Приложение

к Постановлению администрации

Сандовского муниципального округа от 12.02.2021г № 60

### **ПОЛОЖЕНИЕ**

### **О РАБОТЕ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ В**

**АДМИНИСТРАЦИИ САНДОВСКОГО МУНИЦИПАЛЬНОГО ОКРУГА И В САМОСТОЯТЕЛЬНЫХ СТРУКТУРНЫХ ПОДРАЗДЕЛЕНИЯХ**

**1. ОБЩИЕ ПОЛОЖЕНИЯ**

1.1. Положение о работе с персональными данными в Администрации Сандовского муниципального округа и в самостоятельных структурных подразделениях (далее – Положение) устанавливает порядок получения, обработки, использования, хранения и гарантии конфиденциальности персональных данных физических лиц, необходимых для осуществления деятельности администрации Сандовского района и самостоятельных структурных подразделений в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – Федеральный закон), нормативными правовыми актами Российской Федерации в области муниципальной службы, защиты информации, трудовых отношений.

1.2. Задачей Администрации Сандовского муниципального округа и самостоятельных структурных подразделений (далее – администрации) в области защиты персональных данных является обеспечение в соответствии с законодательством Российской Федерации обработки, хранения и защиты персональных данных субъекта **персональных данных**, персональные данные которых подлежат обработке, на основании полномочий администрации, а также персональных данных, содержащихся в документах, полученных из других организаций, от иных субъектов персональных данных, обращениях граждан.

1.3. Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, определяемая нормативными правовыми актами Российской Федерации.

1.4. Иные понятия, используемые в Положении, применяются в значениях, определенных Федеральным законом.

1.5. Состав персональных данных, обрабатываемых в администрации, определяется согласно приложению 1 к Положению.

### **2. ПРИНЦИПЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

2.1. Обработка персональных данных должна осуществляться на основе принципов:

а) законности целей и способов обработки персональных данных и добросовестности;

б) соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям оператора;

в) соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;

г) достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;

д) недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

2.2. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки; персональные данные подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

2.3. Субъект персональных данных является собственником своих персональных данных и самостоятельно решает вопрос передачи оператору своих персональных данных.

2.4. Держателем персональных данных является оператор, которому субъект персональных данных добровольно передает во владение свои персональные данные. Оператор выполняет функцию владения этими данными и обладает полномочиями распоряжения ими в пределах, установленных законодательством.

2.5. Право доступа к персональным данным субъекта персональных данных имеют лица, уполномоченные оператором.

2.6. Потребителями (пользователями) персональных данных являются юридические и физические лица, обращающиеся к собственнику или оператору за получением необходимых сведений и пользующиеся ими без права передачи, разглашения.

**3. СОЗДАНИЕ, ОБРАБОТКА И ХРАНЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ**

3.1. Создание персональных данных.

Документы, содержащие персональные данные, создаются путём:

а) копирования оригиналов (документ об образовании, свидетельство ИНН, пенсионное свидетельство, паспорт, военный билет и другие документы личного характера);

б) внесения сведений в учётные формы (на бумажных и электронных носителях);

в) получения оригиналов необходимых документов (трудовая книжка, личный листок по учёту кадров, автобиография, медицинское заключение).

3.2. 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.

3.2.1. При обработке персональных данных в целях их защиты и обеспечения прав и свобод человека и гражданина, а также при определении объема и содержания обрабатываемых персональных данных должны строго учитываться положения Конституции Российской Федерации, Трудового Кодекса Российской Федерации и иных федеральных законов.

3.2.2. Обработка персональных данных осуществляется исключительно в целях:

а) обеспечения соблюдения законов и иных нормативных правовых актов;

б) содействия в трудоустройстве;

в) обеспечения личной безопасности;

г) контроля количества и качества выполняемой работы;

д) обеспечения сохранности имущества.

3.2.3. Все персональные данные субъекта **персональных данных** следует получать у него самого, за исключением случаев, если их получение возможно только у третьей стороны.

3.2.4. Получение персональных данных субъекта **персональных данных** у третьих лиц, возможно только при уведомлении об этом заранее и с его письменного согласия.

В уведомлении о получении его персональных данных у третьих лиц должна содержаться следующая информация:

а) о целях получения персональных данных;

б) о предполагаемых источниках и способах получения персональных данных;

в) о характере подлежащих получению персональных данных;

г) о последствиях отказа дать письменное согласие на их получение.

3.2.5. Администрация не имеет права получать и обрабатывать персональные данные субъекта **персональных данных** о его политических, религиозных и иных убеждениях и частной жизни, а равно как персональные данные субъекта **персональных данных** о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации администрация вправе получать и обрабатывать данные о частной жизни субъекта **персональных данных** только с его письменного согласия.

3.2.6. При принятии решений, затрагивающих интересы субъекта **персональных данных**, администрация не имеет права основываться на персональных данных субъекта **персональных данных**, полученных исключительно в результате их автоматизированной обработки или электронного получения.

3.2.7. Субъекты **персональных данных** и их представители должны быть ознакомлены под расписку с документами администрации, устанавливающими порядок обработки персональных данных, а также об их правах и обязанностях в этой области.

3.3. Сведения, содержащие персональные данные работника, иного субъекта персональных данных, включаются в его личное дело, карточку формы Т-2, другие формы разрабатываемых документов, а также содержатся на электронных носителях информации, доступ к которым разрешён лицам, непосредственно использующих персональные данные работника в служебных целях. Перечень должностных лиц определён в пункте 4.1 настоящего положения.

3.4. Создание, обработка и хранение персональных данных в отделе бухгалтерского учета и отчетности администрации (далее - бухгалтерии), финансового управления, централизованной бухгалтерии отдела образования (далее - подразделений):

а) персональные данные, содержащиеся на бумажных носителях, хранятся в запираемом шкафу, установленном на рабочем месте главного бухгалтера.

б) персональные данные, содержащиеся на электронных носителях информации, хранятся в ПК специалистов бухгалтерии и отделов; передаются в ИФНС, ФСС, Пенсионный фонд, в кредитные учреждения, по запросам надзорных и контрольных органов на бумажных носителях, электронных носителей и по защищенным каналам связи.

3.4.1. Персональные данные администрации и отделов, включённые в состав личных дел, хранятся в запираемых шкафах, установленных на рабочих местах; в администрации – заведующего юридическим отделом; в подразделениях – специалистов, ответственных за ведение личных дел. Персональные данные, содержащиеся на электронных носителях информации, хранятся в ПК; в администрации – заведующего юридическим отделом; в подразделениях – специалистов, ответственных за ведение личных дел.

3.4.2. Трудовые книжки, документы воинского учёта, карточки формы Т-2 хранятся в запираемом металлическом сейфе.

3.4.3. Записи актов гражданского состояния хранятся в запираемом металлическом сейфе, установленном на рабочем месте заведующего отделом ЗАГС. Персональные данные, содержащиеся на электронных носителях информации, хранятся в ПК заведующего отделом ЗАГС, передаются в Пенсионный фонд, ИФНС, отдел ЗАГС Тверской области в электронном виде, по защищенному каналу связи, по запросам надзорных и контрольных органов на бумажных носителях.

3.4.4. Договора аренды земельных участков, помещений, зданий, приватизации, купли-продажи, хранятся в запираемом шкафу, установленном на рабочем месте заведующего отделом земельных и имущественных отношений. Персональные данные, содержащиеся на электронных носителях информации, хранятся в ПК специалистов отдела земельных и имущественных отношений; передаются в управление Росреестра, налоговую инспекцию, Правительство Тверской области, ФАС, по запросам надзорных и контрольных органов на бумажных носителях; в министерство имущественных и земельных отношений в электронном виде, по защищенному каналу связи.

3.4.5. Обращения граждан подшиваются в дело и хранятся в запираемом сейфе, установленном на рабочем месте заведующего организационным отделом.

3.4.6. Реестр субъектов малого и среднего предпринимательства подшивается в дело и хранится в запираемом шкафу, установленном в отделе экономики. Персональные данные, содержащиеся на электронных носителях информации, хранятся в ПК специалистов отдела экономики; передаются в министерство экономического развития, министерство имущественных и земельных отношений, по запросам надзорных и контрольных органов, на бумажных носителях и по защищенным каналам связи.

3.4.7. Документы о постановке граждан на учет в качестве нуждающихся в улучшении жилищных условий, вторые экземпляры разрешений на строительство, ввод в эксплуатацию объектов капитального строительства, актов обследования подшиваются в дела и хранятся в запираемом шкафу, установленном в отделе земельных и имущественных отношений (сектор строительства и архитектуры). Персональные данные, содержащиеся на электронных носителях информации, хранятся в ПК специалистов отдела; могут передаваться в государственные и муниципальные органы власти, по запросам надзорных и контрольных органов на бумажных носителях и по защищенным каналам связи.

3.4.8. Документы комиссии по делам несовершеннолетних и защите их прав подшиваются в дела и хранятся в запираемом шкафу, установленном в кабинете ответственного секретаря КДН и ЗП. Персональные данные, содержащиеся на электронных носителях информации, хранятся в ПК ответственного секретаря КДН и ЗП; передаются участникам производства, субъектам профилактики безнадзорности и правонарушений на бумажных и электронных носителях.

3.4.9. Документы отдела культуры, молодежи и спорта подшиваются в дела и хранятся в запираемом шкафу, установленном на рабочем месте заведующего отдела культуры, молодежи и спорта. Персональные данные, содержащиеся на электронных носителях информации, хранятся в ПК главных специалистов отдела культуры, молодежи и спорта; передаются в комитет по делам молодежи на бумажных и электронных носителях.

3.4.10. Доступ к ПК строго ограничен кругом лиц, определённых в пункте 4.1 настоящего Положения. Персональные данные, содержащиеся на бумажных носителях, сдаются в архив после истечения установленного срока хранения.

**4. ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ**

4.1. Внутренний доступ (работники администрации Сандовского муниципального округа), в т.ч. помещения, предназначенные для обработки персональных данных. Доступ к персональным данным имеют следующие должностные лица, непосредственно использующие их в служебных целях:

- Глава муниципального округа;

- заместители Главы муниципального округа;

- управляющий делами администрации муниципального округа;

- заведующий и специалисты организационного отдела;

- заведующий юридическим отделом;

- заведующие и специалисты финансового управления, отдела бухгалтерского учета и отчетности, централизованной бухгалтерии отдела образования;

- специалист (по обеспечению безопасности);

- заведующий и специалисты отдела земельных и имущественных отношений, сектора строительства и архитектуры;

- заведующий и специалист отдела экономики;

- ответственный секретарь КДН и ЗП;

- заведующий и специалисты отдела образования;

- заведующий отделом ЗАГС;

- заведующий архивным отделом;

- заведующий и специалисты отдела жизнеобеспечения;

- заведующий отделом ЗАГС;

- заведующий архивным отделом;

- начальник и специалист отдела благоустройства и поселкового хозяйства;

- заведующие и специалисты территориальных отделов;

- заведующий и специалисты отдела культуры, молодежи и спорта.

4.1.1. Уполномоченные лица имеют право получать только те персональные данные субъекта **персональных данных**, которые необходимы для выполнения конкретных функций в соответствии с должностной инструкцией указанных лиц. Все остальные работники имеют право на полную информацию только об их персональных данных и обработке этих данных.

4.1.2. Получение сведений о персональных данных третьей стороной разрешается только при наличии заявления с указанием конкретных персональных данных и целей, для которых они будут использованы, а также письменного согласия субъекта **персональных данных**, персональные данные которого затребованы.

4.1.3. Получение персональных данных третьей стороной без его письменного согласия возможно в случаях, когда это необходимо в целях предупреждения угрозы жизни и здоровья, а также в случаях, установленных законом.

4.2. Внешний доступ (другие организации и граждане).

Сообщение сведений о персональных данных другим организациям и гражданам разрешается при наличии письменного согласия и заявления, подписанного руководителем организации либо гражданином, запросившим такие сведения.

4.2.1. Предоставление сведений о персональных данных без соответствующего их согласия возможно в следующих случаях:

а) в целях предупреждения угрозы жизни и здоровья;

б) при поступлении официальных запросов в соответствии с положениями Федерального закона «Об оперативно-розыскных мероприятиях»;

в) при поступлении официальных запросов из налоговых органов, органов Пенсионного Фонда России, органов Федерального социального страхования, судебных органов.

4.2.2. Субъект, о котором запрашиваются сведения, должен быть уведомлён о передаче его персональных данных третьим лицам, за исключением случаев, когда такое уведомление невозможно в силу форс-мажорных обстоятельств, а именно: стихийных бедствий природного и техногенного характера.

4.2.3. Запрещается передача персональных данных в коммерческих целях без его согласия.

4.2.4. Должностные лица, имеющие доступ к персональным данным, отвечают за проведение мероприятий по обезличиванию персональных данных, в соответствии с правилами, определенными приказом Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных».

**5. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ**

5.1. При передаче персональных данных субъекта **персональных данных** с соблюдением условий, предусмотренных разделом 3 настоящего Положения, должностные лица администрации, обязаны предупредить лиц об ответственности в соответствии с законодательством Российской Федерации.

5.2. В целях обеспечения защиты персональных данных, хранящихся в личных делах, работники имеют право:

а) получать полную информацию о своих персональных данных и обработке этих данных (в том числе автоматизированной);

б) осуществлять свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральным законом;

в) требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением федерального закона. Работник при отказе работодателя исключить или исправить персональные данные работника имеет право заявлять в письменной форме работодателю о своём несогласии, обосновав соответствующим образом такое несогласие. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения;

г) требовать от работодателя уведомления всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведённых в них изменениях или исключениях из них;

д) обжаловать в суд любые неправомерные действия или бездействие работодателя при обработке и защите персональных данных гражданского служащего.

5.3. Запрещается передавать информацию о состоянии здоровья субъекта персональных данных, за исключением сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции.

5.4. При передаче персональных данных работников или иного субъекта персональных данных третьим лицам, в том числе представителям работников, руководствоваться порядком, установленным Трудовым кодексом Российской Федерации и настоящим Положением, и ограничивать эту информацию только теми персональными данными, которые необходимы для выполнения третьими лицами их функций.

5.5. Защита персональных данных субъекта **персональных данных** от неправомерного их использования или утраты обеспечивается за счёт средств администрации в порядке, установленном федеральным законом.

5.6. В случае отказа субъекта персональных данных предоставить оператору свои персональные данные, ему должны быть разъяснены юридические последствия такого отказа в соответствии с типовой формой разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные (приложение 2).

5.7. Запрещается нахождение в помещениях, предназначенных для обработки ПДн, посторонних лиц без сопровождения лиц, имеющих право самостоятельного доступа.

5.8. Установку и замену оборудования в помещениях, предназначенных для обработки ПДн, а также ремонт помещений проводить по согласованию с ответственным за обработку персональных данных.

### **6. КОНФИДЕНЦИАЛЬНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ**

6.1. Администрацией и третьими лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных, за исключением случаев, предусмотренных пунктом 6.2. настоящего Положения.

6.2. Обеспечение конфиденциальности персональных данных не требуется:

а) в случае обезличивания персональных данных;

б) в отношении общедоступных персональных данных.

### **7. ОБЩЕДОСТУПНЫЕ ИСТОЧНИКИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

7.1. С целью информационного обеспечения деятельности могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги и др.). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные субъектом персональных данных.

7.2. Сведения о субъекте персональных данных исключаются в любое время из общедоступных источников персональных данных по его требованию, либо по решению администрации, либо суда или иных уполномоченных государственных органов.

### **8. ПРАВА И ОБЯЗАННОСТИ СТОРОН В ОБЛАСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

8.1. Субъект персональных данных:

а) передает администрации или ее представителю комплекс достоверных, документированных персональных данных, состав которых установлен трудовым законодательством, включая сведения об образовании, специальных знаниях, стаже работы, отношении к воинской обязанности, гражданстве, месте жительства и иные сведения;

б) своевременно сообщает администрации об изменении своих персональных данных;

в) получает полную информацию о своих персональных данных;

г) имеет свободный без взимания платы доступ к своим персональным данным, включая право на получение копий любой записи, содержащей его персональные данные, за исключением случаев, предусмотренных законодательством;

д) получает сведения об администрации, о месте ее нахождения, о наличии у администрации персональных данных, относящихся к соответствующему субъекту персональных данных;

е) требует от администрации 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 принимать предусмотренные законом меры по защите своих прав;

ж) получает информацию, касающуюся обработки его персональных данных, в том числе содержащую подтверждение факта обработки персональных данных администрацией, а также цель такой обработки; способы обработки персональных данных, применяемые администрацией; сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ; перечень обрабатываемых персональных данных и источник их получения; сроки обработки персональных данных, в том числе сроки их хранения; сведения о том, какие юридические последствия для него может повлечь за собой обработка его персональных данных;

з) при отказе администрации исключить или исправить персональные данные субъекта персональных данных он имеет право заявить в письменной форме оператору о своем несогласии с соответствующим обоснованием такого несогласия. Сведения о наличии персональных данных предоставляются субъекту персональных данных в доступной форме, не содержащей персональные данные, относящиеся к другим субъектам персональных данных.

Доступ к своим персональным данным предоставляется субъекту персональных данных или его представителю администрацией при личном обращении либо при получении запроса.

Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных или его представителя. Запрос может быть направлен в электронной форме и подписан электронной цифровой подписью в соответствии с законодательством Российской Федерации.

8.2. Право субъекта персональных данных на доступ к своим персональным данным ограничивается, в случае если:

а) обработка персональных данных осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

б) предоставление персональных данных нарушает конституционные права и свободы других лиц;

в) в иных случаях, предусмотренных законодательством Российской Федерации.

8.3. Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных пунктом 8.4. настоящего Положения.

8.4. Решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, принимается на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия субъекта персональных данных в письменной форме или в случаях, предусмотренных федеральными законами.

8.5. Администрация разъясняет субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставляет возможность заявить возражение против такого решения, а также разъяснить порядок защиты своих прав и законных интересов. Администрация рассматривает возражение субъекта персональных данных в течение 7 рабочих дней со дня его получения и уведомляет его о результатах рассмотрения такого возражения.

8.6. Если обязанность предоставления персональных данных субъектом персональных данных установлена федеральным законом, администрация разъясняет субъекту персональных данных юридические последствия отказа предоставить свои персональные данные.

8.7. Если персональные данные были получены не от субъекта персональных данных, за исключением случаев, если персональные данные были предоставлены оператору на основании федерального закона или если персональные данные являются общедоступными, администрация до начала обработки таких персональных данных предоставляет субъекту персональных данных следующую информацию:

а) наименование и адрес администрации или ее представителя;

б) цель обработки персональных данных и ее правовое основание;

в) предполагаемые пользователи персональных данных;

г) права субъекта персональных данных в области защиты персональных данных.

8.8. Администрация безвозмездно предоставляет субъекту персональных данных возможность ознакомления с персональными данными, относящимися к соответствующему субъекту персональных данных, а также вносит в них необходимые изменения, уничтожает или блокирует соответствующие персональные данные по предоставлении субъектом персональных данных сведений, подтверждающих, что персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и предпринятых мерах администрация обязана уведомить субъекта персональных данных и третьих лиц, которым персональные данные этого субъекта персональных данных были переданы.

8.9. В случае выявления недостоверных персональных данных или неправомерных действий с ними администрация осуществляет блокирование персональных данных, относящихся к соответствующему субъекту персональных данных, с момента получения такой информации на период проверки. В случае подтверждения факта недостоверности персональных данных администрация на основании соответствующих документов уточняет персональные данные и снимает их блокирование.

В случае выявления неправомерных действий с персональными данными администрация в срок, не превышающий трех рабочих дней с даты такого выявления, устраняет допущенные нарушения.

В случае невозможности устранения допущенных нарушений администрация в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, уничтожает персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных оператор уведомляет субъекта персональных данных.

8.10. В случае достижения цели обработки персональных данных администрация незамедлительно прекращает обработку персональных данных и уничтожает соответствующие персональные данные в срок, не превышающий трех рабочих дней с даты достижения цели обработки персональных данных, если иное не предусмотрено федеральными законами, и уведомляет об этом субъекта персональных данных.

8.11. В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных администрация прекращает обработку персональных данных и уничтожает персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением сторон. Об уничтожении персональных данных администрация уведомляет субъекта персональных данных.

## **9. БЕЗОПАСНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ**

9.1. Администрация при обработке персональных данных обязана принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

9.2. Использование и хранение биометрических персональных данных вне ИСПДн осуществляются 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, уничтожения, изменения, блокирования, копирования, распространения.

**10. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, СВЯЗАННОЙ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ**

10.1. Лица, виновные в нарушении требований Федерального закона, несут предусмотренную законодательством Российской Федерации ответственность.

Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных настоящим Федеральным законом, а также требований к защите персональных данных, установленных в соответствии с настоящим Федеральным законом, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

10.2. За каждый дисциплинарный проступок может быть применено только одно дисциплинарное взыскание.

10.3. Копия распоряжения о применении к работнику дисциплинарного взыскания с указанием оснований его применения вручается работнику под расписку в течение пяти дней со дня издания приказа.

10.4. Если в течение года со дня применения дисциплинарного взыскания работник не будет подвергнут новому дисциплинарному взысканию, то он считается не имеющим дисциплинарного взыскания. Работодатель до истечения года со дня издания распоряжения о применении дисциплинарного взыскания, имеет право снять его с работника по собственной инициативе, по письменному заявлению работника или по ходатайству его непосредственного руководителя.

## **11. ПОРЯДОК КЛАССИФИКАЦИИ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ**

11.1. При обработке персональных данных в информационных системах устанавливаются 4 уровня защищенности персональных данных.

11.2. Необходимость обеспечения 1-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает либо специальные категории персональных данных, либо биометрические персональные данные, либо иные категории персональных данных;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

11.3. Необходимость обеспечения 2-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

в) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает биометрические персональные данные;

г) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

д) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

е) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

11. 4. Необходимость обеспечения 3-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные сотрудников оператора или общедоступные персональные данные менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

в) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

г) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает биометрические персональные данные;

д) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

11.5. Необходимость обеспечения 4-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

### **12. ПОРЯДОК РАЗРАБОТКИ, ВВОДА В ДЕЙСТВИЕ И ЭКСПЛУАТАЦИЮ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ**

12.1. Порядок предпроектного обследования ИСПДн включает:

а) определение перечня персональных данных, обрабатываемых в ИСПДн;

б) определение перечня персональных данных, подлежащих защите от несанкционированного доступа (далее — НсД);

в) определение условий расположения ИСПДн относительно границ контролируемой зоны;

г) определение конфигурации и топологии ИСПДн в целом и ее отдельных компонентов; физические, функциональные и технологические связи как внутри этих систем, так и с другими системами различного уровня и назначения;

д) определение технических средств и систем, предполагаемых к использованию в разрабатываемой ИСПДн, условия их расположения; общесистемные и прикладные программные средства, имеющиеся и предлагаемые к разработке;

е) определение режимов обработки персональных данных в ИСПДн в целом и в отдельных компонентах;

ж) определение класса ИСПДн;

з) уточнение степени участия должностных лиц в обработке персональных данных, характер их взаимодействия между собой;

и) разработка модели угроз безопасности персональных данных применительно к конкретным условиям функционирования ИСПДн (Приложения № 3 – 4).

12.2. По результатам предпроектного обследования на основе документа с учетом установленного класса ИСПДн задаются конкретные требования по обеспечению безопасности персональных данных, включаемые в техническое задание на разработку СЗПДн. Разработка технического задания на создание СЗПДн включает:

а) обоснование разработки СЗПДн;

б) исходные данные создаваемой (модернизируемой) ИСПДн в техническом, программном, информационном и организационном аспектах;

в) класс ИСПДн;

г) требования федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, с учетом которых будет разрабатываться СЗПДн и приниматься в эксплуатацию ИСПДн;

д) перечень предполагаемых к использованию сертифицированных средств защиты информации;

е) обоснование проведения разработок собственных средств защиты информации при невозможности или нецелесообразности использования имеющихся на рынке сертифицированных средств защиты информации;

ж) состав, содержание и сроки проведения работ по этапам разработки и внедрения СЗПДн.

12.3. Проектирование и реализация СЗПДн включает:

а) разработку задания и проекта проведения работ (в том числе строительных и строительно-монтажных) по созданию (реконструкции) ИСПДн в соответствии с требованиями технического (частного технического) задания на разработку СЗПДн;

б) выполнение работ в соответствии с проектной документацией;

в) закупку обоснованной совокупности используемых в ИСПДн серийно выпускаемых технических средств обработки, передачи и хранения информации;

г) разработку мероприятий по защите информации в соответствии с предъявляемыми требованиями;

д) закупку обоснованной совокупности используемых в ИСПДн сертифицированных технических, программных и программно-технических средств защиты информации и их установка;

е) проведение сертификации по требованиям безопасности информации технических, программных и программно-технических средств защиты информации, в случае, когда на рынке отсутствуют требуемые сертифицированные средства защиты информации;

ж) разработку и реализацию разрешительной системы доступа пользователей к обрабатываемой на ИСПДн информации;

з) определение структурных подразделений и назначение лиц, ответственных за эксплуатацию средств защиты информации, с их обучением по направлению обеспечения безопасности персональных данных;

и) разработку эксплуатационной документации на ИСПДн и средства защиты информации, а также организационно-распорядительной документации по защите информации;

к) выполнение других мероприятий, характерных для конкретных ИСПДн и направлений обеспечения безопасности персональных данных.

12.4. Ввод в действие СЗПДн включает:

а) выполнение генерации пакета прикладных программ в комплексе с программными средствами защиты информации;

б) опытную эксплуатацию средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПДн;

в) приемо-сдаточные испытания средств защиты информации по результатам опытной эксплуатации;

г) организацию охраны и физической защиты помещений ИСПДн, исключающих несанкционированный доступ к техническим средствам ИСПДн, их хищение и нарушение работоспособности, хищение носителей информации;

д) оценку соответствия ИСПДн требованиям безопасности персональных данных.

### **13. ПОРЯДОК КОНТРОЛЯ ЗА ОБЕСПЕЧЕНИЕМ УРОВНЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ И ОЦЕНКИ СООТВЕТСТВИЯ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ**

13.1. Порядок обследования защищенности персональных данных включает:

а) выделение информационных ресурсов, содержащих в себе персональные данные, а также технические средства, позволяющие осуществлять обработку персональных данных, из всей совокупности обрабатываемой информации;

б) определение соответствия действующей системы обработки персональных данных требованиям, установленным федеральным законодательством;

в) классификацию информационных систем персональных данных.

13.2. По итогам обследования администрация получает:

а) аналитический отчет о предпроектном обследовании и текущей защищенности персональных данных;

б) акт классификации ИСПДн.

13.3. Подготовка ИСПДн к проведению оценки соответствия ИСПДн требованиям безопасности персональных данных и созданию СЗПДн осуществляется путем:

а) анализа информационных ресурсов (определения перечня всех существующих ИСПДн; определения состава и структуры каждой ИСПДн; определения перечня и местонахождения персональных данных, подлежащих защите; категорирования персональных данных; определения режима обработки персональных в целом и отдельных компонентах);

б) анализа уязвимых звеньев и возможных угроз безопасности персональных данных (оценки возможности физического доступа к ИСПДн; выявления возможных каналов утечки информации, в том числе технических; анализа возможностей программно-математического воздействия на ИСПДн; анализа возможностей электромагнитного воздействия на ИСПДн);

в) оценки ущерба от реализации угроз безопасности персональных данных (оценки непосредственного и опосредованного ущерба от реализации угроз безопасности персональных данных);

г) анализа имеющихся в распоряжении мер и средств защиты персональных данных (от физического доступа; от утечки по техническим каналам; от НсД; от программно-математического воздействия; от электромагнитных воздействий).

13.4. Обоснование требований по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн, включает:

а) разработку модели угроз безопасности персональных данных;

б) разработку модели нарушителя безопасности персональных данных;

в) составление перечня и проведение оценки актуальных угроз безопасности персональных данных;

г) определение класса ИСПДн.

13.5. Проведение работ по организации обеспечения безопасности персональных данных при их обработке в ИСПДн включает:

а) разработку и согласование с уполномоченными службами требований к СЗПДн и формулирование задач по защите персональных данных (разработка перечня мероприятий по защите персональных данных в соответствии с выбранным классом ИСПДн);

б) выбор способов, мер и средств защиты персональных данных в соответствии с мероприятиями по защите;

в) разработку технического задания на СЗПДн;

г) разработку документов, регламентирующих вопросы организации обеспечения безопасности персональных данных и эксплуатации СЗПДн в ИСПДн (Приложения № 5 – 16);

д) развертывание и ввод в опытную эксплуатацию СЗПДн в ИСПДн;

е) доработку СЗПДн по результатам опытной эксплуатации;

ж) проведение работ по аттестации ИСПДн по требованиям безопасности информации.