УТВЕРЖДЕНО
приказом директора бюджетного учреждения культуры Вологодской области «Вологодский областной театр юного зрителя» от «01» июня 2022 г. № 66 (приложение № 1 к приказу)

ПОЛОЖЕНИЕ
об обработке и защите персональных данных работников бюджетного учреждения культуры Вологодской области «Вологодский областной театр юного зрителя»

1. Общие положения

1.1. Настоящее Положение определяет порядок и условия обработки персональных данных с использованием средств автоматизации и без использования таких средств, а также мероприятия по защите персональных данных в бюджетном учреждении культуры Вологодской области «Вологодский областной театр юного зрителя» (далее – Учреждение).

1.2. Целью настоящего Положения является защита персональных данных работников Учреждения от несанкционированного доступа и разглашения.

1.3. Настоящее Положение разработано в соответствии с:

– Конституцией Российской Федерации;

– Трудовым кодексом Российской Федерации;

– Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон о персональных данных);

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

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

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

– приказом ФСТЭК РФ от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– иными нормативными правовыми актами, регулирующими отношения, связанные с обработкой и защитой персональных данных.

1.4. Настоящее Положение и изменения к нему утверждаются директором Учреждения и вводятся приказом по Учреждению. Все работники Учреждения должны быть ознакомлены под роспись с данным Положением и изменениями к нему.

2. Основные понятия. Состав и категории персональных данных

2.1. Для целей настоящего Положения используются следующие основные понятия:

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

субъект персональных данных – физическое лицо, персональные данные которого обрабатываются Учреждением в связи с осуществлением его деятельности (работники, бывшие работники, претенденты на работу, контрагенты и другие);

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;

автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

пользователь – работник, участвующий в рамках своих функциональных обязанностей в процессах обработки информации;

распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

трансграничная передача данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу, иностранному юридическому лицу;

блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

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;

обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

информация – сведения (сообщения, данные) независимо от формы их представления;

доступ к информации – возможность получения информации и ее использования;

документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;

конфиденциальная информация – документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации;

носитель информации – любой материальный объект или среда, используемые для хранения или передачи информации;

контролируемая зона – пространство (территория, здание, часть здания, кабинеты), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств;

информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

автоматизированное рабочее место – персональный компьютер и подключенные к нему периферийные устройства (принтер, многофункциональные устройства, сканеры и т.д.);

база данных – информация, упорядоченная в виде набора элементов, записей одинаковой структуры;

программное обеспечение – все или часть программ, процедур, правил и соответствующей документации системы обработки информации;

дистрибутив программного обеспечения – файл или файлы, предназначенные для установки программного обеспечения;

защита информации – деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на информацию, то есть процесс, направленный на достижение информационной безопасности;

средство защиты информации – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации;

несанкционированный доступ – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т.д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т.д. различных организаций путем изменения (повышения, фальсификации) своих прав доступа;

антивирусная защита – комплекс мер, направленных на предотвращение, обнаружение и обезвреживание действий вредоносного программного обеспечения при помощи антивирусных программных продуктов;

средство антивирусной защиты – программный пакет, предназначенный для эффективной защиты, перехвата и удаления из операционной системы компьютера максимального количества вредоносных (или потенциально вредоносных) программ;

вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и / или воздействия на защищаемую информацию или ресурсы информационной системы;

угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных;

уровень защищенности персональных данных – комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

утечка защищаемой информации – неконтролируемое распространение информации от ее носителя;

пароль – секретная комбинация цифр, знаков, слов, или осмысленное предложение, служащие для защиты информации от несанкционированного доступа к информационным ресурсам;

компрометация пароля – раскрытие, обнаружение или утеря пароля.

2.2. Обработка персональных данных в Учреждении осуществляется в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества Учреждения, а также в целях выполнения возложенных на Учреждение функций и обязанностей.

2.3. Учреждение обрабатывает персональные данные следующих категорий субъектов персональных данных:

- работники;
- родственники работников;
- бывшие работники;
- кандидаты на замещение вакантных должностей;
- граждане и их законные представители;
- практиканты;
- контрагенты (физические лица);
- представители/работники контрагентов (юридических лиц);
- обратившиеся граждане.

2.4. Учреждение обрабатывает:

- персональные данные работников исключительно в следующих целях: выполнение требований законодательства Российской Федерации, осуществление трудовых отношений, заключение и выполнение обязательств по трудовым договорам;
- персональные данные родственников работников исключительно в следующих целях: ведение кадрового делопроизводства, бухгалтерского учета;
- персональные данные бывших работников исключительно в следующих целях: ведение кадрового делопроизводства, бухгалтерского учета;
- персональные данные кандидатов на замещение вакантных должностей исключительно в следующих целях: принятие решения о трудоустройстве;
- персональные данные практикантов исключительно в следующих целях: прохождение учебной практики и производственной практики;
- персональные данные контрагентов (физических лиц) исключительно в следующих целях: заключение и выполнение обязательств по договорам;
- персональные данные представителей/работников контрагентов (юридических лиц) исключительно в следующих целях: заключение и выполнение обязательств по договорам;
- персональные данные обратившихся граждан исключительно в следующих целях: информационно-справочного обслуживания, рассмотрения обращения гражданина и принятия мер по результату рассмотрения обращения.

2.5. Перечень обрабатываемых персональных данных работников:

– фамилия, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения);

– пол, возраст;

– число, месяц, год рождения;

– место рождения;

– информация о гражданстве (в том числе предыдущие гражданства, иные гражданства);

– вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;

– адрес места жительства (адрес регистрации, фактического проживания);

– номер контактного телефона или сведения о других способах связи;

– реквизиты страхового свидетельства государственного пенсионного страхования;

– идентификационный номер налогоплательщика;

– анкетные и биографические данные;

– реквизиты свидетельства государственной регистрации актов гражданского состояния;

– семейное положение, состав семьи и сведения о близких родственниках (в том числе бывших);

– сведения о трудовой деятельности;

– сведения о воинском учете и реквизиты документов воинского учета;

– сведения об образовании, в том числе о послевузовском профессиональном образовании (наименование и год окончания образовательного учреждения, наименование и реквизиты документа об образовании, квалификация, специальность по документу об образовании);

– сведения об ученой степени;

– информация о владении иностранными языками, степень владения;

– занимаемая должность или выполняемая работа, сведения о переводах на другую работу;

– табельный номер;

– сведения о заработной плате работника;

– сведения о дисциплинарных взысканиях;

– сведения о наградах и поощрениях работника;

– сведения о профессиональной переподготовке и (или) повышении квалификации;

– информация о ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения заработной платы;

– сведения о социальных гарантиях и льготах и основаниях их предоставления;

– результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей, сведения об инвалидности;

– сведения из водительского удостоверения;

– фотография;

– сведения о доходах, об имуществе и обязательствах имущественного характера;

– информация, содержащаяся в трудовом договоре, дополнительных соглашениях к трудовому договору и в иных кадровых документах, касающихся работника;

– номер расчетного счета, номер банковской карты;

– иные персональные данные, необходимые для достижения целей обработки персональных данных.

2.6. Перечень документов, содержащих персональные данные работников:

– анкета, автобиография;

– копия документа, удостоверяющего личность работника;

– личная карточка по форме № Т-2;

– трудовая книжка;

– копии свидетельств о заключении (расторжении) брака, рождении детей;

– документы воинского учета;

– справка о доходах с предыдущего места работы;

– справка о заработке для расчета пособий;
– карточка-справка на работника;
– документы об образовании;

– документы обязательного пенсионного страхования;
– трудовой договор, дополнительные соглашения к трудовому договору;
– подлинники и копии приказов по личному составу;
– дела, содержащие материалы аттестации работников;
– справочно-информационный банк данных по работникам (картотеки, журналы);
– подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству Учреждения;
– копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения;
– иные документы, содержащие персональные данные работников.

2.7. Персональные данные контрагентов и других лиц составляют:
– фамилия, имя, отчество;
– паспортные данные;
– адрес места жительства, номер телефона;
– другие сведения, полученные Учреждением при осуществлении своей деятельности.

2.8. Категории персональных данных.

2.8.1. По степени доступа персональные данные делятся на:
- общедоступные персональные данные;
- конфиденциальные персональные данные.

Все персональные данные являются конфиденциальными, за исключением общедоступных персональных данных. Раскрытие конфиденциальных персональных данных третьим лицам и их распространение не допускается без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Общедоступными персональными данными являются сведения, к которым обеспечен доступ неограниченного круга лиц самим субъектом персональных данных или по его просьбе, либо федеральным законом предусмотрено, что указанная информация относится к категории общедоступной.

В целях информационного обеспечения в Учреждении могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия работника могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые работником. Сведения о работнике должны быть в любое время исключены из общедоступных источников персональных данных по требованию работника либо по решению суда или иных уполномоченных государственных органов.

2.8.2. По направлению выделяют следующие категории персональных данных:
- специальные персональные данные (персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни);
- обычные персональные данные (все персональные данные, кроме тех, которые отнесены к специальным персональным данным).

2.8.3. По содержанию персональные данные разделяют на:
- биометрические персональные данные (сведения, характеризующие физиологические и биологические особенности человека, на основании которых можно

установить его личность, например, отпечатки пальцев, ладони, радужка сетчатки глаза, особенности строения тела, его отдельных частей, почерк и другие);

- не биометрические персональные данные (сведения, которые не относятся к биометрическим персональным данным).

3. Порядок обработки персональных данных работников Учреждения и иных лиц

3.1. Получение персональных данных и условия их обработки. Требования к обработке персональных данных

3.1.1. Источником информации обо всех персональных данных работника является непосредственно работник, который принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе.

3.1.2. Если предоставление персональных данных является обязательным в соответствии с федеральным законом, Учреждение обязано разъяснить работнику юридические последствия отказа предоставить его персональные данные.

3.1.3. Информация, представляемая работником при поступлении на работу в Учреждение, должна иметь документальную форму.

При заключении трудового договора в соответствии со статьей 65 Трудового кодекса Российской Федерации лицо, поступающее на работу, предъявляет Работодателю:

– паспорт или иной документ, удостоверяющий личность;

– трудовую книжку и (или) сведения о трудовой деятельности (статья 66.1 Трудового кодекса Российской Федерации), за исключением случаев, если трудовой договор заключается впервые;

– документ, подтверждающий регистрацию в системе индивидуального (персонифицированного) учета, в том числе в форме электронного документа;

– документы воинского учета – для военнообязанных и лиц, подлежащих призыву на военную службу;

– документ об образовании и (или) о квалификации или наличии специальных знаний - при поступлении на работу, требующую специальных знаний или специальной подготовки;

– дополнительные документы – в случаях, предусмотренных Трудовым кодексом Российской Федерации, иными федеральными законами, указами Президента Российской Федерации и постановлениями Правительства Российской Федерации.

На основании указанных документов, а также сведений, сообщенных о себе работником, на каждого работника заполняется унифицированная форма № Т-2 «Личная карточка работника».

3.1.4. В случае изменения своих персональных данных работник обязан незамедлительно уведомить об этом Учреждение.

3.1.5. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие.

Учреждение должно сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

3.1.6. При получении персональных данных не от работника Учреждение до начала обработки таких персональных данных обязано предоставить работнику следующую информацию:

– наименование и адрес Учреждения;

– цель обработки персональных данных и ее правовое основание;

– предполагаемые пользователи персональных данных;

– установленные Законом о персональных данных права работника;

– источник получения персональных данных.

Учреждение освобождается от обязанности предоставить работнику указанные сведения в случаях, если:

1) работник уведомлен об осуществлении обработки его персональных данных соответствующим оператором;

2) персональные данные получены Учреждением на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является работник;

3) персональные данные сделаны общедоступными работником или получены из общедоступного источника;

4) Учреждение осуществляет обработку персональных данных для статистических или иных исследовательских целей, если при этом не нарушаются права и законные интересы работника;

5) предоставление работнику указанных сведений нарушает права и законные интересы третьих лиц.

3.1.7. Обработка персональных данных работника осуществляется с его письменного согласия на обработку персональных данных, которое должно быть конкретным, информированным и сознательным и включать в себя:

– фамилию, имя, отчество, адрес работника, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

– наименование и адрес Учреждения;

– цель обработки персональных данных;

– перечень персональных данных, на обработку которых дается согласие работника;

– перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Учреждением способов обработки персональных данных;

– срок, в течение которого действует согласие работника, а также способ его отзыва, если иное не установлено федеральным законом;

– подпись работника.

3.1.8. Согласие работника не требуется в случаях, предусмотренных Законом о персональных данных, в том числе в следующих случаях:

– обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на Учреждение функций, полномочий и обязанностей;

– обработка персональных данных осуществляется в связи с участием лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах;

– обработка персональных данных необходима для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;

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

– обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов работника, если получение согласия работника невозможно;

– обработка персональных данных 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 работника;

– обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей продвижения товаров, работ, услуг на рынке и политической агитации, при условии обязательного обезличивания персональных данных;

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

– осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

3.1.9. Согласие на обработку персональных данных может быть отозвано работником. В случае отзыва работником согласия на обработку его персональных данных Учреждение обязано прекратить их обработку и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является работник, иным соглашением между Учреждением и работником либо если Учреждение не вправе осуществлять обработку персональных данных без согласия работника на основаниях, предусмотренных Законом о персональных данных или другими федеральными законами.

В случае отсутствия возможности уничтожения персональных данных в течение установленного срока Учреждение осуществляет блокирование таких персональных данных и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

В случае отзыва работником согласия на обработку персональных данных Учреждение вправе продолжить обработку персональных данных без согласия работника при наличии оснований, указанных в пунктах 2 – 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Закона о персональных данных.

3.1.10. Обработка персональных данных работников осуществляется как с использованием средств автоматизации, так и без использования таких средств.

3.1.11. При обработке персональных данных работников уполномоченные лица обязаны соблюдать следующие требования:

а) обработка персональных данных должна осуществляться на законной и справедливой основе;

б) при определении объема и содержания обрабатываемых персональных данных работника Учреждение должно руководствоваться Конституцией Российской Федерации, Трудовым кодексом Российской Федерации и иными федеральными законами;

в) обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных. Обработке подлежат только те персональные данные, которые отвечают целям их обработки;

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

д) 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;

е) 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. Учреждение должно принимать необходимые меры по удалению или уточнению неполных или неточных данных;

ё) при принятии решений, затрагивающих интересы работника, Учреждение не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения;

ж) защита персональных данных работника от неправомерного их использования или утраты обеспечивается в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами;

з) обеспечение конфиденциальности персональных данных работников, за исключением случаев обезличивания персональных данных и в отношении общедоступных персональных данных;

и) хранение персональных данных должно осуществляться в форме, позволяющей определить работника и иное лицо, являющееся субъектом 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 либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом. Факт уничтожения персональных данных оформляется соответствующим актом.

3.1.12. Обработка специальных категорий персональных данных работника не допускается, за исключением случаев, предусмотренных частью 2 статьи 10 Закона о персональных данных, в том числе за исключением следующих случаев:

- работник дал согласие в письменной форме на обработку своих персональных данных;

- персональные данные сделаны общедоступными работником;

- обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, пенсионным законодательством Российской Федерации;

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

- обработка персональных данных необходима для установления или осуществления прав работника или третьих лиц, а равно и в связи с осуществлением правосудия;

- обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством.

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

3.1.13. Биометрические персональные данные работника могут обрабатываться только при наличии согласия в письменной форме работника, за исключением случаев, предусмотренных частью 2 статьи 11 Закона о персональных данных.

3.1.14. В целях организации обработки персональных данных в Учреждении приказом директора Учреждения назначается лицо, ответственное за организацию обработки персональных данных, которое получает указания непосредственно от директора Учреждения и подотчетно ему.

Лицо, ответственное за организацию обработки персональных данных, в частности, обязано:

1) осуществлять внутренний контроль за соблюдением Учреждением и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

2) доводить до сведения работников Учреждения положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

3) организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

3.2. Обработка персональных данных без использования средств автоматизации

3.2.1. Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека. Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из нее.

3.2.2. Персональные данные при их неавтоматизированной обработке должны обособляться от иной информации, в частности путем их фиксации на отдельных материальных носителях персональных данных (далее – материальные носители), в специальных разделах или на полях форм (бланков).

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

различных категорий персональных данных для каждой категории персональных данных должен использоваться отдельный материальный носитель.

3.2.4. Лица, осуществляющие неавтоматизированную обработку персональных данных (в том числе работники Учреждения или лица, осуществляющие такую обработку по договору с Учреждением), до начала такой обработки должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется Учреждением без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами Учреждения.

3.2.5. 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, наименование и адрес Учреждения, 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 Учреждением 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, чьи персональные данные содержатся в документе, имел возможность ознакомиться со своими персональными данными, 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.

3.2.6. 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, принимаются 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.

3.2.7. 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).

3.2.8. Правила, предусмотренные подпунктами 3.2.6 и 3.2.7 настоящего Положения, применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.

3.2.9. Уточнение персональных данных при неавтоматизированной обработке 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.

3.2.10. 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.

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

3.3. Автоматизированная обработка персональных данных

3.3.1. Автоматизированная обработка персональных данных в Учреждении осуществляется:

1) в Единой информационной системе бюджетного (бухгалтерского) учета на платформе «АС Смета»;

2) на автоматизированных рабочих местах работников Учреждения, осуществляющих обработку персональных данных.

3.3.2. Указанная информационная система содержит персональные данные работников Учреждения и физических лиц, являющихся стороной гражданско-правовых договоров, заключаемых Учреждением, и включает в себя, в том числе (но не ограничиваясь):

– фамилию, имя, отчество субъекта персональных данных;

– дату рождения субъекта персональных данных;

– место рождения субъекта персональных данных;

– серию и номер основного документа, удостоверяющего личность субъекта персональных данных, сведения о дате выдачи указанного документа и выдавшем его органе;

– адрес места жительства субъекта персональных данных;

– почтовый адрес субъекта персональных данных;

– телефон субъекта персональных данных;

– ИНН субъекта персональных данных;

– номер страхового свидетельства государственного пенсионного страхования;

– табельный номер субъекта персональных данных;

– должность субъекта персональных данных;
– данные об образовании субъекта персональных данных;
– данные по воинскому учету;
– данные об иждивенцах субъекта персональных данных;
– номер приказа и дату приема на работу (увольнения) субъекта персональных данных;

3.3.3. Автоматизированные рабочие места работников Учреждения, осуществляющих обработку персональных данных, предполагают обработку персональных данных работников Учреждения, предусмотренных пунктом 2.2 настоящего Положения.

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

3.3.5. Средства защиты информации, применяемые в информационных системах, в обязательном порядке проходят процедуру оценки соответствия в установленном законодательством Российской Федерации порядке.

3.3.6. Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер, а также применения технических и (или) программных средств.

3.3.7. Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

3.3.8. Каждый работник Учреждения, являющийся пользователем информационной системы персональных данных, обязан:

а) строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами информационной системы персональных данных;

б) знать и строго выполнять правила работы со средствами защиты информации, установленными на его автоматизированном рабочем месте;

в) соблюдать правила работы с паролем своей учетной записи;

г) немедленно вызвать ответственного за обеспечение безопасности персональных данных в информационных системах и поставить в известность руководителя структурного подразделения при обнаружении:

- нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на аппаратных средствах автоматизированных рабочих мест или иных фактов совершения в его отсутствие попыток несанкционированного доступа к защищаемому автоматизированному рабочему месту;

- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств автоматизированных рабочих мест;

- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию автоматизированных рабочих мест, выхода из строя или неустойчивого функционирования узлов автоматизированных рабочих мест или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения;

- некорректного функционирования установленных на автоматизированных рабочих местах технических средств защиты;

- непредусмотренных отводов кабелей и подключенных к автоматизированным рабочим местам дополнительных устройств.

3.3.9. Всем работникам Учреждения, являющимся пользователями информационной системы персональных данных, запрещается:

а) использовать компоненты программного и аппаратного обеспечения информационной системы персональных данных Учреждения в неслужебных целях;

б) самовольно вносить какие-либо изменения в конфигурацию автоматизированных рабочих мест или устанавливать на автоматизированных рабочих местах любые программные и аппаратные средства, кроме выданных или разрешенных к использованию ответственным за обеспечение безопасности персональных данных;

в) оставлять без присмотра свое автоматизированное рабочее место не активизировав блокировки доступа или оставлять свое автоматизированное рабочее место включенным по окончании работы;

г) умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к нарушению безопасности персональных данных.

3.3.10. Для обеспечения сохранности электронных информационных ресурсов Учреждения необходимо соблюдать следующие требования:

1) для копирования информации не должны использоваться непроверенные на наличие компьютерных вирусов и других вредоносных программ носители информации;

2) субъектам доступа запрещается:

а) установка и использование при работе на автоматизированном рабочем месте вредоносных программ, ведущих к блокированию работы сети;

б) самовольное изменение сетевых адресов;

в) самовольное вскрытие блоков автоматизированных рабочих мест, модернизация или модификация автоматизированных рабочих мест и программного обеспечения;

г) несанкционированная передача автоматизированных рабочих мест с прописанными сетевыми настройками. Передача автоматизированных рабочих мест из одного структурного подразделения в другое производится только ответственным за обеспечение безопасности персональных данных в информационных системах с предварительно удаленными сетевыми настройками;

3) сведения, содержащиеся в электронных документах и базах данных Учреждения, должны использоваться только в служебных целях в рамках полномочий работника, работающего с соответствующими материалами.

3.3.11. Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении работника или иным образом затрагивающих его права и законные интересы, за исключением случаев, если имеется согласие работника в письменной

форме, и иных случаев, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов работника.

Работнику должен быть разъяснен порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставлена возможность заявить возражение против такого решения, а также разъяснен порядок защиты работником своих прав и законных интересов. В случае, если работник заявил возражение, оно должно быть рассмотрено в течение тридцати дней со дня его получения, и работник должен быть уведомлен о результатах рассмотрения такого возражения.

4. Передача персональных данных

4.1. При передаче персональных данных работника Учреждение должно соблюдать следующие требования:

4.1.1. Не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных Трудовым кодексом Российской Федерации или иными федеральными законами.

В случае если лицо, обратившееся с запросом, не уполномочено федеральным законом на получение такой информации либо отсутствует письменное согласие работника на передачу его персональных данных третьей стороне Учреждение обязано отказать в предоставлении персональных данных.

В этом случае лицу, обратившемуся с запросом, направляется письменный мотивированный отказ в предоставлении персональных данных.

4.1.2. Не сообщать персональные данные работника в коммерческих целях без его письменного согласия.

4.1.3. Предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными работников в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами.

4.1.4. Осуществлять передачу персональных данных работника в пределах Учреждения в соответствии с настоящим Положением, с которым работник должен быть ознакомлен под роспись.

4.1.5. Разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций.

4.1.6. Не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции.

4.1.7. Передавать персональные данные работника представителям работников в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

4.2. Без письменного согласия работника его персональные данные предоставляются по основаниям, предусмотренным действующим законодательством Российской Федерации.

4.3. Персональные данные субъекта могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого субъекта, за исключением случаев, когда передача персональных данных субъекта без его согласия допускается действующим законодательством Российской Федерации либо договором, регламентирующим правоотношения Учреждения с субъектом.

4.4. Ответы на мотивированные запросы третьих лиц в пределах их компетенции и предоставленных полномочий даются в письменной форме, на бланке организации и в том объеме, который позволяет не разглашать излишний объем персональных данных о субъектах и в соответствии с Разъяснениями Роскомнадзора от 14 декабря 2012 года.

4.5. Работники Учреждения, передающие документы (или иные материальные носители информации) с персональными данными субъектов третьим лицам, должны передавать их с обязательным составлением двустороннего акта приема-передачи документов (иных материальных носителей информации), содержащих персональные данные субъектов. Акт составляется по установленной форме, и должен содержать следующие условия:

- уведомление лица, получающего данные документы об обязанности использования полученных персональных данных лишь в целях, для которых они сообщены;

- предупреждение об ответственности за противоправную обработку персональных данных в соответствии с действующим законодательством Российской Федерации.

4.6. Работникам, имеющим доступ к персональным данным работника, запрещается отвечать на вопросы, связанные с передачей персональной информации, по телефону или факсу.

5. Использование, хранение и уничтожение персональных данных

5.1. Внутренний доступ.

5.1.1. Право доступа к персональным данным работника имеют:

– директор Учреждения или лицо, исполняющее его обязанности;

– руководители структурных подразделений по направлению деятельности (доступ к документам, содержащим персональные данные подчиненного им работника);

– руководитель иного подразделения при переводе работника из одного структурного подразделения в другое;

– работник - носитель персональных данных;

– работники (заместитель директора по финансовой работе, специалист по кадрам, специалист по охране труда, ведущий инженер, техник-энергетик, ведущий экономист);

5.1.2. Правом ознакомления с документами, содержащими персональные данные работника, имеет директор Учреждения. По распоряжению директора специалист по кадрам, ответственный за работу с соответствующими документами, обязан лично передать требуемые документы непосредственно директору.

5.1.3. Руководители структурных подразделений имеют право ознакомиться с документами, содержащими персональные данные подчиненного им работника, в

кабинете № 5 в присутствии специалиста по кадрам, ответственного за работу с соответствующими документами.

5.1.4. Работник имеет право ознакомиться с документами, содержащими его персональные данные, в кабинете № 219 в присутствии специалиста по кадрам, ответственного за работу с соответствующими документами.

5.2. Внешний доступ.

5.2.1. К лицам, которым могут быть переданы персональные данные вне Учреждения, при условии соблюдения требований законодательства, относятся представители: налоговой инспекции; правоохранительных органов; органов статистики; страховых агентств; военкоматов; органов социального страхования; государственного пенсионного фонда; подразделений муниципальных органов управления.

5.2.2. Надзорно-контрольные органы имеют доступ к информации только в пределах своей компетенции.

5.2.3. Организации, в которые работник перечисляет денежные средства (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения), могут получить доступ к персональным данным работника только при наличии его письменного разрешения.

5.2.4. Сведения о работающем или уволенном работнике могут быть предоставлены другой организации только по письменному запросу на бланке организации с приложением согласия работника.

5.3. Лица, имеющие доступ к персональным данным, а также лица, ответственные за их обработку, должны принимать меры, препятствующие ознакомлению с персональными данными работников лиц, не имеющих доступа к персональным данным.

5.4. Допуск к конфиденциальным персональным данным включает в себя:

1) ознакомление работника с законодательством Российской Федерации в области персональных данных, локальными нормативными актами, в том числе перечнем обрабатываемых персональных данных;

2) принятие работником на себя обязанности по соблюдению конфиденциальности персональных данных, к которым получает доступ;

3) соблюдение требований по защите конфиденциальной информации.

5.5. В целях обеспечения защиты персональных данных работника от их неправомерного доступа или утраты с работниками, имеющими доступ к персональным данным других работников, оформляется обязательство о неразглашении персональных данных.

5.6. Все документы, содержащие конфиденциальные персональные данные должны сохраняться в режиме конфиденциальности и быть доступными только тем лицам, которые имеют допуск к таким сведениям в силу исполнения ими своих должностных обязанностей.

Лица, должностные обязанности которых не связаны с обработкой персональных данных, могут быть допущены к персональным данным только с их письменного согласия. При случайном получении персональных данных неуполномоченным лицом, оформляется обязательство о неразглашении персональных данных.

Умышленное получение персональных данных неуполномоченными лицами является основанием для привлечения к ответственности, предусмотренной законодательством Российской Федерации.

5.7. При работе с документами, содержащими конфиденциальные персональные данные, запрещается:

- делать выписки без соответствующего разрешения директора Учреждения;

- знакомить с конфиденциальными документами неуполномоченных лиц, в том числе других работников;

- использовать информацию из таких документов в открытых сообщениях, докладах, переписке;

- предоставлять свой компьютер для работы другим работникам;

- оставлять без присмотра на рабочем месте конфиденциальные документы, включенный компьютер.

5.8. С работниками, имеющими доступ к персональным данным, не реже одного раза в год лицом, ответственным за организацию обработки персональных данных в Учреждении, проводится обучение и проверка знания требований нормативно-технических документов в области обработки и защиты персональных данных.

Внеочередное обучение и проверка знаний проводится при изменении законодательства Российской Федерации в области персональных данных и внесении изменений и дополнений в настоящее Положение.

5.9. Персональные данные работников могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде (посредством локальной компьютерной сети).

5.10. Хранение персональных данных осуществляется в порядке, исключающем их утрату или неправомерное использование.

5.11. Все персональные данные, в том числе персональные данные, полученные от работника при приеме на работу и в процессе выполнения им своей трудовой функции (трудовая книжка, личная карточка по форме № Т-2, трудовой договор, заявления, приказы, письменное согласие на обработку персональных данных, бухгалтерские документы и т.д.), хранятся в местах, исключающих доступ посторонних лиц к персональным данным.

5.12. Персональные данные работника могут также храниться в электронном виде на локальной компьютерной сети. Доступ к электронным базам данных, содержащим персональные данные работника, обеспечивается системой паролей.

5.13. По возможности персональные данные должны быть обезличены.

5.14. В случае достижения цели обработки персональных данных Учреждение обязано прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является работник, иным соглашением между Учреждением и работником либо если Учреждение не вправе осуществлять обработку персональных данных без согласия работника на основаниях, предусмотренных Законом о персональных данных или другими федеральными законами.

В случае отсутствия возможности уничтожения персональных данных в течение установленного срока Учреждение осуществляет блокирование таких персональных данных и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

5.15. Уничтожение носителей персональных данных осуществляется комиссией. Комиссию возглавляет ответственный за организацию обработки персональных данных в Учреждении. Уничтожение должно происходить в присутствии всех членов комиссии.

5.16. Уничтожение бумажных носителей осуществляется путем измельчения.

5.17. Уничтожение электронных файлов, содержащих персональные данные, осуществляется путем их удаления с использованием средств операционной системы с

последующим «очищением корзины». Допускается гарантированное удаление информации методом многократной перезаписи с помощью специализированных программ.

5.18. Уничтожение машинных носителей, содержащих персональные данные, осуществляется путем деформирования, нарушения единой целостности носителя. Факт уничтожения машинных носителей фиксируется комиссией в Акте уничтожения носителей.

6. Защита персональных данных. Права работника в целях обеспечения защиты персональных данных

6.1. Общие положения по защите персональных данных

6.1.1. Защита персональных данных представляет собой регламентированный технологический процесс, предупреждающий нарушение установленного порядка доступности, целостности, достоверности и конфиденциальности персональных данных и обеспечивающий безопасность информации в процессе управленческой и производственной деятельности Учреждения.

6.1.2. В целях обеспечения внешней защиты персональных данных работников помещения, в которых хранятся персональные данные, должны быть оборудованы техническими средствами пожарной сигнализации, а помещения, расположенные на первом этаже здания, также должны быть оборудованы техническими средствами охраны.

6.1.3. Меры по обеспечению внутренней защиты персональных данных:

6.1.3.1. Определение и закрепление перечня обрабатываемых персональных данных.

6.1.3.2. Ограничение доступа к информации, составляющей персональные данные, посредством установления порядка обращения с этой информацией и контроля за его соблюдением.

6.1.3.3. Установление перечня работников, имеющих допуск к персональным данным, оформление обязательств о неразглашении персональных данных.

6.1.3.4. Избирательное и обоснованное распределение документов и информации, содержащей персональные данные, между лицами, уполномоченными на работу с такими данными.

6.1.3.5. Рациональное размещение рабочих мест для исключения бесконтрольного использования защищаемой информации, создание необходимых условий для работы с документами и базами данных, содержащими персональные данные работников.

6.1.3.6. Обучение и регулярная проверка знания работниками, имеющими доступ к персональным данным, требований нормативно-технических документов в области обработки и защиты персональных данных.

6.1.3.7. Своевременное выявление и устранение нарушений установленных требований по защите персональных данных работников, проведение профилактической работы с лицами, имеющими доступ к персональным данным работников, по предупреждению разглашения таких сведений.

6.1.4. Защита персональных данных при их обработке в информационных системах персональных данных.

6.1.4.1. Уполномоченными лицами при обработке персональных данных в информационных системах должна быть обеспечена их безопасность с помощью системы защиты, включающей организационные меры и средства защиты информации.

6.1.4.2. Обеспечение безопасности персональных данных при их обработке в информационных системах достигается, в частности:

- определением угроз безопасности персональных данных;
- применением организационных и технических мер по обеспечению безопасности персональных данных;
- применением соответствующих средств защиты информации;
- оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы;
- учетом машинных носителей персональных данных;
- обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;
- восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установлением правил доступа к персональным данным, обрабатываемым в информационной системе, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе;
- контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем.

6.1.4.3. При обработке персональных данных в информационной системе Учреждения устанавливается 3-й уровень защищенности персональных данных.

Для обеспечения указанного уровня защищенности принимаются следующие меры:

- установление режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
- обеспечение сохранности носителей персональных данных;
- утверждение директором Учреждения перечня лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими должностных обязанностей;
- назначение лица, ответственного за обеспечение безопасности персональных данных в информационной системе.

6.1.4.4. Лицом, ответственным за обеспечение безопасности персональных данных при их обработке в информационной системе, должно быть обеспечено:

а) своевременное обнаружение фактов несанкционированного доступа к персональным данным и немедленное доведение этой информации до руководства Учреждения;

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

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

г) постоянный контроль за обеспечением уровня защищенности персональных данных;

д) знание и соблюдение условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

е) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

ё) при обнаружении нарушений порядка предоставления персональных данных незамедлительное приостановление предоставления персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин;

ж) разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

6.1.4.5. В случае выявления нарушений порядка обработки персональных данных в информационной системе Учреждения, уполномоченными лицами принимаются меры по установлению причин нарушений и их устранению.

6.2. Организация антивирусной защиты

6.2.1. К использованию в Учреждении допускаются только сертифицированные и лицензионные средства антивирусной защиты, закупленные у разработчиков или поставщиков данных средств.

6.2.2. Организация установки средств антивирусного контроля на автоматизированных рабочих местах и серверах информационных систем Учреждения осуществляется ответственным за обеспечение безопасности персональных данных в информационных системах, настройка параметров средств антивирусного контроля осуществляется в соответствии с руководствами по применению конкретных антивирусных средств и требованиями нормативных документов ФСТЭК РФ в области защиты информации.

6.2.3. Антивирусный контроль должен быть настроен в режиме постоянной антивирусной защиты.

6.2.4. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), хранящаяся на автоматизированных рабочих местах, передающаяся по сети, а также информация на съемных носителях. Контроль входящей информации должен осуществляться автоматически, непосредственно после ее приема. При передаче файлов, запакованных в архивы, без их распаковки, должна вручную инициироваться антивирусная проверка этих архивов.

6.2.5. Процедура обновления баз средства антивирусной защиты должна проводиться в автоматическом режиме не реже 1 (одного) раза в день на всех автоматизированных рабочих местах информационных систем, работающих в сети, не реже 1 (одного) раза в неделю для всех автоматизированных рабочих мест информационных систем, работающих автономно.

6.2.6. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено пользователями информационных систем на предмет отсутствия вредоносного программного обеспечения.

6.2.7. Подключаемые к компьютеру внешние устройства и носители информации должны проверяться антивирусным программным обеспечением непосредственно после подключения.

6.2.8. Периодический контроль за состоянием антивирусной защиты (обновление антивирусной программы и антивирусных баз, а также проверка работоспособности средств антивирусной защиты) в информационных системах Учреждения, осуществляется ответственным за обеспечение безопасности персональных данных в информационных системах, пользователями информационных систем и всеми должностными лицами, настраивающими и сопровождающими средства антивирусной защиты в информационных системах Учреждения.

6.2.9. При возникновении подозрения на наличие вредоносного программного обеспечения (частые ошибки в работе программ, появление посторонних графических и звуковых эффектов, искажения данных, неконтролируемое пропадание файлов, появление сообщений о системных ошибках, замедление работы компьютера и т.п.) пользователь информационной системы самостоятельно или вместе с ответственным за обеспечение безопасности персональных данных в информационных системах обязан провести внеочередной антивирусный контроль своего автоматизированного рабочего места.

При самостоятельном проведении антивирусного контроля пользователю информационной системы необходимо уведомить о результатах ответственного за обеспечение безопасности персональных данных в информационных системах для определения им факта наличия или отсутствия вредоносного программного обеспечения.

6.2.10. В случае появления информационного окна средства антивирусной защиты, сигнализирующем об обнаружении вредоносного программного обеспечения, пользователь информационной системы обязан:

- приостановить обработку данных;

- немедленно поставить в известность о факте обнаружения вредоносного программного обеспечения ответственного за обеспечение безопасности информации, владельца зараженных файлов, а также смежные структурные подразделения, использующие эти файлы в работе;

- совместно с владельцем файлов, зараженных вредоносным программным обеспечением, провести анализ необходимости дальнейшего их использования;

- произвести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь ответственного за обеспечение безопасности персональных данных в информационных системах).

6.3. Организация парольной защиты

6.3.1. Личные пароли должны выбираться пользователями информационной системы самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 6 символов;

- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);

- пароль не должен включать в себя имя пользователя, легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков (111, qwerty, абвгд и т.д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), аббревиатуры, клички домашних

животных, номера автомобилей, телефонов и другие значимые сочетаний букв и знаков, которые можно угадать, основываясь на информации о пользователе;

- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6-ти позициях.

6.3.2. Пользователям допускается использовать пароли, составленные из первых букв слов запоминающихся высказываний в разном регистре, смешанные в произвольном порядке со специальными символами (например, Кожзгсф7!).

6.3.3. Для обеспечения возможности использования имен и паролей некоторых работников в их отсутствие (например, в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п.), работники обязаны сразу же после установки своих паролей передавать их на хранение вместе с именами своих учетных записей ответственному за обеспечение безопасности персональных данных в информационных системах в запечатанном конверте или опечатанном пенале.

6.3.4. При вводе пароля пользователю необходимо исключить произнесение его вслух, возможность его подсматривания посторонними лицами (человек за спиной, наблюдение человеком за движением пальцев в прямой видимости или в отраженном свете) и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т.п.).

6.3.5. Смена паролей должна проводиться регулярно, не реже одного раза в 3 месяца, самостоятельно каждым пользователем.

6.3.6. В случае прекращения полномочий пользователя (увольнение, переход на другую работу и т.п.) должно производиться немедленное удаление его учетной записи сразу после окончания последнего сеанса работы данного пользователя с системой.

6.3.7. Временный пароль, заданный ответственным за обеспечение безопасности персональных данных в информационных системах при регистрации нового пользователя, должен действовать в течение ограниченного срока времени. Пользователь должен изменить временный пароль при первом входе в систему.

6.3.8. Срочная (внеплановая) полная смена паролей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) ответственных за обеспечение безопасности персональных данных в информационных системах, администраторов информационной системы и других работников, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты.

6.3.9. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке, мобильном телефоне и любых других предметах и носителях информации.

6.3.10. Запрещается сообщать свой пароль полностью или частично другим пользователям, запрещается спрашивать или подсматривать пароль других пользователей.

6.3.11. Запрещается регистрировать других пользователей в информационной системе со своим личным паролем, запрещается входить в информационную систему под учетной записью и паролем другого пользователя.

6.3.12. В случае утери или компрометации (разглашения, утраты) или подозрения в компрометации пароля пользователя должна быть немедленно проведена внеплановая процедура смены пароля.

6.4. Права работника в целях обеспечения защиты персональных данных

6.4.1. В целях обеспечения защиты персональных данных, хранящихся в Учреждении, работник вправе:

а) получать полную информацию о своих персональных данных и обработке этих данных;

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

в) определять своих представителей для защиты своих персональных данных;

г) получать доступ к медицинской документации, отражающей состояние его здоровья, с помощью медицинского работника по его выбору;

д) требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением требований Трудового кодекса Российской Федерации или иного федерального закона. При отказе Учреждения исключить или исправить персональные данные работника он имеет право заявить в письменной форме о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения;

е) требовать об извещении Учреждением всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;

ё) обжаловать в порядке, установленном законодательством Российской Федерации, любые неправомерные действия или бездействия уполномоченных лиц при обработке и защите его персональных данных.

6.4.2. В случае выявления неточных персональных данных при обращении работника или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных Учреждение обязано осуществить блокирование персональных данных, относящихся к этому работнику, с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы работника или третьих лиц.

В случае подтверждения факта неточности персональных данных Учреждение на основании сведений, представленных работником или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязано уточнить персональные данные в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

6.4.3. В случае выявления неправомерной обработки персональных данных при обращении работника или его представителя либо по запросу работника или его представителя либо уполномоченного органа по защите прав субъектов персональных данных Учреждение обязано осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому работнику, с момента такого обращения или получения указанного запроса на период проверки.

6.4.4. В случае выявления неправомерной обработки персональных данных, осуществляемой Учреждением, Учреждение в срок, не превышающий трех рабочих дней с даты этого выявления, обязано прекратить неправомерную обработку персональных данных.

В случае, если обеспечить правомерность обработки персональных данных невозможно, Учреждение в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязано уничтожить такие персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных Учреждение обязано уведомить работника или его представителя,

а в случае, если обращение работника 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.

7. Порядок взаимодействия Учреждения с субъектами персональных данных

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

1) подтверждение факта обработки персональных данных Учреждением;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые Учреждением способы обработки персональных данных;

4) наименование и место нахождения Учреждения, сведения о лицах (за исключением работников Учреждения), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Учреждением 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 Законом 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 Учреждения, если обработка поручена или будет поручена такому лицу;

10) иные сведения, предусмотренные Законом о персональных данных или другими федеральными законами.

Указанные сведения должны быть предоставлены субъекту 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 персональных данных.

7.2. Сведения предоставляются субъекту персональных данных или его представителю Учреждением при обращении либо при получении запроса субъекта персональных данных или его представителя, который должен содержать:

- номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе;

- сведения, подтверждающие участие субъекта персональных данных в отношениях с Учреждением (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Учреждением;

- подпись субъекта персональных данных или его представителя.

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

7.3. Учреждение обязано сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя.

7.4. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных работнике или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя Учреждение обязано дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Закона о персональных данных или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

7.5. Учреждение обязано предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных.

7.6. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, Учреждение обязано внести в них необходимые изменения.

7.7. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Учреждение обязано уничтожить такие персональные данные.

7.8. Учреждение обязано 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.

7.9. В случае, если информация, касающаяся обработки персональных данных субъекта персональных данных, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к Учреждению или направить ему повторный запрос в целях получения указанной информации и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

7.10. Субъект персональных данных вправе обратиться повторно к Учреждению или направить ему повторный запрос в целях получения информации, касающейся обработки персональных данных субъекта персональных данных, а также в целях ознакомления с обрабатываемыми персональными данными до истечения указанного срока в случае, если такая информация и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам

рассмотрения первоначального обращения. Повторный запрос в обязательном порядке должен содержать обоснование его направления.

7.11. Учреждение вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего установленным условиям. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Учреждении.

7.12. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе в случаях, предусмотренных частью 8 статьи 14 Закона о персональных данных.

8. Ответственность за нарушение норм, регулирующих обработку персональных данных

8.1. Работники Учреждения, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъектов, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

8.2. Разглашение персональных данных субъекта (передача их посторонним лицам, в том числе другим работникам, не имеющим к ним допуск), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных локальными нормативно-правовыми актами Учреждения, влечет наложение на работника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде: замечания, выговора, увольнения.

Работник Учреждения, имеющий доступ к персональным данным субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба Учреждению в соответствии с пунктом 7 статьи 243 Трудового кодекса Российской Федерации.

8.3. В отдельных случаях, при разглашении персональных данных, работник, совершивший указанный проступок, несет ответственность в соответствии со статьей 13.14 Кодекса об административных правонарушениях Российской Федерации.

8.4. В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушения неприкосновенности частной жизни), предусмотрена ответственность в соответствии со статьей 137 Уголовного кодекса Российской Федерации.