ПРАВИЛА
обработки персональных данных в ТОГБУЗ «ГКБ №3 г. Тамбова»

1. Общие положения

Настоящий документ устанавливает правила рассмотрения запросов субъектов персональных данных или их представителей направленных на предотвращение нарушений законодательства Российской Федерации при обработке персональных данных, определяет сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований регламентирует порядок работы с документами и электронными и магнитными носителями, содержащими персональные данные в ТОГБУЗ «ГКБ №3 г. Тамбова» (далее – Учреждение), в целях реализации: Трудового кодекса Российской Федерации, Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Федерального закона от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», Постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановления 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 правыми актами, операторами, являющимися государственными или муниципальными органами», Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

При организации обработки и защиты ПДн необходимо руководствоваться следующими документами:

Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

Требованиями к защите персональных данных при их обработке в информационных системах персональных данных (утверждены постановлением Правительства Российской Федерации от 01 ноября 2012 г. № 1119);

Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации (утверждено постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687);

Положением по аттестации объектов информатизации по требованиям безопасности информации (утверждено председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г.);

Специальными требованиями и рекомендациями по технической защите конфиденциальной информации (утверждены приказом председателя Гостехкомиссии России от 30 августа 2002 г. № 282);

нормативными и методическими документами по технической защите информации Гостехкомиссии России, ФСТЭК России и ФСБ России.

2. Категории субъектов персональных данных

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

граждан, проживающих в Тамбовской области;

граждан, проживающих в другом субъекте Российской Федерации;

сотрудников Учреждения.

Обработка персональных данных сотрудников Учреждения и кандидатов на замещение вакантных должностей Учреждения осуществляется в соответствии с законодательством о государственной гражданской службе и трудовым законодательством Российской Федерации.

3. Принципы обработки персональных данных

Обработка ПДн в Учреждения должно 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 объема 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 оператором при удалении или уточнении неполных или неточных данных;

осуществления хранения ПДн оператором в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом 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 федеральным законом;

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;

обязанности лица, осуществляющего обработку ПДн по поручению оператора, соблюдать принципы и правила обработки ПДн;

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 сотрудников действующим

законодательством и иными нормативными актами по обработке ПДн;

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 (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

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

Цели обработки ПДн должны быть четко определены и соответствовать:

заявленным в Уставе, регламенте Учреждения и положениях о структурных подразделениях Учреждения основным полномочиям и правам;

задачам и функциям структурных подразделений (должностных лиц) Учреждения, указанным в положениях о таких структурных подразделениях (должностных регламентах).

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 Учреждении осуществляется для следующих целей:

исполнения функций по оказанию услуг населению в сфере здравоохранения;

формирования и подготовки кадрового резерва.

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 Уставе, регламенте Учреждения и положениях о структурных подразделениях Учреждения основными полномочиями и правами Учреждения 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, в частности, при необходимости использования или распространения определенных 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 и использованию, и 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 ее 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;

общее описание используемых оператором способов обработки ПДн;

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 уточненными персональными данными.

5.2. Правила обработки персональных данных средствами автоматизации

Обработка ПДн средствами автоматизации в Учреждении допускается в следующих случаях:

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

обработка ПДн необходима для достижения целей, предусмотренных законом, для осуществления и выполнения возложенных законодательством Российской Федерации на Учреждение, 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 Учреждения 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 либо по его просьбе (персональные данные, сделанные общедоступными субъектом персональных данных);

осуществляется обработка ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с Федеральным законом.

Обработка ПДн средствами автоматизации должна осуществляться на основании правил, инструкций, руководств, регламентов и иных документов, определяющих технологический процесс обработки информации, содержащей такие данные, определенных для выполнения конкретных операций с заранее определенными целями, с учетом 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 дает согласие на их обработку свободно, своей волей и в своем интересе.

Согласие на обработку ПДн должно быть:

конкретным;

информированным;

сознательным.

Согласие на обработку ПДн Учреждению 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 признается согласие в форме электронного документа, подписанного в соответствии с Федеральным законом электронной подписью.

Получение согласия субъекта персональных данных в форме электронного документа на обработку его ПДн в целях предоставления государственных услуг, а также услуг, которые являются необходимыми и обязательными для предоставления государственных услуг, осуществляется в порядке, установленном Правительством Российской Федерации.

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 дает 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 Учреждении.

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

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.

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

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

с согласия субъекта персональных данных;

если иное не предусмотрено Федеральным законом;

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

путем принятия соответствующего акта.

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

В поручении оператора:

должен быть определен 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 Учреждением 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 Учреждение такого согласия.

В случае если Учреждение поручает обработку ПДн другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет Учреждение.

В случае необходимости получения согласия на обработку ПДн от субъекта

персональных данных обязанность получения такого согласия возлагается на Учреждение.

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

В случае поручения обработки ПДн средствами автоматизации Учреждения 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, Учреждение обязано добиться их определения и документального оформления.

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

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

Учреждение 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 Учреждении 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 Учреждении разрешается обработка сведений специальных категорий ПДн в минимально необходимом объеме при обязательном соблюдении любого из следующих условий:

субъект персональных данных дал согласие в письменной форме на обработку своих ПДн;

обработка ПДн осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, законодательством Российской Федерации о пенсиях по государственному пенсионному обеспечению, о трудовых пенсиях;

обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно;

обработка ПДн необходима для установления или осуществления прав субъекта персональных данных или третьих лиц;

обработка ПДн осуществляется в соответствии с законодательством об обязательных видах страхования, страховым законодательством;

обработка ПДн о судимости осуществляется в пределах полномочий, предоставленных Учреждением в соответствии с законодательством Российской Федерации.

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

Обработка специальных категорий ПДн должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась обработка, если иное не установлено Федеральным законом.

9.2. Правила обработки биометрических персональных данных

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

сведения, которые характеризуют физиологические и биологические особенности человека;

сведения, на основании которых можно установить его личность;

сведения, которые используются Учреждением для установления личности субъекта ПДн.

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

9.3. Правила обработки общедоступных персональных данных

Общедоступные персональные данные физических лиц, полученные из сторонних общедоступных источников ПДн, в Учреждении 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, так как в случае обработки общедоступных ПДн обязанность доказывания того, что обрабатываемые персональные данные являются общедоступными, возлагается на Учреждение. По достижении целей обработки общедоступных ПДн они подлежат немедленному уничтожению.

С целью информационного обеспечения и осуществления взаимодействия как внутри Учреждения, так и со сторонними физическими и юридическими лицами в Учреждении могут создаваться общедоступные источники ПДн. Создание общедоступного источника ПДн осуществляется по решению руководителя Учреждения. В решении о создании общедоступного источника ПДн должны быть указаны:

цель создания общедоступного источника ПДн;

ссылка на нормативный акт, устанавливающий необходимость создания общедоступного источника ПДн (при наличии);

перечень ПДн, которые вносятся в общедоступный источник ПДн;

порядок включения ПДн в общедоступный источник ПДн;

порядок уведомления пользователей общедоступного источника ПДн об исключении из него ПДн либо внесении в него изменений;

порядок получения письменного согласия субъекта персональных данных на

включение ПДн в общедоступный источник ПДн;

ссылка на нормативный акт, устанавливающий порядок исключения ПДн из общедоступного источника ПДн.

В общедоступный источник ПДн с письменного согласия субъекта персональных данных могут включаться: должность, фамилия, имя, отчество, абонентский номер рабочего телефона, место получения образования, достигнутые результаты и другая информация.

Включение в общедоступные источники персональных данных ПДн субъекта персональных данных допускается только на основании его письменного согласия.

Исключение ПДн из указанного общедоступного источника осуществляется при утрате необходимости в обработке таких данных, либо на основании заявления субъекта персональных данных в соответствии с действующим законодательством Российской Федерации.

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

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

правила обработки ПДн с целью однократного пропуска субъекта персональных данных на охраняемую территорию;

правила обработки ПДн при трансграничной передаче ПДн;

правила работы с обезличенными данными.

10.1. Правила обработки персональных данных с целью однократного пропуска субъекта персональных данных на охраняемую территорию

При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию Учреждения, должны соблюдаться следующие условия:

необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена правовым актом Учреждения, содержащим сведения о цели обработки ПДн, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (по должностям), имеющих доступ к материальным носителям и перечень лиц, ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки ПДн, а также сведения о порядке пропуска субъекта персональных данных на территорию Учреждения, без подтверждения подлинности ПДн, сообщенных субъектом персональных данных;

копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;

персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта персональных данных на охраняемую территорию.

10.2. Правила обработки персональных данных при трансграничной передаче персональных данных

Трансграничная передача ПДн Учреждением не осуществляется.

В случае принятия Учреждением 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;

предусмотренных федеральными законами, если это необходимо в целях защиты основ конституционного строя Российской Федерации, обеспечения обороны страны и безопасности государства, а также обеспечения безопасности, устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства;

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.

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

10.3. Правила работы с обезличенными данными

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

Порядок обезличивания в Учреждении установлен Правилами работы с обезличенными персональными данными Учреждения.

11. Правовое основание обработки персональных данных

Правовое основание обработки ПДн включает в себя:

определение законности целей обработки ПДн;

оценку вреда, который может быть причинен 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 определенных 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 так- же особые цели обработки ПДн (однократный пропуск на охраняемую территорию, 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 определенного и оформленного правового основания обработки ПДн не допускается.

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

Оценкой вреда, который может быть причинен 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 при выполнении заявленных в Уставе основных полномочий и прав, либо в рамках перечня задач и функций структурных подразделений (должностных лиц) Учреждения, указанных в положениях о таких структурных подразделениях (должностных регламентах) с учетом особых правил и способов обработки 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 причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн и принимаемых мер.

Обработка ПДн без оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн, не допускается.

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 Федеральным законом.

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

К таким характеристикам относятся:

требование по обеспечению защищенности от уничтожения ПДн;

требование по обеспечению защищенности от изменения ПДн;

требование по обеспечению защищенности от блокирования ПДн;

требование по обеспечению защищенности от иных несанкционированных действий.

Обеспечение указанных характеристик безопасности ПДн устанавливается федеральными законами и иными нормативными правовыми актами.

При определении правовым актом Учреждения необходимости обеспечения характеристик безопасности ПДн, отличных от конфиденциальности, основным критерием должна служить оценка вреда, который может быть причинен субъекту персональных данных, с чьим ПДн произошло нарушение таких характеристик безопасности.

Обработка ПДн без документально определенного и оформленного решения по определению характеристик безопасности ПДн не допускается.

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 определенных 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 Федеральным законом. При этом в случае наличия ПДн в таких документах, обработка которых более не требуется, производятся действия по уничтожению таких данных.

Включение в состав Архивного фонда Российской Федерации документов, содержащих персональные данные, осуществляется на основании экспертизы ценности документов и оформляется договором между Учреждением и государственным архивом. При этом объем передаваемых документов и условия передачи определяются условиями такого договора и действующими требованиями законодательства об архивном деле Российской Федерации.

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

Обработка ПДн без документально определенных и оформленных сроков обработки, в том числе хранения ПДн, не допускается.

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 Учреждении создается комиссия, определяющая факт достижения целей обработки ПДн и достижение предельных сроков хранения документов, содержащих персональные данные.

12. Действия (операции) с персональными данными

Обработкой ПДн называется любое действие (операция) или совокупность действий (операций), 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 (операций), совершаемых с персональными данными, не допускается.

13. Осуществление сбора персональных данных

13.1. Способы сбора персональных данных и источники их получения

В Учреждении 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 Учреждении 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 Федеральным законом, Учреждение 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 категорически запрещается.

Если персональные данные получены не от субъекта персональных данных, Учреждение 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 ее правовое основание;

сведения о предполагаемых пользователях ПДн;

сведения об установленных правах субъекта персональных данных;

сведения об источниках получения ПДн.

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

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

персональные данные получены Учреждением 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;

Учреждение 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 Учреждении 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 в Учреждении.

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

15. Осуществление записи и извлечения персональных данных

Запись ПДн в ИСПДн Учреждения 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 в Учреждении должна осуществляться с соблюдением настоящих Правил и действующего законодательства Российской Федерации.

В Учреждении приняты следующие способы передачи ПДн субъектов персональных данных:

передача ПДн на электронных и бумажных носителях информации нарочным;

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 Учреждение функций, полномочий и обязанностей.

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

17. Осуществление хранения персональных данных

Хранение ПДн в Учреждении допускается только в форме документов - зафиксированной на материальном носителе информации (содержащей персональные данные) с реквизитами, позволяющими ее 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 - текстовой 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 Учреждении осуществляется в форме, позволяющей определить субъекта 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 Учреждении осуществляется только на таких материальных носителях информации и с применением такой технологии ее 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 Учреждения, включая архивы баз данных, содержащих такие персональные данные.

Блокирование ПДн в Учреждении 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 Учреждение осуществляет снятие блокирования ПДн.

Решение о блокировании и снятии блокирования ПДн субъекта персональных данных принимается ответственным за организацию обработки ПДн в Учреждении.

19. Осуществление обезличивания персональных данных

Обезличивание ПДн в Учреждении 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 обезличивание ПДн при обработке ПДн без использования средств автоматизации производить 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 Учреждении производится только в следующих случаях:

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 необходимость 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, содержавшем персональные данные;

физическое уничтожение частей носителей информации - разрушение или сильная деформация - для носителей информации на жестком магнитном диске (уничтожению подлежат внутренние диски и микросхемы); CD (DVD)-дисках, USB- и Flash-носителях (уничтожению подлежат модули и микросхемы долговременной памяти);

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 базы 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, только в присутствии лица, ответственного за организацию обработки ПДн в Учреждении.

По факту уничтожения ПДн составляется акт об уничтожении ПДн, который подписывается лицами, производившими уничтожение, заверяется лицом, ответственным за организацию обработки ПДн в Учреждении, присутствовавшим при уничтожении, и утверждается руководителем Учреждения (заместителем руководителя Учреждения).

Хранение актов об уничтожении ПДн осуществляется в течение срока исковой давности, если иное не установлено нормативными правовыми актами Российской Федерации.

21. Способы обозначения документов, содержащих персональные данные

С целью доведения до сотрудников Учреждения фактов работы с документами, содержащими персональные данные, все такие документы (в том числе машинные носители и документы в электронном виде) подлежат специальному обозначению (маркированию или визуальному выделению).

На документах в правом верхнем углу проставляется:

в первой строке: "Содержит персональные данные";

во второй строке: Экз. №___.

В третьей строке при необходимости дополнительно могут проставляться иные реквизиты документа, в том числе его регистрационный номер по журналам учета.

В конце документа проставляется фамилия и инициалы лица (лиц) исполнившего и отпечатавшего документ, количество отпечатанных экземпляров, дата печати.

Ответственным за специальное обозначение документов является их исполнитель.

Специальное обозначение осуществляется при печати документов машинным способом или путем проставления штампа (клише) на ранее созданных документах и машинных носителях (в свободном месте на имеющихся наклейках или на специально наклеенном листе или корпусе носителя).

Специальное обозначение ранее созданных документов должно производиться при обращении к ним.

22. Права и обязанности субъекта персональных данных и Учреждения при обработке персональных данных

22.1. Права субъекта персональных данных

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

на получение сведений о подтверждении факта обработки ПДн Учреждением;

на получение сведений о правовых основаниях и цели обработки ПДн;

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

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

на получение сведений о 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 Учреждения, если обработка поручена или будет поручена такому лицу;

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

требовать от Учреждения 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 Учреждения 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 Учреждения в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке, если субъект персональных данных считает, что Учреждение осуществляет обработку его ПДн с нарушением требований Федерального закона или иным образом нарушает его права и свободы;

на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке;

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.

22.2. Обязанности субъекта персональных данных

Субъект персональных данных, чьи персональные данные обрабатываются в Учреждении, 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.

22.3. Права Учреждения при обработке персональных данных субъектов персональных данных

Учреждение при обработке ПДн субъектов персональных данных 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, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта;

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, в том числе, 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 оператор осуществляет обработку 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 федеральными законами;

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 Учреждение обладает другими правами, предоставляемыми ему действующим законодательством Российской Федерации.

22.4. Обязанности Учреждения при обработке персональных данных субъектов персональных данных

Учреждение при обработке ПДн субъектов персональных данных 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;

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

незамедлительно 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 субъекта 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 Федеральным законом;

до начала обработки ПДн, полученных не от субъекта персональных данных, предоставить субъекту персональных данных информацию о своем наименовании и адресе, цели обработки ПДн и ее 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 внесенных 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 оператор обязан 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;

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 оператор обязан 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;

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

уведомить субъекта 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;

прекратить обработку ПДн или обеспечить ее 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, если обработка ПДн осуществляется без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом;

в случае отзыва субъектом персональных данных согласия на обработку его ПДн, если обработка ПДн осуществляется без согласия субъекта персональных данных на

основаниях, предусмотренных Федеральным законом;

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;

неукоснительно соблюдать все требования настоящих Правил;

ознакомить сотрудников Учреждения, 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, локальными актами по вопросам обработки ПДн, и обучить таких сотрудников.

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

23. 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:

реализация мер, направленных на обеспечение выполнения оператором своих обязанностей;

выполнение предусмотренных законодательством о ПДн обязанностей, возложенных на Учреждение;

обеспечение личной ответственности сотрудников Учреждения, 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 и локальными актами Учреждения;

сокращение объема обрабатываемых данных;

сокращение числа должностей сотрудников Учреждения, замещение которых предусматривает осуществление обработки ПДн либо осуществление доступа к персональным данным;

стандартизация операций, осуществляемых с персональными данными;

определение порядка доступа сотрудников Учреждения в помещения, в которых ведется обработка ПДн;

проведение необходимых мероприятий по обеспечению безопасности ПДн и носителей их содержащих;

проведение периодических проверок условий обработки ПДн;

повышение осведомленности сотрудников Учреждения, занимающих должности, замещение которых предусматривает обработку ПДн либо доступ к ПДн, путем их ознакомления с положениями законодательства Российской Федерации о ПДн (в том числе с требованиями к защите ПДн), локальными актами Учреждения по вопросам обработки ПДн и организация обучения указанных сотрудников;

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 персональных;

публикация на официальном сайте Учреждения документов, определяющих политику в отношении обработки ПДн.

Указанный перечень процедур, направленных на предотвращение и выявление нарушений законодательства в отношении обработки ПДн и устранение таких последствий, является открытым и может дополняться мероприятиями в конкретных случаях.

24. Требования к служащим Учреждения, осуществляющим доступ к персональным данным или их обработку

Учреждение осуществляет ознакомление сотрудников, непосредственно осуществляющих обработку ПДн или доступ к ним, с положениями законодательства Российской Федерации о ПДн (в том числе с требованиями к защите ПДн), локальными актами Учреждения по вопросам обработки ПДн, включая настоящие Правила:

при оформлении служебного контракта;

после каждого перерыва в исполнении своих обязанностей на срок более 28 рабочих дней;

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, локальные акты Учреждения по вопросам обработки ПДн, включая настоящие Правила.

Сотрудники Учреждения, непосредственно осуществляющие обработку ПДн или доступ к ним обязаны:

неукоснительно следовать принципам обработки ПДн;

знать и строго соблюдать положения действующего законодательства Российской Федерации в области ПДн;

знать и строго соблюдать положения локальных актов Учреждения в области обработки и обеспечения безопасности ПДн;

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

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

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 в Учреждении.

Сотрудники Учреждения несут личную ответственность за соблюдение указанных обязанностей в предусмотренном действующим законодательством Российской Федерации объеме.

25. Конфиденциальность персональных данных

Запрет раскрытия ПДн третьим лицам и распространения ПДн без согласия субъекта персональных данных, если иное не предусмотрено Федеральным законом, Учреждением и иными лицами, получившим доступ к ПДн, называется конфиденциальностью ПДн.

25.1. Режим ограниченного доступа к персональным данным

С целью реализации требований действующего законодательства Российской Федерации в области ПДн по обеспечению конфиденциальности ПДн в Учреждении 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 сотрудников Учреждения, замещение которых предусматривает осуществление обработки ПДн либо осуществление доступа к ПДн;

разработку и корректировку Перечня должностей сотрудников Учреждения, 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, с составлением актов соответствия или проведением, при необходимости, доработок помещений по инженерно-технической укрёпленности по защите объектов от преступных посягательств;

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

получение расписок в ознакомлении сотрудников Учреждения, доступ которых к информации ограниченного доступа, обладателем которой является Учреждение, 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 Учреждения 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) сотрудников Учреждения, допущенных к обработке ПДн, по вопросам обработки и обеспечения безопасности ПДн;

разработку и ведение Журнала учета машинных носителей информации;

разработку и ведение Журнала учета сейфов, металлических шкафов, спецхранилищ и ключей от них;

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 Учреждения;

разработку инструкций о действиях сотрудников Учреждения в отношении носителей

ПДн при возникновении чрезвычайных ситуаций (стихийных бедствий, техногенных катастроф, наводнений, пожаров, нарушениях правопорядка и др.);

разработку инструкций для сотрудников Учреждения по вопросам обеспечения безопасности ПДн.

25.2. 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».

Учет (регистрация) носителей осуществляются структурным подразделением Учреждения, которому поручен учет несекретной документации.

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

Носители передаются в структурные подразделения Учреждения (исполнителям) под расписку, пересылаются сторонним организациям фельдъегерской связью, заказными или ценными почтовыми отправлениями.

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

Носители хранятся в надежно запираемых и опечатываемых шкафах (ящиках, хранилищах). Места хранения носителей и лица, ответственные за хранение, определяются и назначаются приказом руководителя Учреждения.

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

Передача носителей от одного служащего другому осуществляется с разрешения соответствующего руководителя.

При смене служащего, ответственного за учет, составляется акт приема-сдачи, который утверждается руководителем Учреждения (заместителем руководителя Учреждения).

Проверка наличия носителей проводится не реже одного раза в год комиссией, назначаемой приказом руководителя Учреждения. В состав такой комиссии обязательно включаются лица, ответственные за учет и хранение этих носителей. Результаты проверки оформляются актом.

По фактам утраты носителей назначается комиссия для расследования обстоятельств утраты. Результаты расследования докладываются руководителю, назначившему комиссию.

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

26. Обеспечение безопасности персональных данных при их обработке

В соответствии с требованиями действующего законодательства в области ПДн при обработке ПДн Учреждение 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 осуществляется 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.

Работы по обеспечению безопасности ПДн при их обработке в информационных системах в Учрежденииявляются неотъемлемой частью работ по созданию информационных систем.

26.1. Принципы обеспечения безопасности персональных данных при их обработке

Обеспечение безопасности ПДн в Учреждении 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 локальными нормативными актами Учреждения;

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 защищенности ПДн;

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

Категорически запрещается нарушать указанные принципы по обеспечению безопасности ПДн.

26.2. Требования по уровню обеспечения безопасности

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

Определение уровня защищенности ПДн включает в себя следующие этапы:

сбор и анализ исходных данных по ИСПДн;

присвоение ИСПДн соответствующего уровня защищенности ПДн и его документальное оформление.

При определении уровня защищенности ПДн учитываются следующие исходные данные:

категория обрабатываемых в ИСПДн ПДн;

объем 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 защищенности ПДн, соответствующий наиболее высокому уровню защищенности ПДн входящих в нее подсистем.

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

Результаты определения уровня защищенности ПДн оформляются соответствующим актом установки уровня защищенности ПДн.

26.3. Состав мероприятий по обеспечению безопасности персональных данных

Мероприятия по обеспечению безопасности ПДн должны носить комплексный характер и включать в себя правовые, организационные и технические меры, описанные в настоящих Правилах.

Порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются настоящими Правилами.

26.4. 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.

Ответственным за организацию и контроль за обеспечением безопасности ПДн в Учреждении при обработке ПДн, осуществляемой без использования средств автоматизации, является структурное подразделение Учреждения, ответственное за организацию обработки ПДн.

26.5. 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 Учреждении 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;

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

учет 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 защищенности 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 (обслуживающего персонала) к информационным ресурсам, информационной системе и связанным с ее использованием работам, документам;

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

разграничение доступа пользователей и обслуживающего персонала 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;

учет и хранение съемных носителей информации и их использование, исключающее хищение, подмену и уничтожение;

резервирование технических средств, дублирование массивов и носителей информации;

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

использование защищенных 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 съемных 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 скрытия структуры информационной системы;

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

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

защита информации при ее передаче по каналам связи;

использование смарт-карт, электронных замков и других носителей информации для надежной 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 счет побочных электромагнитных излучений и наводок в ИСПДн с установленным первым уровнем защищенности ПДн могут применяться следующие методы и способы защиты информации:

использование технических средств в защищенном 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.

В ИСПДн с установленным вторым уровнем защищенности ПДн для обработки информации используются средства вычислительной техники, удовлетворяющие требованиям национальных стандартов по электромагнитной совместимости, по безопасности и эргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видеодисплейным терминалам средств вычислительной техники.

При применении в информационных системах функции голосового ввода ПДн в

информационную систему или функции воспроизведения информации акустическими средствами информационных систем для ИСПДн с установленным первым уровнем защищенности ПДн реализуются 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 информационной системе 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.

27. 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.

Определение уровня специального оборудования помещения осуществляется специально создаваемой комиссией. По результатам определения класса и обследования помещения на предмет его соответствия такому классу составляются акты.

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.

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

В случае появления обстоятельств непреодолимой силы, возникших в результате событий чрезвычайного характера, которые Учреждение не может предвидеть, за возникновение которых оно не несет ответственности и не может предотвратить разумными мерами, должностные лица Учреждения 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,

решения органов государственной власти, препятствующие исполнению требований законодательства в области ПДн.

Надлежащим доказательством наличия указанных выше обстоятельств будут служить официальные документы Учреждения и органов государственной власти Российской Федерации.

Учреждение в случае возникновения указанных выше обстоятельств и нарушения прав субъектов персональных данных, связанных с такими обстоятельствами, извещает субъекта персональных данных всеми доступными способами.