УТВЕРЖДЕНО
Приказом ФГБНУ ФНАЦ ВИМ
от 31.08.2022 № 221/1

ПОЛОЖЕНИЕ
о защите персональных данных работников Федерального государственного бюджетного научного учреждения «Федеральный научный агроинженерный центр ВИМ» (ФГБНУ ФНАЦ ВИМ)

г. Москва

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение разработано в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Гражданским кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

1.2. Цель разработки Положения - определение порядка обработки и защиты персональных данных работников ФГБНУ ФНАЦ ВИМ, далее – Учреждение, полученных в процессе деятельности Учреждения и необходимых в связи с трудовыми отношениями, и иных субъектов персональных данных, персональные данные которых подлежат обработке на основании полномочий Учреждения; обеспечение защиты прав и свобод человека и гражданина, в т.ч. работников Учреждения, при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.3. Режим конфиденциальности персональных данных снимается в случаях их обезличивания и по истечении 75 лет срока их хранения, или продлевается на основании заключения экспертной комиссии Учреждения, если иное не определено законом.

2. ОСНОВНЫЕ ПОНЯТИЯ, СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ И ПЕРЕЧЕНЬ ДОКУМЕНТОВ И СВЕДЕНИЙ, СОДЕРЖАЩИХ ПЕРСОНАЛЬНЫЕ ДАННЫЕ РАБОТНИКА

2.1. Для целей настоящего Положения используются следующие основные понятия:

- персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации субъекту персональных данных;

- биометрические персональные данные – сведения, характеризующие физиологические и биологические особенности субъекта персональных данных, которые используются оператором для установления личности субъекта персональных данных;

- обработка персональных данных – любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемых с использованием средств автоматизации (с помощью средств вычислительной техники) или без их использования, в том числе сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, распространение (в том числе передача, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

- конфиденциальность персональных данных – обязательное для соблюдения назначенного ответственного лица, получившего доступ к персональным данным, требование не допускать их распространения без согласия субъекта персональных данных или иного законного основания;

- распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

- использование персональных данных – действия (операции) с персональными данными, совершаемые должностным лицом Учреждения в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъектов персональных данных либо иным образом затрагивающих их права и свободы или права и свободы других лиц;

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

- блокирование персональных данных – временное прекращение обработки персональных данных, в т.ч. сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи (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 или в результате которых уничтожаются материальные носители персональных данных;

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

- общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;

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

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

- документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель;

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

- угроза 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 информационной системе.

2.2. В состав персональных данных работников Учреждения входят:

- анкета;
- автобиография;
- сведения об образовании;
- сведения о трудовом и общем стаже;
- сведения о предыдущем месте работы;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- сведения о заработной плате сотрудника;
- сведения о социальных льготах;
- специальность;
- занимаемая должность;
- наличие судимостей;
- ИНН, СНИЛС;
- адрес места жительства, регистрации;
- номера домашнего и мобильного (сотового) телефона;
- содержание трудового договора;
- содержание декларации, подаваемой в налоговую инспекцию;
- подлинники и копии приказов по личному составу;
- личные дела, трудовые книжки и сведения о трудовой деятельности работников;
- основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке работников, их аттестации, служебным расследованиям;
- копии отчетов, направляемые в органы статистики;
- копии документов об образовании;
- результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей;

- фотографии и иные сведения, относящиеся к персональным данным работника;

- рекомендации, характеристики;

- принадлежность лица к конкретной нации, этнической группе, расе;

- привычки и увлечения, в том числе вредные (алкоголь, наркотики и др.);

- семейное положение, наличие детей, родственные связи;

- религиозные и политические убеждения (принадлежность к религиозной конфессии, членство в политической партии, участие в общественных объединениях, в том числе в профсоюзе и др.);

- финансовое положение (доходы, долги, владение недвижимым имуществом, денежные вклады и др.);

- деловые и иные личные качества, которые носят оценочный характер;

- прочие сведения, которые могут идентифицировать человека.

2.3. Комплект документов, сопровождающий процесс оформления трудовых отношений работника в Учреждения при его приеме, переводе и увольнении:

2.3.1. Информация, представляемая работником при поступлении на работу или обучение в Учреждение, должна иметь документальную форму. При заключении трудового договора в соответствии со ст. 65 Трудового кодекса Российской Федерации лицо, поступающее на работу, предъявляет работодателю следующие документы, содержащие его персональные данные, в том числе:

- паспорт или иной документ, удостоверяющий личность;

- трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или работник поступает на работу на условиях совместительства, либо трудовая книжка у работника отсутствует в связи с ее утратой или по другим причинам;

- документ, подтверждающий регистрацию в системе индивидуального (персонифицированного) учета, в том числе в форме электронного документа (страховое свидетельство (карточка) СНИЛС или уведомление о регистрации в системе индивидуального (персонифицированного) учета (форма АДИ-РЕГ));

- свидетельство о постановке на учет в налоговом органе (при наличии его у работника);

- документы воинского учета – для военнообязанных и лиц, подлежащих воинскому учету;

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

- справку, выданную органами МВД России, о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования по реабилитирующим основаниям (при поступлении на работу, к выполнению которой в соответствии с Трудовым кодексом Российской Федерации или иным федеральным законом не допускаются лица, имеющие или имевшие судимость, подвергающиеся или подвергавшиеся уголовному преследованию);

- дополнительные документы – в отдельных случаях, предусмотренных Трудовым кодексом Российской Федерации, иными федеральными законами, указами Президента Российской Федерации и постановлениями Правительства Российской Федерации, в том числе медицинское заключение о состоянии здоровья с возможностью занимать определенные должности.

2.3.2. При оформлении работника в Учреждение работником отдела кадров заполняется унифицированная форма Т-2 «Личная карточка работника», в которой отражаются следующие анкетные и биографические данные работника:

- общие сведения (Ф.И.О. работника, дата рождения, место рождения, гражданство, образование, профессия, стаж работы, состояние в браке, паспортные данные);
- сведения о воинском учете;
- данные о приеме на работу, включая должностной оклад.

В дальнейшем в личную карточку вносятся:

- сведения о переводах на другую работу;
- сведения об аттестации;
- сведения о повышении квалификации;
- сведения о профессиональной переподготовке;
- сведения о наградах (поощрениях), почетных званиях;
- сведения об отпусках;
- сведения о социальных гарантиях;
- сведения о месте жительства и контактных телефонах;
- иная необходимая информация.

2.3.3. В Учреждении создаются и хранятся следующие группы документов, содержащие данные о работниках в единичном или сводном виде:

2.3.3.1. Документы, содержащие персональные данные работников (комплекты документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении; комплект материалов по анкетированию, тестированию; проведению собеседований с кандидатом на должность; подлинники и копии приказов по личному составу; личные дела и трудовые книжки работников; дела, содержащие основания к приказу по личному составу; дела, содержащие материалы аттестации работников; служебных расследований; сведения о здоровье; справочно-информационный банк данных по персоналу (картотеки, журналы); подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству Учреждения, руководителям структурных подразделений; копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения, в ФГБНУ «Дирекция научно-технических программ», Единую государственную информационную систему учета научно-исследовательских, опытно-конструкторских и технологических работ гражданского назначения»).

2.3.3.2. Документация по организации работы структурных подразделений (положения о структурных подразделениях, должностные инструкции работников, приказы, распоряжения, указания руководства Учреждения); документы по планированию, учету, анализу и отчетности в части работы с персоналом Учреждения.

3. ОБЩИЕ ТРЕБОВАНИЯ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ И ГАРАНТИИ ИХ ЗАЩИТЫ

3.1. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных. Обработка персональных данных работника осуществляется исключительно в

целях обеспечения соблюдения законов и иных нормативных правовых актов.

3.2. Правовым основанием обработки персональных данных является совокупность правовых актов, во исполнение которых и в соответствии с которыми Учреждение осуществляет обработку персональных данных. В качестве правового обоснования могут быть указаны:

- федеральные законы и принятые на их основе нормативные правовые акты, регулирующие отношения, связанные с деятельностью Учреждения;
- учредительные документы Учреждения;
- договоры, заключаемые между Учреждением и работником;
- согласие на обработку персональных данных.

3.3. Все персональные данные работника передаются им лично. 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. Работодатель должен 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.

3.4. Работодатель вправе обрабатывать персональные данные работников только с их письменного согласия.

3.5. Письменное согласие работника на обработку своих персональных данных должно включать в себя в частности:

1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

3) наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;

4) цель обработки персональных данных;

5) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

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

7) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

8) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом.

Требования к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения, устанавливаются уполномоченным органом по защите прав субъектов персональных данных.

3.6. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных.

3.7. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев, предусмотренных федеральным законом.

Обработка указанных специальных категорий персональных данных допускается в случаях, если:

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

2) обработка персональных данных, разрешенных субъектом персональных данных для распространения, осуществляется с соблюдением запретов и условий, предусмотренных федеральными законами;

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

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

7) обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-розыскной деятельности, об исполнительном производстве и с уголовно-исполнительным законодательством Российской Федерации;

7.1) обработка полученных в установленных законодательством Российской Федерации случаях персональных данных осуществляется органами прокуратуры в связи с осуществлением ими прокурорского надзора;

8) обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством;

9) обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о гражданстве Российской Федерации.

Обработка специальных категорий персональных данных, осуществлявшаяся в указанных случаях, должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась обработка.

3.8. Согласие работника не требуется в следующих случаях:

1) обработка персональных данных осуществляется на основании Трудового кодекса Российской Федерации или иного федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия работодателя;

2) обработка персональных данных осуществляется в целях исполнения трудового договора;

3) обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных

данных;

4) персональные данные относятся к состоянию здоровья работника и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия работника невозможно;

5) по требованию полномочных государственных органов в случаях, предусмотренных федеральным законом.

3.9. Согласие на обработку персональных данных, разрешенных работником для распространения, оформляется отдельно от иных согласий работника на обработку его персональных данных.

3.10. Предоставление биометрических персональных данных не может быть обязательным, за исключением случаев, предусмотренных федеральными законами.

4. ПОРЯДОК ХРАНЕНИЯ И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. В соответствии со ст. 86, гл. 14 Трудового кодекса Российской Федерации в целях обеспечения прав и свобод человека и гражданина директор Учреждения (далее – работодатель) и его представители при обработке персональных данных работника должны соблюдать следующие общие требования:

4.1.1. При определении объема и содержания обрабатываемых персональных данных работодатель должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом Российской Федерации и иными федеральными законами.

4.1.2. При принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения.

4.1.3. Защита персональных данных работника от неправомерного их использования или утраты обеспечивается работодателем за счет его средств в порядке, установленном федеральным законом.

4.1.4. Работники и их представители должны быть ознакомлены под расписку с документами Учреждения, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

4.1.5. Во всех случаях отказ работника от своих прав на сохранение и защиту тайны недействителен. Персональные данные работника хранятся после автоматизированной обработки на электронном и бумажном носителях в личном деле работника.

4.2. Персональные данные на бумажном носителе хранятся в отделе кадров, финансово-экономическом отделе, отделе бухгалтерского учета и отчетности и в архиве.

4.3. Персональные данные на электронных носителях хранятся на компьютерах специалистов отдела кадров, а также в программах автоматизации бухгалтерского и налогового учета, доступ к которым имеют директор Учреждения работники бухгалтерии и отдела кадров. Вход в программу осуществляется только

при введении личного пароля пользователя.

4.4. Персональные данные работников вносятся в Единую государственную информационную систему учета научно-исследовательских, опытно-конструкторских и технологических работ гражданского назначения (далее – ЕГИСУ НИОКТР). Доступ к ЕГИСУ НОКТР имеют директор Учреждения, ученый секретарь, начальник отдела организации и координации научной деятельности, заведующий сектором патентных исследований. Вход в ЕГИСУ НИОКТР осуществляется только при введении личного пароля пользователя.

4.4.1. Персональные данные работников вносятся в систему экспертиз ФГБНУ «Дирекция научно-технических программ» (далее – система экспертиз). Доступ к системе экспертиз имеют заместитель директора Учреждения по научно-организационной работе, ученый секретарь, начальник отдела организации и координации научной деятельности. Вход в систему экспертиз осуществляется только при введении личного пароля пользователя.

4.4.2. Персональные данные работников вносятся в электронном виде при подаче заявок на изобретение/полезную модель, регистрацию программы для ЭВМ или базы данных через личный кабинет в Федеральное государственное бюджетное учреждение «Федеральный институт промышленной собственности» (далее – ФИПС). Доступ к ФИПС имеет заведующий сектором патентных исследований. Вход в личный кабинет ФИПС осуществляется только при введении личного пароля пользователя.

4.5. При поступлении лица на обучение в Учреждение формируется личное дело, которое хранится в отделе образования на бумажном и электронном носителях.

4.6. Иные профильные подразделения Учреждения, созданные в Учреждении комиссии обрабатывают и хранят документы и информацию, содержащие персональные данные, относящиеся к сфере их деятельности.

4.7. Допуск к персональным данным работника разрешен только тем должностным лицам, которым персональные данные необходимы в трудовой деятельности согласно Списку специально уполномоченных лиц (приложение к настоящему Положению).

Право доступа к персональным данным работников имеют:

- директор Учреждения;
- заместители директора Учреждения;
- ученый секретарь Учреждения;
- работники отдела кадров;
- работники бухгалтерии;
- начальник отдела экономической безопасности (информация о фактическом месте проживания и контактные телефоны работников);
- работники секретариата (информация о фактическом месте проживания и контактные телефоны работников);
- начальник отдела внутреннего контроля (доступ к персональным данным работников в ходе плановых проверок);
- начальник отдела организации и координации научной деятельности (анкета; дата рождения; образование; специальность; ученая степень; ученое звание; занимаемая должность; ИНН; СНИЛС);
- руководители структурных подразделений по направлению деятельности (доступ к персональным данным только работников своего подразделения);

- председатель первичной профсоюзной организации (паспортные данные, ИНН, СНИЛС, свидетельства о рождении детей, сведения о взносах, перечисленных в Федерацию профсоюзов);

- председатель и члены жилищной комиссии (персональные данные, содержащиеся в документах, представляемых работниками на рассмотрение жилищной комиссии).

4.8. Допуск к документам, содержащим персональные работников, внутри Учреждения осуществляется на основании Регламента допуска работников к обработке персональных данных.

4.9. От работников, ответственных за хранение персональных данных, а также работников, владеющих персональными данными в силу своих должностных обязанностей, берутся обязательства о неразглашении конфиденциальной информации о персональных данных работников.

4.10. Внешний доступ к персональным данным работников имеют контрольно-надзорные органы при наличии документов, на основании которых они проводят проверку. Дистанционно персональные данные работников могут быть представлены контрольно-надзорным органам только по письменному запросу. Другие организации, а также родственники и члены семьи работника не имеют доступа к персональным данным работника, за исключением наличия письменного согласия самого работника.

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

4.12. Автоматизированная обработка и хранение персональных данных работников допускаются только после выполнения всех основных мероприятий по защите информации.

4.13. Помещения, в которых хранятся персональные данные работников, должны быть оборудованы надежными замками и системой сигнализации.

5. ПРАВИЛА ПЕРЕДАЧИ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ

5.1. Передача персональных данных по запросам третьих лиц, если такая передача прямо не предусмотрена законодательством Российской Федерации, допускается исключительно с согласия работника на обработку его персональных данных в части их предоставления или согласия на распространение персональных данных.

5.2. Передача информации, содержащей сведения о персональных данных работников, по телефону в связи с невозможностью идентификации лица, запрашивающего информацию, запрещается.

5.3. При передаче персональных данных работника Работодатель должен соблюдать следующие требования:

5.3.1. 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 случаях, установленных федеральным законом.

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

5.3.3. Предупредить лиц, получивших 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, получившие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное Положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами.

5.3.4. Осуществлять передачу персональных данных работников в пределах Учреждения в соответствии с настоящим Положением.

5.3.5. 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 конкретной функции.

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

При получении персональных данных не от работника (за исключением случаев, если персональные данные были предоставлены работодателю на основании федерального закона или если персональные данные являются общедоступными) работодатель до начала обработки таких персональных данных обязан предоставить работнику следующую информацию:

- наименование (фамилия, имя, отчество) и адрес оператора или его представителя;
- цель обработки персональных данных и ее правовое основание;
- предполагаемые пользователи персональных данных;
- установленные федеральным законом права субъекта персональных данных.

5.4. В случае необходимости взаимодействия с третьими лицами в рамках достижения целей обработки персональных данных в адрес третьих лиц, в том числе находящихся за пределами Российской Федерации (трансграничная передача), необходимо указывать условия передачи персональных данных, в том числе указать конкретное наименование и местонахождение соответствующих третьих лиц, цели осуществляемой (трансграничной) передачи, объем передаваемых персональных данных, перечень действий по их обработке, способы и иные условия обработки, включая требования к защите обрабатываемых персональных данных.

5.5. Трансграничная передача персональных данных на территории иностранных государств осуществляется в соответствии с Федеральным законом «О защите персональных данных» и может быть запрещена или ограничена в целях защиты основ конституционного строя Российской Федерации, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороны страны и безопасности государства.

6. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Учреждение при обработке персональных данных принимает необходимые правовые, организационные и технические меры или обеспечивает их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

6.2. Обеспечение безопасности персональных данных достигается, в частности:

1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;

3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

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

5) учетом машинных носителей персональных данных;

6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них;

7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

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

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

6.3. Работодатель принимает следующие меры по защите персональных данных:

6.3.1. Назначение лица, ответственного за обработку персональных данных, которую осуществляет Учреждение, обучение и инструктаж, внутренний контроль за соблюдением работниками требований к защите персональных данных. Лицо, ответственное за организацию обработки персональных данных, получает указания непосредственно от директора Учреждения и подотчетно ему.

6.3.2. Учреждение обязано предоставлять лицу, ответственному за организацию обработки персональных данных, сведения, указанные в части 3 статьи 22 Федерального закона «О персональных данных».

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

1) осуществлять внутренний контроль за соблюдением работниками законодательства Российской Федерации о персональных данных, в том числе

требований к защите персональных данных;

2) доводить до сведения работников 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.

6.3.3. Разработка политики в отношении обработки персональных данных.

6.3.4. Установление правил доступа к персональным данным, обеспечение регистрации и учета всех действий, совершаемых с персональными данными.

6.3.5. Установление индивидуальных паролей доступа работников в информационную систему в соответствии с их производственными обязанностями.

6.3.6. Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации.

6.3.7. Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами.

6.3.8. Соблюдение условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный к ним доступ.

6.3.9. Обнаружение фактов несанкционированного доступа к персональным данным.

6.3.10. Восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

6.3.11. Обучение работников, непосредственно осуществляющих обработку персональных данных, положениям законодательства Российской Федерации о персональных данных, в том числе требованиям к защите персональных данных, документам, определяющим политику работодателя в отношении обработки персональных данных, локальным нормативным актам по вопросам обработки персональных данных.

6.3.12. Осуществление внутреннего контроля и аудита.

6.3.13. Определение типа угроз безопасности и уровней защищенности персональных данных, которые хранятся в информационных системах.

6.4. Угрозы защищенности персональных данных.

6.4.1. Угрозы первого типа. Угрозы 1-го типа актуальны для информационной системы, если для нее, в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

6.4.2. Угрозы второго типа. Угрозы 2-го типа актуальны для информационной системы, если для нее, в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

6.4.3. Угрозы третьего типа. Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

6.5. Уровни защищенности персональных данных.

6.5.1. 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.

6.5.2. 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.

6.5.3. 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.

6.5.4. 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.

6.5.5. Для обеспечения 4-го уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

а) организация 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;

б) обеспечение сохранности носителей персональных данных;

в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

6.5.6. Для обеспечения 3-го уровня защищенности персональных данных при их обработке в информационных системах необходимо, чтобы было назначено должностное лицо (работник), ответственный за обеспечение безопасности персональных данных в информационной системе.

6.5.7. Для обеспечения 2-го уровня защищенности персональных данных при их обработке в информационных системах необходимо, чтобы доступ к содержанию электронного журнала сообщений был возможен исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.

6.5.8. Для обеспечения 1-го уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований: