УТВЕРЖДЕНО
распоряжением председателя
Избирательной комиссии Пермского края

от 07.03.2013 № 20-р

ПОЛОЖЕНИЕ
о порядке обработки и обеспечении безопасности персональных данных в информационных системах персональных данных Избирательной комиссии Пермского края, а также персональных данных, обрабатываемых без использования средств автоматизации

г. Пермь, 2013

Содержание

1. Общие положения

Настоящее положение принято в целях сохранения личной тайны и защиты персональных данных Избирательной комиссии Пермского края (далее - Комиссия).

Положение определяет права и обязанности руководителей и работников, порядок использования указанных данных в служебных целях, а также порядок взаимодействия по поводу сбора, документирования, хранения и уничтожения персональных данных работников.

Настоящее Положение разработано на основе и во исполнение части 1 статьи 23 и статьи 24 Конституции Российской Федерации; Гражданского кодекса Российской Федерации, Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»; Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»; главы 7 Федерального закона от 27.07.2004 № 79-ФЗ «О государственной гражданской службе Российской Федерации», положений главы 14 Трудового кодекса Российской Федерации «Защита персональных данных работника» Закон Пермского края от 07.12.2006 № 34-КЗ «О государственной гражданской службе Пермского края».

Председатель Комиссии определяет лиц из числа работников Комиссии, уполномоченных на обработку персональных данных, обеспечивающих обработку персональных данных в соответствии с требованиями Федерального закона от 27.06.2006 № 152-ФЗ «О персональных данных», других нормативных правовых актов Российской Федерации и несущих ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты этих персональных данных.

1.1. Основные термины и определения

Автоматизированная обработка персональных данных – обработка персональных данных с использованием средств автоматизации.

Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Информационная система персональных данных (ИСПДн) - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Неавтоматизированная обработка персональных данных – обработка персональных данных без использования средств автоматизации.

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Персональные данные работника – информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника.

Работник - физическое лицо, вступившее в трудовые отношения с работодателем.

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

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

1.2. Правовой статус обработки персональных данных

1.2.1. Правовое основание обработки персональных данных

Основанием обработки персональных данных является Постановление Госстандарта России № 454-ст «О принятии и введении в действие ОКВЭД». Приложение А к ОКВЭД описывает виды экономической деятельности, которые соответствуют характеру действий при обработке персональных данных:

«72.30. Обработка данных

– все стадии обработки данных, включая подготовку и ввод данных, с применением технического и программного обеспечения потребителя или собственного.

72.40. Деятельность по созданию и использованию баз данных и информационных ресурсов:

– проектирование баз данных (разработка концепций, структуры, состава баз данных);

– формирование и ведение баз данных, в том числе сбор данных из одного или более источников, а также ввод, верификация и актуализация данных;

– *администрирование баз данных, в том числе обеспечение возможности доступа к базе данных в режиме непосредственного или телекоммуникационного доступа;*

– *поиск данных, их отбор и сортировка по запросам, предоставление отобранных данных пользователям, в том числе в режиме непосредственного доступа;*

– *создание информационных ресурсов различных уровней (федеральных, ведомственных, корпоративных, ресурсов предприятий).*

1.2.2. Правовое основание обработки персональных данных средствами автоматизации

Основанием автоматизированной обработки персональных данных является нахождение Комиссии в Реестре операторов персональных данных.

1.3. Документы, которыми руководствуется Комиссия при работе с персональными данными:

– Конституция Российской Федерации от 12.12.1993;

– Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

– Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

– Трудовой кодекс Российской Федерации;

– Гражданский кодекс Российской Федерации;

– Уголовный кодекс Российской Федерации;

– Кодекс Российской Федерации об административных правонарушениях;

– Федеральный закон от 27.07.2004 № 79-ФЗ «О государственной гражданской службе Российской Федерации»;

–

– Указ Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера»;

– Указ Президента Российской Федерации от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;

– Постановление Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Постановление Правительства Российской Федерации от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

– Совместный Приказ ФСТЭК России № 55, ФСБ России № 86 и Мининформсвязи России от 13.02.2008 № 20 «Об утверждении Порядка проведения классификации информационных систем персональных данных»;

– «Положение о методах и способах защиты информации в информационных системах персональных данных». Утверждено Приказом ФСТЭК России от 05.02. 2010 № 58;

– «Административный регламент исполнения Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций государственной функции по осуществлению государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных». Утвержден приказом Министерства связи и массовых коммуникаций Российской Федерации от 14.11.2011 № 312;

– «Типовой регламент проведения в пределах полномочий мероприятий по контролю (надзору) за выполнением требований, установленных Правительством Российской Федерации, к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». Утвержден Руководством 8 Центра ФСБ России от 08.08.2009 № 149/7/2/6-1173;

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

– «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных». Утверждена заместителем директора ФСТЭК России от 15.02.2008;

– «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных». Утверждена заместителем директора ФСТЭК России от 14.02.2008;

– Инструкция об организации и обеспечении безопасности, хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденная Приказом ФАПСИ при Президенте Российской Федерации от 13.06.2001 №152;

– Постановление Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

2. Персональные данные

2.1. Принципы обработки персональных данных:

– обработка персональных данных должна осуществляться на законной и справедливой основе;

– обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

– не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

– обработке подлежат только персональные данные, которые отвечают целям их обработки;

– содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки;

– при обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных;

– хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению или обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

2.2. Круг субъектов, персональные данные которых подлежат обработке

Субъектами персональных данных являются бывшие и работающие на данный момент сотрудники Комиссии, лица, желающие устроиться на работу в Комиссию, председатели, секретари, члены территориальных и участковых избирательных комиссий Пермского края, сотрудники аппаратов территориальных избирательных комиссий, лица, получающие вознаграждения по договорам гражданско-правового характера, лица, участвующие в конкурсах и мероприятиях, проводимых Комиссией, а также лица, участвующие в избирательном процессе на территории Пермского края.

2.3. Состав персональных данных, необходимый для обработки

Состав персональных данных определяется нормативно-правовыми актами в сфере служебных, трудовых правоотношений и финансовыми документами Комиссии. Запрещено обрабатывать дополнительные персональные данные.

2.4. Источники получения персональных данных

Источниками персональных данных являются субъекты персональных данных.

2.5. Сроки хранения и период обработки персональных данных

Сроки обработки персональных данных для сотрудников Комиссии определены Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» в соответствии с целями обработки.

Период временного хранения документов, содержащих персональные данные, определен Федеральным законом от 22.10.2004 № 125-ФЗ «Об архивном деле в Российской Федерации» и составляет 75 лет после увольнения соответствующего работника.

2.6. Способы обработки персональных данных

Обработка персональных данных осуществляется с применением информационных технологий и технических средств в информационных системах персональных данных (ИСПДн). Под техническими средствами, позволяющими осуществлять обработку персональных данных, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и прочее), средства защиты информации, применяемые в информационных системах.

3. Учет персональных данных

3.1. Носители персональных данных

Носителями персональных данных являются:

– электронные носители – магнитные и оптические (CD и DVD) накопители, съемные жесткие диски и флэш-накопители, применяемые для создания резервных копий информации или переноса информации;

– бумажные носители информации о персональных данных.

3.2. Порядок организации делопроизводства содержащих персональные данные документов и информации

Документы, содержащие персональные данные, относятся к категории конфиденциальных и требуют организации отдельного делопроизводства и хранения.

Распоряжением председателя Комиссии назначаются ответственные за организацию делопроизводства и хранения государственные гражданские служащие аппарата Комиссии, определяются места и условия хранения документов, перечень лиц, имеющих право изготовления и ознакомления с документами, места изготовления и размножения документов, порядка маркировки, учета и рассылки документов, порядок и очередность эвакуации документов при возникновении чрезвычайных ситуаций, подготовки документов к сдаче на архивное хранение или уничтожение по мере надобности.

Ведется обязательная фиксация событий, касающихся движения документов (как электронных, так и бумажных), содержащих персональные данные.

Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее - материальные носители).

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

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

При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

а) при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

б) при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

Уточнение персональных данных 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.

3.3. Требования к типовым формам документов

При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

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

в) 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;

г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

4. Требования к работникам Оператора персональных данных

Ответственным за обеспечение безопасности персональных данных при их обработке в информационной системе распоряжением председателя Комиссии назначается должностное лицо из состава руководства (далее - уполномоченное лицо). Существенным условием является обязанность уполномоченного лица обеспечить конфиденциальность персональных данных и их безопасность при их обработке в информационной системе.

Для осуществления мероприятий по обработке персональных данных в информационной системе распоряжением председателя Комиссии назначается администратор безопасности, ответственный за обеспечение безопасности персональных данных в процессе их обработки, передачи по каналам связи, созданию и хранению резервных копий баз этих данных.

Персонал, доступ которого к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, допускается к соответствующим персональным данным на основании списка, утверждаемого распоряжением председателя Комиссии.

При работе с персональными данными в информационной системе лица, допущенные к обработке этих данных в процессе выполнения служебных обязанностей, должны обеспечивать:

а) проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

б) своевременное обнаружение фактов несанкционированного доступа к персональным данным;

в) недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование и целостность данных;

г) возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

д) постоянный контроль за обеспечением уровня защищенности персональных данных.

Требования к должностным обязанностям лиц, осуществляющим обработку и хранение персональных данных в Комиссии, включаются в их должностные обязанности в соответствии с «Квалификационным справочником должностей руководителей, специалистов и других служащих», утвержденным Постановлением Минтруда Российской Федерации № 37 от 21.08.1998.

В Комиссии составляется план проведения и организуется обучение персонала по вопросам работы и обеспечения защиты персональных данных в информационных системах персональных данных, ответственности персонала за нарушения при работе с персональными данными, порядке их взаимодействия с субъектами персональных данных.

5. Порядок взаимодействия с субъектами персональных данных

Субъект персональных данных имеет право на получение сведений об операторе, о месте его нахождения, о наличии у оператора персональных данных, относящихся к соответствующему субъекту персональных данных, а также на ознакомление с такими персональными данными. Субъект персональных данных вправе требовать от оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также имеет право принимать предусмотренные законом меры по защите своих прав.

Сведения о наличии персональных данных должны предоставляться субъекту персональных данных оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

Доступ к своим персональным данным предоставляется субъекту персональных данных или его законному представителю оператором при обращении либо при получении запроса субъекта персональных данных или его законного представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных или его

законного представителя. Запрос может быть направлен в электронной форме и подписан электронной подписью в соответствии с законодательством Российской Федерации.

Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных оператором;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые оператором способы обработки персональных данных;

4) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;

5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

6) сроки обработки персональных данных, в том числе сроки их хранения;

7) порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

10) иные сведения, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если:

1) обработка персональных данных, включая персональные данные, полученные в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

2) обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

3) обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

4) доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;

5) обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

Решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных данных или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.

Оператор обязан разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных 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.

Оператор обязан рассмотреть возражение против автоматизированной обработки в течение тридцати дней со дня его получения и уведомить субъекта персональных данных о результатах рассмотрения такого возражения.

Если субъект персональных данных считает, что оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

6. Обязанности Оператора при обработке персональных данных в информационных системах

При обработке персональных данных в информационных системах должно быть обеспечено:

а) назначение ответственного за организацию обработки персональных данных;

б) издание документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

в) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

г) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;

д) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

е) ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

7. Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах

Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:

а) определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

б) применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

в) применение процедуры оценки соответствия средств защиты информации;

г) оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

д) учет машинных носителей персональных данных;

е) обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;

ж) восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

з) установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечение регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

и) контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

8. Меры по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации

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

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

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

9. Правила допуска, хранения и пересылки персональных данных

Допуск лиц к обработке персональных данных в информационной системе осуществляется на основании соответствующих разрешительных документов и ключей (паролей) доступа.

Пересылка персональных данных без использования специальных средств защиты по общедоступным сетям связи, в том числе сети Интернет, запрещается.

10. Ответственность за нарушение норм, регулирующих обработку персональных данных

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работников, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством.