субъектов персональных данных, которые отвечают целям их обработки;
- соответствия содержания и объёма обрабатываемых ПДн заявленным целям обработки;
- исключения избыточности обрабатываемых ПДн по отношению к заявленным целям их обработки;

обеспечения точности, достаточности и актуальности ПДн по отношению к целям обработки ПДн;

обеспечения принятия необходимых мер при удалении или уточнении неполных или неточных данных;

осуществления хранения ПДн в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральными законами или договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;

уничтожения либо обезличивания ПДн по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральными законами;

обеспечения защиты прав и свобод человека и гражданина при обработке его ПДн, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну;

соблюдения принципов и правил обработки ПДн при поручении такой обработки другому лицу;

соблюдения конфиденциальности ПДн;

обработки ПДн (в том числе при обработке общедоступных ПДн, специальных категорий ПДн, биометрических ПДн, при принятии решений на основании исключительно автоматизированной обработки ПДн, при трансграничной передаче ПДн) с письменного согласия субъектов персональных данных либо на ином законном основании;

соблюдения законности при осуществлении трансграничной передачи ПДн;

соблюдения обязанностей, возлагаемых на Управление действующим законодательством;

принятия мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных законодательством в области ПДн;

принятия необходимых правовых, организационных и технических мер или обеспечение их принятия для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн;

недопустимости ограничения прав и свобод человека и гражданина по мотивам, связанным с использованием различных способов обработки ПДн или обозначения принадлежности ПДн, содержащихся в государственных информационных системах персональных данных (далее - ИСПДн), конкретному субъекту персональных данных;

недопустимости использования оскорбляющих чувства граждан или унижающих человеческое достоинство способов обозначения принадлежности ПДн, содержащихся в государственных ИСПДн, конкретному субъекту персональных данных;

личной ответственности должностных лиц, осуществляющих обработку ПДн;

документального оформления всех принятых решений по обработке и обеспечению безопасности ПДн.

#### 4. Цели обработки персональных данных

Управление, являясь оператором ПДн, должно определять цели обработки ПДн.

Цели обработки ПДн должны быть четко определены и соответствовать: заявленным в Положении о финансовом управлении, утвержденном постановлением главы администрации Тамбовской области от 22.11.2010 №21 (далее - Положении) основным функциям;

Цели обработки ПДн определяют:  
содержание и объем обрабатываемых ПДн;  
категории субъектов, персональные данные которых обрабатываются;  
сроки их обработки и хранения;  
порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований.

Цели обработки ПДн должны быть:

конкретны;  
заранее определены;  
законны;  
заявлены.

Обработка ПДн в Управлении осуществляется для следующих целей:  
оформления отношений при поступлении на государственную гражданскую службу;

участия граждан в конкурсах на замещение вакантных должностей государственной гражданской службы;  
ведения бухгалтерского учета;  
осуществления производства по делам об административных правонарушениях;  
обработки сведений о государственных и муниципальных платежах.

Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

Совместимость целей определяется по наличию общей цели, связанной с заявленными в Положении или по наличию общей цели, определяемой действующим законодательством Российской Федерации.

#### 5. Способы и правила обработки персональных данных в ИСПДн в зависимости от применения средств автоматизации

Способы обработки ПДн в ИСПДн:

обработка ПДн без использования средств автоматизации;  
обработка ПДн с использованием средств автоматизации.

##### 5.1. Правила обработки персональных данных без использования средств автоматизации

Для обработки различных категорий ПДн, осуществляемой без использования средств автоматизации, для каждой категории ПДн должен использоваться отдельный материальный носитель.

При фиксации ПДн на материальных носителях не допускается фиксация на одном материальном носителе ПДн, цели обработки которых заведомо не совместимы.

При несовместимости целей обработки ПДн, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку ПДн отдельно от других зафиксированных на том же носителе ПДн, должны быть приняты меры по обеспечению раздельной обработки ПДн. При необходимости использования или распространения определённых ПДн отдельно от находящихся на том же материальном носителе других ПДн, осуществляется копирование ПДн, подлежащих распространению или использованию, способом, исключающим одновременное копирование ПДн, не подлежащих распространению (использованию). Далее используется (распространяется) копия ПДн.

При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн, должны соблюдаться следующие условия:

- типовая форма или связанные с ней документы (инструкция по её заполнению, карточки, реестры и журналы) должны содержать:

- сведения о цели обработки ПДн, осуществляемой без использования средств автоматизации;

- имя (наименование) и адрес оператора;

- фамилию, имя, отчество и адрес субъекта персональных данных, источник получения ПДн;

- сроки обработки ПДн;

- перечень действий с персональными данными, которые будут совершаться в процессе их обработки;

- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку ПДн, осуществляемую без использования средств автоматизации, при необходимости получения письменного согласия на обработку ПДн;

- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

- типовая форма должна исключать объединение полей, предназначенных для внесения ПДн, цели обработки которых заведомо не совместимы.

Уточнение ПДн при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях, либо путем изготовления нового материального носителя с уточнёнными персональными данными.

## 5.2. Правила обработки персональных данных средствами автоматизации

Обработка ПДн средствами автоматизации в Управлении допускается в следующих случаях:

обработка ПДн осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

обработка ПДн необходима для достижения целей, предусмотренных законодательством Российской Федерации, для осуществления и выполнения возложенных на Управление функций, полномочий и обязанностей;

обработка ПДн необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

обработка ПДн необходима для осуществления прав и законных интересов Управления или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

обработка ПДн осуществляется в статистических или иных исследовательских целях при условии обязательного обезличивания ПДн;

осуществляется обработка ПДн, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных по его просьбе (персональные данные, сделанные общедоступными субъектом персональных данных);

осуществляется обработка ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральными законами.

Обработка ПДн средствами автоматизации должна осуществляться на основании правил, инструкций, руководств, регламентов и иных документов, определяющих технологический процесс обработки информации, содержащей такие данные, определённых для выполнения конкретных операций с заранее определёнными целями, с учётом требований настоящих Правил.

## 6. Обработка персональных данных с согласия субъекта персональных данных

В случае если обработка ПДн субъекта персональных данных в ИСПДн осуществляется на основании согласия и не имеется оснований для обработки таких ПДн без получения согласия, должны выполняться указанные в настоящем пункте правила.

Субъект персональных данных принимает решение о предоставлении его ПДн и даёт согласие на их обработку свободно, своей волей и в своём интересе.

Согласие на обработку ПДн должно быть:

конкретным;

информированным;

сознательным.

Согласие на обработку ПДн Управлению может быть дано субъектом персональных данных или его представителем только в письменной форме. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признаётся согласие в форме электронного документа, подписанного электронной подписью в соответствии с действующим законодательством об электронной подписи.

В случае получения согласия на обработку ПДн от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от

имени субъекта персональных данных проверяются оператором.

В случае недееспособности субъекта персональных данных согласие на обработку его ПДн даёт законный представитель субъекта персональных данных.

В случае смерти субъекта персональных данных согласие на обработку его ПДн дают наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

В случае получения согласия от законного представителя субъекта персональных данных или наследников субъекта персональных данных они обязаны представить документы, подтверждающие их полномочия.

Допускается включение согласия в типовые формы (бланки) материальных носителей ПДн и в договор с субъектом персональных данных.

Письменные согласия субъектом персональных данных должны храниться в Управлении.

Согласие на обработку ПДн может быть отозвано субъектом персональных данных путем направления запроса в Управление.

## 7. Обработка персональных данных без согласия субъекта персональных данных

Обработка ПДн без получения согласия на такую обработку от субъекта персональных данных может осуществляться при наличии оснований, предусмотренных пунктами 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.06.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный Закон).

## 8. Правила обработки персональных данных средствами автоматизации при поручении обработки персональных данных

### 8.1. Правила обработки персональных данных средствами автоматизации при поручении обработки персональных данных другому лицу

Управление вправе поручить обработку ПДн другому лицу (поручение оператора):

с согласия субъекта персональных данных;

на основании заключаемого с этим лицом договора, в том числе государственного контракта;

путём принятия соответствующего акта.

Лицо, осуществляющее обработку персональных данных по поручению Управления, обязано соблюдать принципы и правила обработки персональных данных.

В поручении оператора:

должен быть определён перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных;

должны быть определены цели обработки персональных данных;

должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных;

должна быть установлена обязанность такого лица обеспечивать безопасность

персональных данных при их обработке;

должны быть указаны требования к защите обрабатываемых ПДн в соответствии с настоящими Правилами и техническим заданием на создание системы защиты ПДн;

установлена ответственность такого лица перед Управлением в случаях нарушений установленных требований и законодательства Российской Федерации в области ПДн;

при необходимости получения согласия на обработку ПДн от субъекта персональных данных предусмотрен порядок сбора и передачи в Управление такого согласия.

В случае необходимости получения согласия на обработку ПДн от субъекта персональных данных обязанность получения такого согласия возлагается на Управление.

## 8.2. Правила обработки персональных данных средствами автоматизации при поручении обработки персональных данных другим лицом

В случае поручения обработки ПДн средствами автоматизации Управлению другим лицом, такое лицо своим поручением оператору обязано:

определить перечень действий (операций) с персональными данными;

определить цели обработки ПДн;

установить обязанность соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке;

указать требования к защите обрабатываемых ПДн.

В случае неопределения такой информации и требований другим лицом, Управление обязано добиться их определения и документального оформления.

В случае принятия поручения на обработку ПДн Управление от другого лица без указанной информации и требований, такая обработка не считается обработкой, осуществляемой по поручению оператора, и оператором ПДн будет являться Управление.

Управление обязано выполнить все требования, установленные другим лицом в поручении оператора, и за все нарушения в обработке ПДн несёт ответственность перед таким лицом.

Управление при осуществлении обработки ПДн по поручению оператора не обязано получать согласие субъекта персональных данных на обработку его ПДн.

## 9. Правила обработки персональных данных в ИСПДн в зависимости от категории обрабатываемых персональных данных

В Управлении устанавливаются следующие особые правила обработки ПДн в зависимости от категории обрабатываемых ПДн:

обработка специальных категорий ПДн;

обработка биометрических ПДн;

обработка общедоступных ПДн.

### 9.1. Правила обработки специальных категорий персональных данных

К специальным категориям ПДн относятся сведения, касающиеся:

расовой принадлежности;

национальной принадлежности;



политических взглядов;  
религиозных убеждений;  
философских убеждений;  
состояния здоровья;  
интимной жизни;  
судимости.

В Управлении разрешается обработка специальных категорий ПДн при соблюдении условий, указанных в ч. 2 ст. 10 Федерального закона.

Обработка специальных категорий ПДн в остальных случаях в Управлении не допускается.

## 9.2. Правила обработки биометрических персональных данных

К биометрическим персональным данным относятся (обязательное выполнение всех трёх условий одновременно):

сведения, которые характеризуют физиологические и биологические особенности человека;

сведения, на основании которых можно установить его личность;

сведения, которые используются Управлением для установления личности субъекта ПДн.

В случае принятия решения об обработке биометрических ПДн, такие данные могут обрабатываться только при наличии согласия субъекта персональных данных в письменной форме.

## 9.3. Правила обработки общедоступных персональных данных

Общедоступные персональные данные физических лиц, полученные из сторонних общедоступных источников ПДн, в Управлении обрабатываются в исключительных случаях в сроки, не превышающие необходимые для их использования. При этом совместно с такими данными должны собираться реквизиты их источника и подтверждение согласия субъекта персональных данных на включение такой информации в общедоступные источники ПДн. По достижении целей обработки общедоступных ПДн они подлежат немедленному уничтожению.

## 10. Правила обработки персональных данных в ИСПДн в зависимости от цели обработки персональных данных

В Управлении устанавливаются следующие особые правила обработки ПДн в зависимости от цели обработки ПДн:

правила обработки ПДн при трансграничной передаче ПДн;

правила работы с обезличенными данными.

### 10.1. Правила обработки персональных данных при трансграничной передаче персональных данных

Трансграничная передача ПДн Управлением не осуществляется.

В случае принятия решения о трансграничной передаче ПДн такие данные могут обрабатываться только в следующих случаях:

при наличии согласия в письменной форме субъекта персональных данных на трансграничную передачу его ПДн;

предусмотренных международными договорами Российской Федерации;

исполнения договора, стороной которого является субъект персональных данных;

защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц при невозможности получения согласия в письменной форме субъекта персональных данных.

Управление до начала осуществления трансграничной передачи ПДн обязано убедиться в том, что иностранным государством, на территорию которого осуществляется передача ПДн, обеспечивается адекватная защита прав субъекта персональных данных.

## 10.2. Правила работы с обезличенными персональными данными

Обезличиванием ПДн называются действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту персональных данных.

Порядок обезличивания в Управлении устанавливается Правилами работы с обезличенными персональными данными.

### 11. Основные составляющие принципы в обработке персональных данных

Принципы обработки ПДн включают в себя:

определение законности целей обработки ПДн;

оценку вреда, который может быть причинён субъекту персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн;

определение заданных характеристик безопасности ПДн;

определение сроков обработки, в том числе хранения ПДн, осуществление контроля за соблюдением сроков обработки ПДн и фактов достижения целей обработки ПДн.

#### 11.1. Определение законности целей обработки персональных данных

Заявляемые цели обработки ПДн должны быть законны, причем, кроме самого факта обработки ПДн, должны рассматриваться и соответственно иметь правовое основание особые правила обработки определённых наборов ПДн (таких как специальные категории ПДн, биометрические персональные данные и др.), особые способы обработки ПДн (обработка без использования средств автоматизации, исключительно автоматизированная обработка ПДн и др.), а также особые цели обработки ПДн (трансграничная передача ПДн и др.).

При определении правовых оснований обработки ПДн должны определяться реквизиты федеральных законов, а также иных подзаконных актов и документов органов государственной власти, которые требуют обработки ПДн или иных документов, являющихся такими основаниями.

Обработка ПДн без документально определённого и оформленного правового основания обработки ПДн не допускается.

#### 11.2. Оценка вреда, который может быть причинён субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных

Оценкой вреда, который может быть причинён субъекту персональных данных в случае нарушения требований по обработке и обеспечению безопасности

ПДн, является определение юридических или иным образом затрагивающих права и законные интересы последствий в отношении субъекта персональных данных, которые могут возникнуть в случае нарушения требований по обработке и обеспечению безопасности ПДн.

К юридическим последствиям относятся случаи возникновения, изменения или прекращения личных либо имущественных прав граждан или иным образом затрагивающих его права, свободы и законные интересы.

При обработке ПДн должны определяться и документально оформляться все возможные юридические или иным образом затрагивающие права и законные интересы последствия в отношении субъекта персональных данных, которые могут возникнуть в случае нарушения требований по обработке и обеспечению безопасности ПДн.

Определение таких юридических последствий необходимо для недопущения нарушения и обеспечения защиты прав и свобод человека и гражданина при обработке его ПДн, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также определения соотношения вреда, который может быть причинён субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн и принимаемых мер.

### 11.3. Заданные характеристики безопасности персональных данных

Всеми лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных.

Конфиденциальность ПДн - это обязательное для соблюдения оператором или иным получившим доступ к ПДн лицом требование не раскрывать третьим лицам и не распространять ПДн без согласия субъекта персональных данных, если иное не предусмотрено федеральными законами.

Вне зависимости от необходимости обеспечения конфиденциальности ПДн, при обработке ПДн должно определяться наличие требований по обеспечению иных характеристик безопасности ПДн, отличных от неё.

К таким характеристикам относятся:

требование по обеспечению защищённости от уничтожения ПДн;

требование по обеспечению защищённости от изменения ПДн;

требование по обеспечению защищённости от блокирования ПДн;

требование по обеспечению защищённости от иных несанкционированных действий.

### 11.4. Определение сроков обработки, в том числе хранения персональных данных, осуществление контроля за соблюдением сроков обработки персональных данных и фактов достижения целей обработки персональных данных

На основании определённых целей обработки ПДн, способов обработки и образующихся в процессе такой обработки различных видов документов устанавливаются сроки такой обработки ПДн, в том числе хранения.

Определение сроков хранения осуществляется в соответствии с требованиями законодательства об архивном деле Российской Федерации, в том числе в соответствии с перечнями типовых архивных документов с указанием сроков их хранения.

При использовании документов, содержащих ПДн, в различных целях, определение сроков обработки, в том числе хранения, таких документов устанавливается по максимальному сроку, предусмотренному федеральными законами. При этом, в случае наличия ПДн в таких документах, обработка которых более не требуется, производятся действия по уничтожению таких данных.

На документы, включённые в состав Архивного фонда Российской Федерации, действие настоящих Правил не распространяется.

С целью выполнения требования по уничтожению либо обезличиванию ПДн по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено Федеральным законом, в Управлении создается комиссия, определяющая факт достижения целей обработки ПДн и достижение предельных сроков хранения документов, содержащих персональные данные, и осуществляющая уничтожение ПДн.

## 12. Действия с персональными данными

Обработкой ПДн называется любое действие или совокупность действий, совершаемых с использованием средств автоматизации или без использования таких средств ПДн, включая:

- сбор ПДн;
- запись ПДн;
- систематизацию ПДн;
- накопление ПДн;
- хранение ПДн;
- уточнение (обновление) ПДн;
- уточнение (изменение) ПДн;
- извлечение ПДн;
- использование ПДн;
- передачу (распространение) ПДн;
- передачу (предоставление) ПДн;
- передачу (доступ) ПДн;
- обезличивание ПДн;
- блокирование ПДн;
- удаление ПДн;
- уничтожение ПДн.

Обработка ПДн без определенных и документально оформленных действий, совершаемых с персональными данными, не допускается.

## 13. Осуществление сбора персональных данных

### 13.1. Способы сбора персональных данных и источники их получения

В Управлении применяются следующие способы получения ПДн субъектов персональных данных:

- заполнение субъектом персональных данных соответствующих форм (в том числе для заключения договора);
- получение ПДн от третьих лиц;
- получение данных на основании запроса третьим лицам;
- сбор данных из общедоступных источников.

Получение ПДн в Управлении допускается только:  
 непосредственно от субъекта персональных данных;  
 из общедоступных источников;  
 от третьих лиц.

Получение ПДн из иных источников не допускается.

В связи с необходимостью постоянного контроля за наличием ПДн в общедоступных источниках ПДн, получение и использование таких данных является не рекомендуемым и должно осуществляться только в исключительных случаях в сроки, не превышающие необходимых для принятия соответствующего решения.

### 13.2. Правила сбора персональных данных

Если предоставление ПДн является обязательным в соответствии с законодательством Российской Федерации, Управление обязано разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

Если основания на обработку ПДн без согласия отсутствуют, то необходимо получение согласия субъекта персональных данных на обработку его ПДн. Обработка ПДн без получения такого согласия запрещается.

Если персональные данные получены не от субъекта персональных данных, Управление до начала обработки таких ПДн обязано предоставить субъекту персональных данных:

наименование либо фамилию, имя, отчество и адрес оператора или его представителя;

сведения о цели обработки ПДн и её правовое основание;

сведения о предполагаемых пользователях ПДн;

сведения об установленных правах субъекта персональных данных;

сведения об источниках получения ПДн.

Управление освобождается от обязанности предоставлять субъекту персональных данных сведения в случаях, если:

субъект персональных данных уведомлён об осуществлении обработки его ПДн соответствующим оператором;

персональные данные получены Управлением на основании Федерального закона, или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;

персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;

Управление осуществляет обработку ПДн для статистических или иных исследовательских целей, если при этом не нарушаются права и законные интересы субъекта персональных данных;

предоставление субъекту ПДн сведений нарушает права и законные интересы третьих лиц.

### 14. Осуществление систематизации, накопления, уточнения и использования персональных данных

Систематизация, накопление, уточнение, использование ПДн могут осуществляться любыми законными способами в соответствии с правилами,

инструкциями, руководствами, регламентами и иными документами, определяющими технологический процесс обработки информации.

В Управлении могут быть установлены особенности учета ПДн в ИСПДн, в том числе использование различных способов обозначения принадлежности ПДн, содержащихся в соответствующей информационной системе ПДн, конкретному субъекту персональных данных.

Права и свободы человека и гражданина не могут быть ограничены по мотивам, связанным с использованием различных способов обработки ПДн или обозначения принадлежности ПДн, содержащихся в ИСПДн, конкретному субъекту персональных данных.

Не допускается использование оскорбляющих чувства граждан или унижающих человеческое достоинство способов обозначения принадлежности ПДн, содержащихся в ИСПДн, конкретному субъекту персональных данных.

Уточнение ПДн должно производиться только на основании законно полученной в установленном порядке информации.

Решение об уточнении ПДн субъекта персональных данных принимается лицом, ответственным за организацию обработки ПДн.

Использование ПДн должно осуществляться исключительно в заявленных целях. Использование ПДн в заранее не определенных и не оформленных установленным образом целях не допускается.

#### 15. Осуществление записи и извлечения персональных данных

Запись ПДн в ИСПДн Управлением может осуществляться с любых носителей информации или из других ИСПДн.

Извлечение ПДн из ИСПДн может осуществляться с целью:

вывода ПДн на бумажный или иной носитель информации, не предназначенный для его обработки средствами вычислительной техники;

вывода ПДн на носители информации, предназначенные для их обработки средствами вычислительной техники.

#### 16. Осуществление передачи персональных данных

Передача ПДн должна осуществляться с соблюдением настоящих Правил и действующего законодательства Российской Федерации.

В Управлении приняты следующие способы передачи ПДн субъектов персональных данных:

передача ПДн на электронных и бумажных носителях информации нарочно;

передача ПДн на электронных и бумажных носителях посредством почтовой связи;

передача ПДн по каналам электрической связи.

Перед осуществлением передачи ПДн проверяется основание на осуществление такой передачи и наличие согласия на передачу ПДн в согласии субъекта персональных данных на обработку ПДн, или наличие иных законных оснований.

Передача ПДн должна осуществляться на основании:

договора с третьей стороной, которой осуществляется передача ПДн;

запроса, полученного от третьей стороны, которой осуществляется передача ПДн;

исполнения возложенных законодательством Российской Федерации на Управление функций, полномочий и обязанностей.

Передача ПДн без согласия субъекта персональных данных или иных законных оснований запрещается.

### 17. Осуществление хранения персональных данных

Хранение ПДн в Управлении допускается только в форме документов - зафиксированной на материальном носителе информации (содержащей персональные данные) с реквизитами, позволяющими её идентифицировать и определить субъекта персональных данных. При этом предусматриваются следующие виды документов:

изобразительный документ - документ, содержащий информацию, выраженную посредством изображения какого-либо объекта;

фотодокумент - изобразительный документ, созданный фотографическим способом;

текстовый документ - документ, содержащий речевую информацию, зафиксированную любым типом письма или любой системой звукозаписи;

письменный документ - текстовый документ, информация которого зафиксирована любым типом письма;

рукописный документ - письменный документ, при создании которого знаки письма наносят от руки;

машинописный документ - письменный документ, при создании которого знаки письма наносят техническими средствами;

документ на машинном носителе - документ, созданный с использованием носителей и способов записи, обеспечивающих обработку его информации электронно-вычислительной машиной.

Хранение ПДн в Управлении осуществляется в форме, позволяющей определить субъект персональных данных, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен Федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

Хранение ПДн в ИСПДн и вне таких систем в Управлении осуществляется только на таких материальных носителях информации и с применением такой технологии её хранения, которые обеспечивают защиту этих данных от неправомерного или случайного:

- доступа к ним;
- их уничтожения;
- изменения;
- блокирования;
- копирования;
- предоставления;
- распространения.

### 18. Осуществление блокирования персональных данных

Блокированием ПДн называется временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн).

Блокирование ПДн конкретного субъекта персональных данных должно

осуществляться во всех ИСПДн Управления, включая архивы баз данных, содержащих такие персональные данные.

Блокирование ПДн в Управлении осуществляется:

в случае выявления неправомерной обработки ПДн при обращении субъекта персональных данных или его представителя, либо по запросу субъекта персональных данных или его представителя, либо уполномоченного органа по защите прав субъектов персональных данных с момента такого обращения или получения указанного запроса на период проверки;

в случае отсутствия возможности уничтожения ПДн в установленные сроки до их уничтожения.

После устранения выявленной неправомерной обработки ПДн Управление осуществляет снятие блокирования ПДн.

#### 19. Осуществление обезличивания персональных данных

Обезличивание ПДн в Управлении при обработке ПДн с использованием средств автоматизации осуществляется на основании нормативных правовых актов, правил, инструкций, руководств, регламентов и иных документов для достижения заранее определенных и заявленных целей.

Допускается производить обезличивание ПДн при обработке ПДн без использования средств автоматизации способом, исключающим дальнейшую обработку этих ПДн с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

#### 20. Осуществление удаления и уничтожения персональных данных

Уничтожение ПДн - это действия, в результате которых становится невозможным восстановить содержание ПДн в информационной системе ПДн и (или) в результате которых уничтожаются материальные носители ПДн.

Уничтожение ПДн в Управлении производится в следующих случаях:

если обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено Федеральным законом;

персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки;

в случае выявления неправомерной обработки ПДн, если обеспечить правомерность обработки ПДн невозможно;

в случае достижения цели обработки ПДн;

в случае отзыва субъектом персональных данных согласия на обработку его ПДн и в случае, если сохранение ПДн более не требуется для целей обработки ПДн.

По факту уничтожения ПДн обязательно проверяется необходимость уведомления об этом и в случае наличия такого требования осуществляется уведомление указанных в таком требовании лиц.

При уничтожении ПДн необходимо:

убедиться в необходимости уничтожения ПДн;

убедиться в том, что уничтожаются те персональные данные, которые предназначены для уничтожения;

уничтожить персональные данные подходящим способом в соответствии с



настоящими Правилами или способом, указанным в соответствующем требовании или распорядительном документе;

проверить наличие необходимости уведомления об уничтожении ПДн;

при необходимости уведомить об уничтожении ПДн требуемых лиц.

При уничтожении ПДн применяются следующие способы:

измельчение в бумагорезательной (бумагоуничтожительной) машине - для документов, исполненных на бумаге;

тщательное вымарывание (с проверкой тщательности вымарывания) - для сохранения возможности обработки иных данных, зафиксированных на материальном носителе, содержащем персональные данные;

физическое уничтожение частей носителей информации - разрушение или сильная деформация - для носителей информации на жестком магнитном диске, CD (DVD)-дисках, USB- и Flash-носителях;

стирание с помощью сертифицированных средств уничтожения информации - для записей в базах данных и отдельных документов на машинном носителе.

При уничтожении ПДн необходимо учитывать их наличие в архивных базах данных и производить уничтожение во всех копиях баз данных, если иное не установлено действующим законодательством Российской Федерации.

При необходимости уничтожения части ПДн допускается уничтожать материальный носитель одним из указанных в настоящем Положении способов, с предварительным копированием сведений, не подлежащих уничтожению, способом, исключающим одновременное копирование ПДн, подлежащих уничтожению.

Уничтожение ПДн производится лицами, обрабатывающими персональные данные в соответствующей ИСПДн, в которой производится уничтожение ПДн, в присутствии лица, ответственного за организацию обработки ПДн в Управлении.

По факту уничтожения ПДн составляется акт об уничтожении ПДн, который подписывается лицами, производившими уничтожение.

## 21. Права и обязанности субъекта персональных данных и Управления при обработке персональных данных

### 21.1. Права субъекта персональных данных

Субъект персональных данных, чьи персональные данные обрабатываются в Управлении, имеет право:

на получение сведений о подтверждении факта обработки ПДн Управлением;

на получение сведений о правовых основаниях и цели обработки ПДн;

на получение сведений о цели и применяемых Управлением способах обработки ПДн;

на получение сведений о наименовании и месте нахождения Управления, сведений о лицах (за исключением сведений о служащих Управления), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Управлением или на основании Федерального закона;

на получение сведений об обрабатываемых ПДн, относящихся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом;

на получение сведений о сроках обработки ПДн, в том числе сроках их хранения;

на получение сведений о порядке осуществления субъектом персональных данных своих прав, предусмотренных законодательством в области ПДн;

на получение информации об осуществленной или о предполагаемой трансграничной передаче данных;

на получение сведений о наименовании и адресе лица, осуществляющего обработку ПДн по поручению Управления, если обработка поручена или будет поручена такому лицу;

на получение иных сведений, предусмотренных законодательством в области ПДн и другими федеральными законами;

требовать от Управления уточнения его ПДн, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

принимать предусмотренные законом меры по защите своих прав;

требовать от Управления предоставления ему ПДн в доступной форме;

повторного обращения и запроса в целях получения сведений и ознакомления с его персональными данными;

требовать разъяснения порядка принятия решения на основании исключительно автоматизированной обработки его ПДн;

заявить возражение против принятия решения на основании исключительно автоматизированной обработки ПДн решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы;

требовать разъяснения порядка принятия и возможные юридические последствия принятия решения на основании исключительно автоматизированной обработки ПДн решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, а также разъяснения порядка защиты субъектом персональных данных своих прав и законных интересов;

обжаловать действия или бездействие Управления в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке, если субъект персональных данных считает, что Управление осуществляет обработку его ПДн с нарушением требований Федерального закона или иным образом нарушает его права и свободы;

на защиту своих прав и законных интересов;

требовать предоставления безвозмездно субъекту персональных данных или его представителю возможности ознакомления с персональными данными, относящимися к этому субъекту персональных данных;

принимать решение о предоставлении его ПДн и давать согласие на их обработку свободно, своей волей и в своем интересе;

отзывать согласие на обработку ПДн.

Кроме указанных прав в вопросах обработки его ПДн субъект персональных данных обладает другими правами, предоставляемыми ему действующим законодательством Российской Федерации.

## 21.2. Обязанности субъекта персональных данных

Субъект персональных данных, чьи персональные данные обрабатываются в Управлении, обязан:

предоставлять свои персональные данные в случаях, когда федеральными законами предусматриваются случаи обязательного предоставления субъектом персональных данных своих ПДн;

с целью соблюдения его законных прав и интересов подавать только достоверные персональные данные.

Кроме указанных обязанностей в вопросах обработки его ПДн на субъекта персональных данных налагаются иные обязанности, предусмотренные действующим законодательством Российской Федерации.

## 21.3. Права Управления при обработке персональных данных

Управление при обработке ПДн имеет право:

обрабатывать персональные данные в соответствии с действующим законодательством Российской Федерации;

поручить обработку ПДн другому лицу с согласия субъекта персональных данных, если иное не предусмотрено Федеральным законом, на основании заключаемого с этим лицом договора;

мотивированно отказать субъекту персональных данных в выполнении повторного запроса в целях получения сведений, касающихся обработки его ПДн, при нарушении субъектом персональных данных своих обязанностей по подаче такого запроса;

ограничить право субъекта персональных данных на доступ к его персональным данным в соответствии с федеральными законами, в том числе, если обработка ПДн осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

ограничить право субъекта персональных данных на доступ к его персональным данным в соответствии с федеральными законами, если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;

отказать субъекту персональных данных в выполнении запроса в целях получения сведений, касающихся обработки его ПДн, в случае, если субъект персональных данных уведомлен об осуществлении обработки его ПДн соответствующим оператором;

отказать субъекту персональных данных в выполнении запроса в целях получения сведений, касающихся обработки его ПДн, в случае, если персональные данные получены на основании Федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;

отказать субъекту персональных данных в выполнении запроса в целях получения сведений, касающихся обработки его ПДн, в случае, если персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;

отказать субъекту персональных данных в выполнении запроса в целях получения сведений, касающихся обработки его ПДн, в случае, если осуществляется обработка ПДн для статистических или иных исследовательских целей, если при этом не нарушаются права и законные интересы субъекта персональных данных;

отказать субъекту ПДн в выполнении запроса в целях получения сведений, касающихся обработки его ПДн, в случае, если предоставление субъекту персональных данных таких сведений нарушает права и законные интересы третьих лиц;

самостоятельно определять состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных действующим законодательством в области ПДн, если иное не предусмотрено федеральными законами;

осуществлять или обеспечивать блокирование или уничтожение ПДн, если обеспечить правомерность обработки ПДн невозможно;

осуществлять или обеспечивать уничтожение ПДн в случае достижения цели обработки ПДн;

в случае достижения цели обработки ПДн продолжить обработку ПДн, если обработка ПДн осуществляется без согласия субъекта персональных данных на основании пункта 4 статьи 21 Федерального закона;

в случае отзыва субъектом ПДн согласия на обработку его ПДн продолжить обработку ПДн, если обработка ПДн осуществляется без согласия субъекта персональных данных на основании пункта 5 статьи 21 Федерального закона;

в случае отсутствия возможности уничтожения ПДн осуществить блокирование таких ПДн и обеспечить уничтожение ПДн в срок не более чем шесть месяцев, если иной срок не установлен Федеральным законом;

осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку ПДн, указанных в пункте 2 статьи 22 Федерального закона.

Кроме указанных прав в вопросах обработки ПДн субъектов персональных данных Управление обладает другими правами, предоставляемыми ему действующим законодательством Российской Федерации.

#### 21.4. Обязанности Управления при обработке персональных данных

Управление области при обработке ПДн обязано:

строго соблюдать принципы и правила обработки ПДн;

в случае если обработка ПДн осуществляется по поручению оператора, строго соблюдать и выполнять требования поручения оператора;

не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено Федеральным законом;

по требованию субъекта персональных данных, либо по решению суда или иных уполномоченных государственных органов исключить из общедоступных источников ПДн сведения о субъекте персональных данных;

обеспечить конкретность и информированность согласия на обработку ПДн;

получать согласие на обработку ПДн;

в случае получения согласия на обработку ПДн от представителя субъекта

персональных данных проверять полномочия данного представителя на дачу согласия от имени субъекта персональных данных;

предоставить доказательство получения согласия субъекта персональных данных на обработку его ПДн или доказательство наличия оснований обработки ПДн без получения согласия;

соблюдать требования к содержанию согласия в письменной форме субъекта персональных данных на обработку его ПДн;

немедленно прекратить обработку специальных категорий ПДн, если устранены причины, вследствие которых осуществлялась обработка, если иное не установлено Федеральным законом;

убедиться в том, что иностранным государством, на территорию которого осуществляется передача ПДн, обеспечивается адекватная защита прав субъектов персональных данных до начала осуществления трансграничной передачи ПДн;

предоставить субъекту персональных данных сведения по запросу субъекта персональных данных в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких ПДн;

мотивировать и представить доказательства обоснованности отказа в выполнении повторного запроса субъекта персональных данных;

разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его ПДн и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом персональных данных своих прав и законных интересов;

рассмотреть возражение против принятия решения на основании исключительно автоматизированной обработки его ПДн и уведомить субъект персональных данных о результатах рассмотрения такого возражения;

предоставить субъекту персональных данных по его просьбе информацию, касающуюся обработки его ПДн;

разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные, если предоставление ПДн является обязательным в соответствии с законодательством Российской Федерации;

до начала обработки ПДн, полученных не от субъекта персональных данных, предоставить субъекту персональных данных информацию о своем наименовании и адресе, цели обработки ПДн и её правовом основании, предполагаемых пользователей ПДн, установленные права субъекта персональных данных, источник получения ПДн;

принимать меры, необходимые и достаточные для обеспечения выполнения своих обязанностей в области ПДн, если иное не предусмотрено федеральными законами;

опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПДн, к сведениям о реализуемых требованиях к защите ПДн;

по запросу уполномоченного органа по защите прав субъектов персональных данных представить документы и локальные акты, определяющие политику в отношении обработки ПДн, и сведения о реализуемых требованиях к защите ПДн;

принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн;

сообщить субъекту персональных данных или его представителю информацию о наличии ПДн, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо при получении запроса субъекта персональных данных или его представителя;

в случае отказа в предоставлении информации о наличии ПДн о соответствующем субъекте персональных данных или ПДн субъекту персональных данных или его представителю при их обращении, либо при получении запроса субъекта персональных данных или его представителя дать в письменной форме мотивированный ответ;

предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных;

внести в персональные данные необходимые изменения или уничтожить такие персональные данные в случае предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными;

строго соблюдать сроки по уведомлениям, блокированию и уничтожению ПДн;

уведомить субъекта персональных данных или его представителя о внесённых изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы;

сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию;

в случае выявления неправомерной обработки ПДн при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных Управление обязано осуществить блокирование неправомерно обрабатываемых ПДн, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки;

уничтожить персональные данные или обеспечить их уничтожение в случае, если обеспечить правомерность обработки ПДн невозможно;

в случае выявления неточных ПДн при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных Управление обязано осуществить блокирование ПДн, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки,

если блокирование ПДн не нарушает права и законные интересы субъекта персональных данных или третьих лиц;

уточнить персональные данные либо обеспечить их уточнение (если обработка ПДн осуществляется другим лицом, действующим по поручению оператора) и снять блокирование ПДн в случае подтверждения факта неточности ПДн на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов;

прекратить неправомерную обработку ПДн или обеспечить прекращение неправомерной обработки ПДн лицом, действующим по поручению оператора в случае выявления неправомерной обработки ПДн, осуществляемой оператором или лицом, действующим по поручению оператора;

уведомить субъект персональных данных или его представителя, а в случае если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган об устранении допущенных нарушений или об уничтожении ПДн;

уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку ПДн;

уведомить уполномоченный орган по защите прав субъектов персональных данных в случае изменения сведений, указанных в уведомлении о своем намерении осуществлять обработку ПДн;

назначить лицо, ответственное за организацию обработки ПДн;

предоставлять лицу, ответственному за организацию обработки ПДн, необходимые сведения;

ознакомить служащих Управления, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе требованиями к защите ПДн, документами, определяющими политику в отношении обработки ПДн, приказами Управления по вопросам обработки ПДн, и обучить таких служащих;

прекратить обработку ПДн или обеспечить её прекращение (если обработка ПДн осуществляется другим лицом, действующим по поручению оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению оператора):

в случае достижения цели обработки ПДн;

в случае отзыва субъектом персональных данных согласия на обработку его ПДн, если обработка ПДн без согласия субъекта персональных данных запрещена Федеральным законом;

## 22. Процедуры, направленные на предотвращение и выявление нарушений законодательства в отношении обработки персональных данных и устранение таких последствий

К процедурам, направленным на предотвращение и выявление нарушений законодательства в отношении обработки ПДн и устранение таких последствий, относятся:

выполнение предусмотренных законодательством о ПДн обязанностей, возложенных на Управление;  
 обеспечение личной ответственности служащих Управления, осуществляющих обработку либо доступ к персональным данным;  
 организация рассмотрения запросов субъектов персональных данных или их представителей и ответов на такие запросы;  
 организация внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн, установленным действующим законодательством в области ПДн;  
 сокращение объёма обрабатываемых данных;  
 сокращение числа должностей служащих Управления, замещение которых предусматривает осуществление обработки ПДн либо осуществление доступа к персональным данным;  
 стандартизация операций осуществляемых с персональными данными;  
 определение порядка доступа служащих Управления в помещения, в которых ведется обработка ПДн;  
 проведение необходимых мероприятий по обеспечению безопасности ПДн и носителей их содержащих;  
 блокирование, внесение изменений и уничтожение ПДн в предусмотренных действующим законодательством в области ПДн случаях;  
 оповещение субъектов персональных данных в предусмотренных действующим законодательством в области ПДн случаях;  
 разъяснение прав субъекту персональных данных в вопросах обработки и обеспечения безопасности их ПДн;  
 оказание содействия правоохранительным органам в случаях нарушений законодательства в отношении обработки ПДн;  
 публикация на официальном сайте Управления документов, определяющих политику в отношении обработки ПДн.

### 23. Требования к служащим Управления, осуществляющим обработку персональных данных

Управление осуществляет ознакомление служащих, непосредственно осуществляющих обработку ПДн или доступ к ним, с положениями законодательства Российской Федерации о ПДн (в том числе с требованиями к защите ПДн), приказами Управления по вопросам обработки ПДн, включая настоящие Правила:

при оформлении служебного контракта;  
 при первоначальном допуске к обработке ПДн в ИСПДн;  
 при назначении на новую должность, связанную с обработкой ПДн или доступом к ним;  
 после внесения изменений в действующее законодательство Российской Федерации о ПДн, в приказы Управления по вопросам обработки ПДн, включая настоящие Правила.

Служащие Управления, непосредственно осуществляющие обработку ПДн или доступ к ним обязаны:

соблюдать принципы обработки ПДн;  
 соблюдать положения действующего законодательства Российской Федерации в области ПДн;



знать и соблюдать инструкции, руководства и иные эксплуатационные документы на применяемые средства автоматизации, в том числе программное обеспечение, и средства защиты информации;

не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации;

не допускать нарушений требований и правил обработки и обеспечения безопасности ПДн;

обо всех подозрениях и ставших известными случаях нарушений требований и правил обработки и обеспечения безопасности ПДн сообщать лицу, ответственному за обработку ПДн и администратору безопасности ИСПДн.

Служащие Управления несут личную ответственность за соблюдение указанных обязанностей в предусмотренном действующим законодательством Российской Федерации объеме.

## 24. Конфиденциальность персональных данных

Запрет раскрытия ПДн третьим лицам и распространения ПДн без согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации, служащими Управления и иными лицами, получившим доступ к ПДн, называется конфиденциальностью ПДн.

### 24.1. Режим ограниченного доступа к персональным данным

С целью реализации требований действующего законодательства Российской Федерации в области ПДн по обеспечению конфиденциальности ПДн в Управлении вводится режим ограниченного доступа к ПДн.

Создание режима ограниченного доступа к ПДн включает в себя:

разработку и последующее уточнение настоящих Правил в части, касающейся обеспечения конфиденциальности ПДн и обеспечения безопасности ПДн;

разработку и корректировку Перечня помещений, предназначенных для обработки ПДн;

разработку и корректировку Перечня должностей служащих Управления, замещение которых предусматривает осуществление обработки ПДн либо осуществление доступа к ПДн;

разработку и корректировку Перечня должностей служащих Управления ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных;

разработку и корректировку Перечня информационных ресурсов, содержащих ПДн (мест расположения баз данных или иных документов и массивов, содержащих ПДн);

оборудование помещений, предназначенных для обработки ПДн на предмет соответствия требованиям к инженерно-технической укреплённости по защите объектов от преступных посягательств;

проведение мероприятий по обследованию помещений, предназначенных для обработки ПДн, проведением, при необходимости, доработок помещений по инженерно-технической укреплённости по защите объектов от преступных посягательств;

внесение изменений в должностные регламенты (дополнения в служебные контракты) служащих Управления, предусматривающие регулирование отношений по использованию информации ограниченного доступа;

получение расписок в ознакомлении служащих, доступ которых к информации ограниченного доступа, обладателем которой является Управление, необходим для выполнения ими своих трудовых обязанностей, с перечнем информации ограниченного доступа, установленным режимом ограничения доступа к информации и мерами ответственности за его нарушение;

передачу (возврат) служащими при прекращении или расторжении служебного контракта имеющихся в пользовании такого служащего материальных носителей информации, содержащей ПДн;

проведение занятий и иных мероприятий по повышению уровня знаний (квалификации) служащих, допущенных к обработке ПДн, по вопросам обработки и обеспечения безопасности ПДн;

создание и ведение списков лиц, имеющих доступ в помещения, в которых обрабатываются ПДн;

документирование и реализацию разрешительной системы доступа (матриц доступа) к информационным (программным) ресурсам в ИСПДн Управления;

разработку инструкций о действиях служащих в отношении носителей ПДн при возникновении чрезвычайных ситуаций (стихийных бедствий, техногенных катастроф, наводнений, пожаров, нарушениях правопорядка и др.);

разработку инструкций для служащих по вопросам обеспечения безопасности ПДн.

#### 24.2. Порядок использования материальных (внешних) носителей информации

Все материальные (внешние) носители информации (далее - носители), используемые для обработки ПДн, должны быть зарегистрированы в установленном порядке. При необходимости они могут маркироваться пометкой "Для служебного пользования" ("ДСП"), либо любой другой, например: "Персональные данные" ("ПДн"), "Содержит персональные данные".

Автоматизированная обработка информации с использованием данных носителей должна осуществляться на аттестованных по требованиям безопасности автоматизированных рабочих местах или в защищенной ИСПДн.

Размножение (тиражирование) носителей осуществляется только с письменного разрешения исполнителя. Учёт размноженных носителей осуществляется поэкземплярно.

Носители должны храниться в надёжно запираемых хранилищах. Места хранения носителей определяются приказом Управления.

При необходимости направления носителя(ей) в несколько адресов составляется указатель рассылки, в котором поадресно проставляются номера экземпляров отправляемых носителей. Указатель рассылки подписывается исполнителем и его руководителем.

Уничтожение носителей, утративших своё практическое значение и не имеющих исторической ценности, производится по акту. В учетных формах об этом делается отметка со ссылкой на соответствующий акт.

Проверка наличия носителей проводится не реже одного раза в год.

По фактам утраты носителей назначается комиссия для расследования обстоятельств утраты.

На утраченные носители составляется акт, на основании которого делаются соответствующие отметки в учетных формах.

## 25. Обеспечение безопасности персональных данных при их обработке

В соответствии с требованиями действующего законодательства в области ПДн при обработке ПДн Управление обязано принимать необходимые правовые, организационные и технические меры для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также от иных неправомерных действий.

Безопасность ПДн достигается путем исключения несанкционированного, в том числе случайного, доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иных несанкционированных действий.

Для обеспечения безопасности ПДн при их обработке в информационных системах должна осуществляться защита речевой информации и информации, обрабатываемой техническими средствами, а также информации, представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе.

### 25.1. Принципы обеспечения безопасности персональных данных при их обработке

Обеспечение безопасности ПДн в Управлении должно осуществляться на основе следующих принципов:

- соблюдение конфиденциальности ПДн и иных характеристик их безопасности;

- реализация права на доступ к персональным данным лиц, доступ которых к таким данным разрешается в рамках действующего законодательства Российской Федерации и приказами Управления;

- обеспечение защиты информации, содержащей персональные данные, от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

- проведение мероприятий, направленных на предотвращение несанкционированной передачи их лицам, не имеющим права доступа к такой информации;

- своевременное обнаружение фактов несанкционированного доступа к персональным данным;

- недопущение воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование;

- возможность незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- постоянный контроль за обеспечением уровня защищённости ПДн;

- применение средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия требованиям безопасности ПДн.

## 25.2. Требования по уровню обеспечения безопасности

С целью установления методов и способов защиты информации, необходимых для обеспечения безопасности ПДн, определяется уровень защищённости ПДн в зависимости от объёма обрабатываемых ими ПДн и угроз безопасности жизненно важным интересам личности, общества и государства.

Определение уровня защищённости ПДн включает в себя следующие этапы:

сбор и анализ исходных данных по ИСПДн;

присвоение ИСПДн соответствующего уровня защищённости ПДн и его документальное оформление.

При определении уровня защищённости ПДн учитываются следующие исходные данные:

категория обрабатываемых в ИСПДн ПДн;

объём обрабатываемых ПДн (количество субъектов персональных данных, ПДн которых обрабатываются ИСПДн);

заданные характеристики безопасности ПДн, обрабатываемых в ИСПДн;

структура ИСПДн;

наличие подключений ИСПДн к сетям связи общего пользования и (или) сетям международного информационного обмена;

режим обработки ПДн;

режим разграничения прав доступа пользователей ИСПДн;

местонахождение технических средств ИСПДн.

В случае выделения в составе ИСПДн подсистем, каждая из которых является информационной системой, ИСПДн в целом присваивается уровень защищённости ПДн, соответствующий наиболее высокому уровню защищённости ПДн входящих в нее подсистем.

Определение уровня защищённости ПДн проводится на этапе её создания или в ходе эксплуатации (для ранее введенных в эксплуатацию и (или) модернизируемых ИСПДн).

Результаты определения уровня защищённости ПДн оформляются соответствующим актом классификации уровня защищённости ПДн.

## 25.3. Состав мероприятий по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации

Обработка ПДн, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории ПДн можно было определить места хранения ПДн (материальных носителей) и установить перечень лиц, осуществляющих обработку ПДн либо имеющих к ним доступ.

Необходимо обеспечивать раздельное хранение ПДн (материальных носителей), обработка которых осуществляется в различных целях.

При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность ПДн и исключающие несанкционированный к ним доступ.

## 25.4. Состав мероприятий по обеспечению безопасности персональных данных при их обработке, осуществляемой с использованием средств автоматизации

Мероприятия по обеспечению безопасности ПДн при их обработке в

информационных системах ПДн в Управлении включают в себя:

- определение угроз безопасности ПДн при их обработке, формирование на их основе модели угроз;

- разработку на основе модели угроз системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего класса информационных систем;

- проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

- установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

- обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

- учёт применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей ПДн;

- учёт лиц, допущенных к работе с персональными данными в информационной системе;

- контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

- разбирательство и составление заключений по фактам несоблюдения условий хранения носителей ПДн, использования средств защиты информации, которые могут привести к нарушению конфиденциальности ПДн или другим нарушениям, приводящим к снижению уровня защищённости ПДн, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

- описание системы защиты ПДн.

К методам и способам защиты информации в ИСПДн относятся:

- методы и способы защиты информации, обрабатываемой техническими средствами информационной системы, от несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иных несанкционированных действий (далее - методы и способы защиты информации от несанкционированного доступа);

- методы и способы защиты речевой информации, а также информации, представленной в виде информативных электрических сигналов, физических полей, от несанкционированного доступа к персональным данным, результатом которого может стать копирование, распространение ПДн, а также иных несанкционированных действий (далее - методы и способы защиты информации от утечки по техническим каналам).

Методами и способами защиты информации от несанкционированного доступа являются:

- реализация разрешительной системы допуска пользователей к информационным ресурсам, информационной системе и связанным с её использованием документам;

- ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку ПДн, а также хранятся носители информации;

- разграничение доступа пользователей к информационным ресурсам,

программным средствам обработки (передачи) и защиты информации;

регистрация действий пользователей и обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;

учёт и хранение съёмных носителей информации и их использование, исключаящее хищение, подмену и уничтожение;

резервирование технических средств, дублирование массивов и носителей информации;

использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;

использование защищённых каналов связи;

размещение технических средств, позволяющих осуществлять обработку ПДн, в пределах охраняемой территории;

организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку ПДн;

предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок.

В ИСПДн, имеющих подключение к информационно-телекоммуникационным сетям международного информационного обмена (сетям связи общего пользования) или при функционировании которых предусмотрено использование съёмных носителей информации, используются средства антивирусной защиты.

При взаимодействии информационных систем с информационно-телекоммуникационными сетями международного информационного обмена (сетями связи общего пользования) наряду с указанными методами и способами основными методами и способами защиты информации от несанкционированного доступа являются:

межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрывания структуры информационной системы;

обнаружение вторжений в информационную систему, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности ПДн;

анализ защищённости информационных систем, предполагающий применение специализированных программных средств (сканеров безопасности);

защита информации при её передаче по каналам связи;

использование смарт-карт, электронных замков и других носителей информации для надёжной идентификации и аутентификации пользователей;

использование средств антивирусной защиты;

централизованное управление системой защиты ПДн информационной системы.

Защита речевой информации и информации, представленной в виде информативных электрических сигналов и физических полей, осуществляется в случаях, когда при определении угроз безопасности ПДн и формировании модели угроз применительно к информационной системе являются актуальными угрозы утечки акустической речевой информации, угрозы утечки видовой информации и угрозы утечки информации по каналам побочных электромагнитных излучений и наводок.

Для исключения утечки ПДн за счёт побочных электромагнитных излучений и наводок в ИСПДн с установленным первым уровнем защищённости ПДн могут применяться следующие методы и способы защиты информации:

- использование технических средств в защищённом исполнении;
- использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;
- размещение объектов защиты в соответствии с предписанием на эксплуатацию;
- размещение понижающих трансформаторных подстанций электропитания и контуров заземления технических средств в пределах охраняемой территории;
- обеспечение развязки цепей электропитания технических средств с помощью защитных фильтров, блокирующих (подавляющих) информативный сигнал;
- обеспечение электромагнитной развязки между линиями связи и другими цепями вспомогательных технических средств и систем, выходящими за пределы охраняемой территории, и информационными цепями, по которым циркулирует защищаемая информация.

При применении в информационных системах функции голосового ввода ПДн в информационную систему или функции воспроизведения информации акустическими средствами информационных систем для ИСПДн должны реализовываться методы и способы защиты акустической (речевой) информации.

Методы и способы защиты акустической (речевой) информации заключаются в реализации организационных и технических мер для обеспечения звукоизоляции ограждающих конструкций помещений, в которых расположена информационная система, их систем вентиляции и кондиционирования, не позволяющей вести прослушивание акустической (речевой) информации при голосовом вводе ПДн в информационную систему или воспроизведении информации акустическими средствами.

Величина звукоизоляции определяется оператором исходя из характеристик помещения, его расположения и особенностей обработки ПДн в информационной системе.

Размещение устройств вывода информации средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео и буквенно-цифровой информации, входящих в состав ИСПДн, в помещениях, в которых они установлены, осуществляется таким образом, чтобы была исключена возможность просмотра посторонними лицами текстовой и графической видовой информации, содержащей ПДн.

Обмен ПДн при их обработке в ИСПДн осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) путем применения технических средств, в том числе средств криптографической защиты информации.

## 26. Требования к помещениям, в которых производится обработка персональных данных

Размещение оборудования ИСПДн, специального оборудования и охрана помещений, в которых ведется работа с ПДн, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей

ПДн и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

Помещения, в которых располагаются технические средства ИСПДн или хранятся носители ПДн, должны соответствовать требованиям пожарной безопасности, установленным действующим законодательством Российской Федерации.

Кроме указанных мер по специальному оборудованию и охране помещений, в которых устанавливаются криптографические средства защиты информации или осуществляется их хранение, реализуются дополнительные требования, определяемые методическими документами Федеральной службы безопасности России.

#### 27. Мероприятия при возникновении обстоятельств непреодолимой силы (форс-мажор)

В случае появления обстоятельств непреодолимой силы, возникших в результате событий чрезвычайного характера, которые Управление не может предвидеть, за возникновение которых оно не несёт ответственности и не может предотвратить разумными мерами, должностные лица Управления обязаны принять все возможные меры по недопущению нарушения прав субъекта персональных данных.

К обстоятельствам непреодолимой силы относятся события:

землетрясение, наводнение, пожар, забастовки, насильственные или военные действия любого характера, препятствующие исполнению требований законодательства в области ПДн.