Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Шадринский государственный педагогический университет»

ПОЛОЖЕНИЕ
ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ, ОБУЧАЮЩИХСЯ И АБИТУРИЕНТОВ ШАДРИНСКОГО УНИВЕРСИТЕТА

(новая редакция)

Шадринск, 2017

1. Общие положения

1.1. Настоящее положение «Положение по обработке и защите персональных данных работников, обучающихся и абитуриентов Шадринского университета (далее по тексту – «Положение») разработано на основании Конституции Российской Федерации, Трудового кодекса РФ, Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», других действующих нормативно-правовых актов Российской Федерации.

1.2. Положение устанавливает порядок получения, учета, обработки, накопления и хранения документов, содержащих сведения, отнесенные к персональным данным работников и обучающихся Федерального государственного бюджетного образовательного учреждения высшего образования «Шадринский государственный педагогический университет» (далее по тексту – «ШГПУ»).

1.3. Цели и задачи Положения.

Целями настоящего Положения являются:

- обеспечение соответствия законодательству Российской Федерации действий работников ШГПУ, направленных на обработку персональных данных работников, обучающихся, третьих лиц (других граждан);
- обеспечение защиты персональных данных от несанкционированного доступа, утраты, неправомерного их использования или распространения.

Задачами настоящего Положения являются:

- определение принципов, порядка обработки персональных данных;
- определение условий обработки персональных данных, способов защиты персональных данных;
- определение прав и обязанностей ШГПУ и субъектов персональных данных при обработке персональных данных

1.4. Требования настоящего Положения распространяются на всех работников, обучающихся и абитуриентов ШГПУ.

1.5. В настоящем Положении используются следующие понятия и термины:

работник - физическое лицо, вступившее в трудовые отношения с работодателем;

работодатель - ШГПУ;

обучающиеся - студенты, магистранты, аспиранты, слушатели, соискатели, абитуриенты, выпускники ШГПУ;

субъекты персональных данных - работники и обучающиеся ШГПУ, третьи лица;

персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, необходимая ШГПУ в связи с трудовыми отношениями и организацией образовательного процесса;

оператор - ШГПУ и должностные лица ШГПУ, организующие и (или) осуществляющие обработку персональных данных;

обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), защиту, использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;

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 оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающие

права и свободы субъекта персональных данных или других лиц;

блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;

уничтожение персональных данных - действия, в результате которых невозможно 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 определить принадлежность персональных данных конкретному субъекту персональных данных;

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

информационно-телекоммуникационная сеть - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

конфиденциальность персональных данных - обязательное для соблюдения должностным лицом ШГПУ, иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания;

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;

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

доступ к информации - возможность получения информации, и ее использования.

2. Понятие и состав персональных данных

2.1. Под персональными данными работников и обучающихся понимается любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных).

2.1.1. Персональные данные включают в себя: фамилию, имя, отчество, пол, дату рождения, место рождения, гражданство, документ удостоверяющий личность (серия, номер, дата выдачи паспорта, наименование органа, выдавшего паспорт, код подразделения), адрес регистрации/почтовый/места проживания, адрес электронной почты, номер телефона, данные по наличию образования в том числе: наличие диплома, профессиональной переподготовке, повышении квалификации, стажировки, присвоении ученой степени, ученого звания (если таковые имеются), аттестата их серия, номер, наименование органа или учреждения выдавшего, дата выдачи, регистрационный номер, специальность, квалификацию, данные документа воинского учета, анкетные данные, предоставленные при поступлении на работу или в процессе работы (в том числе - автобиография, сведения о семейном положении работника, перемене фамилии, наличии детей и иждивенцев), данные по стажу работы, сведения о предыдущих местах работы (службы), сведения о социальных льготах, доходах, должности, подразделении, табельный номер, оклад, доплаты и надбавки, наличии судимостей, сведения о госнаградах, поощрениях, взысканиях, подлинниках и копиях приказов по личному составу, реквизиты трудового договора, реквизиты трудовой книжки, реквизиты водительского удостоверения, реквизиты медицинских справок, результаты медицинских обследований, реквизиты медицинского полиса, номер лицевого счёта в банке,

реквизиты удостоверения сотрудника ШГПУ, реквизиты пропуска сотрудника, ШГПУ, рекомендации и характеристики направление подготовки, профиль обучения, форма обучения, квоту (при наличии), форму обучения, результаты Единого государственного Экзамена (ЕГЭ), результаты вступительных испытаний, проводимых ШГПУ самостоятельно, наименование (год окончания) образовательного учреждения, дающего право на прохождение обучения в высшем образовательном учреждении, серию, номер, регистрационный номер, дату выдачи, наименование учреждения выдавшего аттестат/диплом, страховых свидетельствах государственного пенсионного и медицинского страховании, ИНН, результаты медицинского обследования, сведения о льготах, изображение лица (фотографию), данные отпечатков пальцев, сведения о воинском учете, данные по успеваемости и выполнению учебного плана, данные о договоре (дополнения к нему) на получение образовательных услуг, данные по выданным документам о полученном в ШГПУ образовании, данные о трудоустройстве, сведения о поощрениях и наложенных дисциплинарных взысканиях, результаты посещения научной библиотеки ШГПУ, администрирование и контроль трафика сети Интернет, номер лицевого счёта в банке, номер читательского билета, номер студенческого билета, номер зачетной книжки, номер пропуска в общежитие (при наличии), личную подпись.

2.1.2. Субъектами персональных данных в ШГПУ являются:

- работники, состоящие с ШГПУ в трудовых отношениях, в том числе работающие в ШГПУ по совместительству и на условиях почасовой оплаты;

- все категории обучающихся (студенты всех форм обучения, аспиранты, соискатели, слушатели курсов повышения квалификации и дополнительных образовательных программ, выпускники всех форм и видов обучения);

- абитуриенты, подавшие заявления о поступлении в ШГПУ;

- близкие родственники работников ШГПУ;

- физические лица, участвующие в проводимых ШГПУ конкурсах, олимпиадах, спартакиадах;

- законных представителей несовершеннолетних обучающихся, абитуриентов и посетителей ШГПУ;

- прочие физические лица, состоящие с ШГПУ в договорных отношениях.

2.1.3. Информация о персональных данных может содержаться:

- на бумажных носителях;
- на электронных носителях;
- в информационно-телекоммуникационных сетях и иных информационных системах. Локальная информационная система ШГПУ

2.1.4. ШГПУ использует следующие способы обработки персональных данных:

- автоматизированная обработка;
- без использования средств автоматизации;
- смешанная обработка (с применением объектов вычислительной техники).

2.2. Обработка персональных данных - действия (операции), включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

ШГПУ, как оператор, осуществляет следующие действия с персональными данными:

- сбор с целью отражения их в документах, указных в пункте 2.2.1, 2.2.3. настоящего положения;

- систематизацию с целью повышения эффективности качества оказания образовательных услуг, и соблюдения трудового законодательства;

- накопление, хранение с целью соблюдения требований законодательства РФ об архивном делопроизводстве;

- уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение с целью оказания

и выполнения должного уровня услуг, обязанностей в области образовательного, трудового законодательства и иных нормативных актов».

2.2.1. Персональные данные работников ШГПУ содержатся в следующих документах (копиях указанных документов):

- заявления работников (о принятии на работу, об увольнении и т.п.);
- паспорт (или иной документ, удостоверяющий личность);
- трудовая книжка;
- страховое свидетельство государственного пенсионного страхования;
- свидетельство о постановке на учёт в налоговый орган и присвоении ИНН;
- документы воинского учёта;
- документы об образовании, о квалификации или наличии специальных знаний, специальной подготовки;
- заполненная унифицированная форма Т2 «Личная карточка работника»;
- заполненная унифицированная форма Т4 «Учетная карточка научного, научно-педагогического работника»;
- автобиография;
- личный листок по учёту кадров;
- медицинское заключение о состоянии здоровья, индивидуальная программа реабилитации, медицинская справка о прохождении медицинских осмотров;
- документы, содержащие сведения об оплате труда;
- другие документы,содержащие персональные данные и предназначенные для использования в служебных целях.

2.2.2. Обработка персональных данных работников осуществляется в целях обеспечения соблюдения Конституции Российской Федерации, федеральных законов и иных нормативных правовых актов Российской Федерации, содействия работникам в исполнении должностных обязанностей, повышении квалификации и

должностном росте, обеспечения личной безопасности при исполнении должностных обязанностей, учета результатов исполнения должностных обязанностей, обеспечения социальными льготами в соответствии с законодательством и нормативными документами ШГПУ.

2.2.3. Персональные данные обучающихся в ШГПУ могут содержаться в следующих документах (копиях указанных документов):

- личное дело обучающегося;
- личное дело абитуриента;
- заявления абитуриента (о допуске к участию в конкурсе для поступления в ШГПУ и др.);
- заявления обучающихся (в том числе о восстановлении, отчислении; о сдаче академической задолженности, о перезачете (переаттестации) дисциплины, о предоставлении академического отпуска и т.п.);
- личная карточка обучающегося;
- учебная карточка обучающегося;
- договор об обучении с оплатой его стоимости;
- справки (в том числе справки об оплате по договору);
- списки лиц, зачисленных в ШГПУ;
- паспорт или иной документ, удостоверяющий личность;
- страховое свидетельство государственного пенсионного страхования;
- документы воинского учёта;
- документы об образовании, о квалификации или наличии специальных знаний, специальной подготовки (аттестат о среднем (полном) общем образовании с приложением, свидетельство о результатах единого государственного экзамена, дипломы, свидетельства и т.п.);
- медицинские документы, содержащие сведения о состоянии здоровья обучающегося (медицинская справка, врачебно-консультативное заключение, протоколы заседания ВКК, пр.);

- экзаменационные листы, зачетные книжки;
- справки об установлении инвалидности; индивидуальная программа реабилитации инвалида;
- документы, содержащие сведения о стипендии, материальной помощи и иных выплатах;
- документы, подтверждающие право на льготный порядок поступления в ШГПУ (свидетельства о смерти родителей, постановление главы города (распоряжение администрации) об установлении опеки, попечительства над несовершеннолетним, свидетельство о рождении, ходатайства отдела опеки и попечительства, департамента семьи, опеки и попечительства о содействии в поступлении в ШГПУ на имя ректора; решения суда о лишении родительских прав и взыскании алиментов; справки об установлении инвалидности, индивидуальная программа реабилитации лица и т.п.);
- документы, подтверждающие целевое направление лица на обучение;
- приказы по студентам, выписки из приказов;
- другие документы, содержащие персональные данные и предназначенные для использования в целях организации образовательного процесса.

2.2.4. Обработка персональных данных всех категорий обучающихся осуществляется в целях обеспечения соблюдения Конституции Российской Федерации, федеральных законов и иных нормативных правовых актов Российской Федерации, содействия в освоении образовательных программ, учета выполнения учебного плана и качества полученных знаний, содействия трудоустройству, обеспечения личной безопасности в период обучения, обеспечения социальными льготами в соответствии с законодательством и нормативными документами ШГПУ.

2.2.5. Обработка персональных данных абитуриентов осуществляется в целях обеспечения соблюдения Конституции Российской Федерации, федеральных законов и иных нормативных правовых актов Российской Федерации, содействия в

оптимальном выборе образовательных программ, обеспечения соблюдения правил приема в соответствии с законодательством и нормативными документами ШГПУ, гласности и открытости деятельности приемной комиссии.

Состав персональных данных, обрабатываемых по указанным категориям субъектов (работники, абитуриенты, обучающиеся) приведены в приложениях 1-3. Данные сведения являются конфиденциальными. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении срока хранения, если иное не определено законом.

2.2. 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.

2.3. Использование персональных данных - действия (операции) с персональными данными, совершаемые в ШГПУ в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении работника (обучающегося) или других лиц либо иным образом затрагивающих права и свободы работника (обучающегося) или других лиц.

2.4. Блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

2.5. Уничтожение персональных данных действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

2.6. Обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному работнику или обучающемуся.

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

2.8. Конфиденциальность персональных данных - обязательное для соблюдения сотрудником ШГПУ или иными получившим доступ к персональным данным лицом требование не допускать их распространения без согласия работника (обучающегося) или наличия иного законного основания. Обеспечения конфиденциальности персональных данных не требуется:

- в случае обезличивания персональных данных;
- в отношении общедоступных персональных данных.
- при трансграничной передаче персональных данных - передаче персональных данных ШГПУ через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.
- при использовании общедоступных персональных данных - данных, доступ неограниченного круга лиц к которым предоставлен с согласия работника (обучающегося) или на которые в соответствии с федеральными законами не распространяется требование соблюдение конфиденциальности.

В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия работника (обучающегося) могут включаться его фамилия, имя, отчество, год и место рождения, адрес проживания и пребывания, абонентский номер телефона коммуникационных услуг, сведения о профессии и иные персональные данные, предоставленные работником или обучающимся.

Сведения о работнике или об обучающемся могут быть в любое время исключены из общедоступных источников персональных данных по требованию

работника (обучающегося), либо по решению суда или иных уполномоченных государственных органов.

3. Обязанности Шадринского университета

3.1. Обработка персональных данных работника или обучающегося может осуществляться исключительно в целях обеспечения соблюдения закона и иных нормативных правовых актов, содействия в трудоустройстве, обучении и продвижении по службе, обеспечении личной безопасности, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

3.2. При определении объема и содержания обрабатываемых персональных данных работника или обучающегося ШГПУ должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом РФ, ФЗ «О персональных данных» и иными федеральными законами.

3.3. ШГПУ должен сообщить работнику или обучающемуся о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника или обучающегося дать письменное согласие на их получение.

3.4. Согласия работника или обучающегося не требуется в следующих случаях:

- обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является работник или обучающийся;
- обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов работника или обучающегося, если получение согласия работника (обучающегося) невозможно;
- обработка персональных данных необходима для доставки почтовых отправлений организациями почтовой связи, для осуществления операторами

электросвязи расчетов с пользователями услуг связи за оказанные услуги связи, а также для рассмотрения претензий пользователей услугами связи;

• обработка персональных данных осуществляется в целях научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и свободы работника или обучающегося;

• обработка персональных данных осуществляется в целях обеспечения развития и нормального функционирования ШГПУ, при этом из обрабатываемых персональных данных должны быть исключены паспортные данные, данные о месте рождения, проживания, семейном, социальном, имущественном положении, доходах и другая информация, которая при несанкционированном доступе к ней может принести материальный и/или моральный вред работнику или обучающемуся.

3.5. В случае, если ШГПУ на основании договора поручает обработку персональных данных другому лицу, существенным условием договора является обязанность обеспечения указанным лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке.

3.6. Если персональные данные были получены не от работника или обучающегося, за исключением случаев, если персональные данные были предоставлены ШГПУ на основании Федерального закона или, если персональные данные являются общедоступными, ШГПУ до начала обработки таких персональных данных обязан предоставить работнику (обучающемуся) следующую информацию:

1) наименование (фамилия, имя, отчество) и адрес представителя ШГПУ;

2) цель обработки персональных данных и ее правовое основание;

3) предполагаемые пользователи персональных данных;

4) установленные Федеральным законом № 152-ФЗ от 27 июля 2006г. «О персональных данных» права работника или обучающегося.

3.7. Меры по обеспечению безопасности персональных данных при их обработке:

• ШГПУ при обработке персональных данных обязан принимать необходимые организационные и технические меры, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

• Правительство Российской Федерации устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

3.8. Обязанности ШГПУ при обращении либо при получении запроса работника (обучающегося) или его законного представителя, а также уполномоченного органа по защите прав субъектов персональных данных:

• ШГПУ обязан в порядке, предусмотренном статьей 14 Федерального закона № 152 - ФЗ от 27 июля 2006г. «О персональных данных», сообщить работнику (обучающемуся) или его законному представителю информацию о наличии персональных данных, относящихся к соответствующему работнику (обучающемуся), а также предоставить возможность ознакомления с ними при обращении работника (обучающегося) или его законного представителя либо в течение десяти рабочих дней с даты получения запроса.

• ШГПУ обязан безвозмездно предоставить работнику (обучающемуся) или его законному представителю возможность ознакомления с персональными данными, относящимися к работнику (обучающемуся), а также внести в них необходимые изменения, уничтожить или блокировать соответствующие персональные данные по предоставлении работником (обучающимся) или его законным представителем сведений, подтверждающих, что персональные данные, которые относятся к работнику (обучающемуся) и обработку которых осуществляет ШГПУ, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О

внесенных изменениях и предпринятых мерах ШГПУ обязан уведомить работника (обучающегося) или его законного представителя и третьих лиц, которым персональные данные этого субъекта были переданы.

• ШГПУ обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по его запросу информацию, необходимую для осуществления деятельности указанного органа, в течение семи рабочих дней с даты получения такого запроса.

3.9. Обязанности ШГПУ по устранению нарушений законодательства, допущенных при обработке персональных данных, а также по уточнению, блокированию и уничтожению персональных данных:

• В случае выявления недостоверных персональных данных работника (обучающегося) или неправомерных действий с ними ШГПУ, при обращении или по запросу субъекта, работника (обучающегося) или его законного представителя, либо уполномоченного органа по защите прав персональных данных субъекта ШГПУ обязан осуществить блокирование персональных данных, относящихся к работнику или обучающемуся, с момента такого обращения или получения такого запроса на период проверки.

• В случае подтверждения факта недостоверности персональных данных ШГПУ на основании документов, представленных работником (обучающимся) или его законным представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные и снять их блокирование.

• В случае выявления неправомерных действий с персональными данными ШГПУ в срок, не превышающий трех рабочих дней с даты такого выявления, обязан устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, обязан уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных ШГПУ обязан уведомить работника

(обучающегося) или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, - также указанный орган.

• В случае достижения цели обработки персональных данных ШГПУ обязан незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий трех рабочих дней с даты достижения цели обработки персональных данных, если иное не предусмотрено федеральными законами, и уведомить об этом работника (обучающегося) или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, - также указанный орган.

• В случае отзыва работником или обучающимся согласия на обработку своих персональных данных ШГПУ обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между ШГПУ и работником (обучающимся). Об уничтожении персональных данных ШГПУ обязан уведомить работника (обучающегося).

3.10. Уведомление об обработке персональных данных.

3.10.1. ШГПУ до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных, за исключением случаев, предусмотренных п.3.10.2.

3.10.2. ШГПУ вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных:

1) относящихся к субъектам персональных данных, которых связывают с оператором трудовые отношения;

2) полученных ШГПУ в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не

распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;

3) относящихся к членам (участникам) общественного объединения или религиозной организации и обрабатываемых соответствующим общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов персональных данных;

4) являющихся общедоступными персональными данными;

5) включающих в себя только фамилии, имена и отчества субъектов персональных данных;

6) необходимых в целях однократного пропуска субъекта персональных данных на территорию, на которой находится ШГПУ, или в иных аналогичных целях;

7) включенных в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус федеральных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;

8) обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных.

3.11. Уведомление должно быть направлено в письменной форме и подписано уполномоченным лицом или направлено в электронной форме и

подписано электронной цифровой подписью в соответствии с законодательством Российской Федерации. Уведомление должно содержать следующие сведения:

1) адрес ШГПУ;
2) цель обработки персональных данных;
3) категории персональных данных;
4) категории субъектов, персональные данные которых обрабатываются;
5) правовое основание обработки персональных данных;
6) перечень действий с персональными данными, общее описание используемых ШГПУ способов обработки персональных данных;
7) описание мер, которые ШГПУ обязуется осуществлять при обработке персональных данных, по обеспечению безопасности персональных данных при их обработке;
8) дата начала обработки персональных данных;
9) срок или условие прекращения обработки персональных данных.

3.12. ШГПУ не имеет права получать и обрабатывать персональные работника или обучающегося о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции РФ ШГПУ вправе получать и обрабатывать данные о частной жизни работника или обучающегося только с его письменного согласия.

3.13. ШГПУ не имеет права получать и обрабатывать персональные данные работника (обучающегося) о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных законом.

3.14. При принятии решений, затрагивающих интересы работника или обучающегося, ШГПУ не имеет права основываться на персональных данных работника (обучающегося), полученных исключительно в результате их автоматизированной обработки или электронного получения.

3.15. Защита персональных данных работника или обучающегося от неправомерного их использования или утраты должна быть обеспечена ШГПУ за

счет его средств.

3.16. Работники и обучающиеся и их представители должны быть ознакомлены под подпись с документами ШГПУ, устанавливающими порядок обработки персональных данных работников и обучающихся, а также об их правах и обязанностях в этой области.

4. Обязанности и права работника или обучающегося

4.1. Работник (обучающийся) обязан:

• передавать ШГПУ комплекс достоверных документированных персональных данных, перечень которых установлен Трудовым кодексом РФ;

• своевременно в срок, не превышающий одного месяца, сообщать ШГПУ об изменении своих персональных данных.

4.2. Работник (обучающийся) имеет право:

• на полную информацию о своих персональных данных и обработке этих данных;

• на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей его персональные данные, за исключением случаев, предусмотренных законодательством РФ;

• на доступ к медицинским данным;

• требовать исключения, исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением требований закона, их блокирования, уничтожения;

• дополнить заявлением, выражающим его собственное мнение, персональные данные оценочного характера;

• обжаловать неправомерные действия ШГПУ при обработке и защите персональных данных.

4.3. Доступ к своим персональным данным предоставляется работнику (обучающемуся) или его законному представителю ШГПУ при обращении либо получении запроса работника (обучающегося) или его законного представителя.

Запрос должен содержать номер основного документа, удостоверяющего личность работника (обучающегося) или его законного представителя, сведения о дате выдаче указанного документа и выдавшем его органе и собственноручную подпись работника (обучающегося) или его законного представителя. Запрос может быть направлен в электронной форме и подписан электронной цифровой подписью в соответствии с законодательством Российской Федерации.

4.4. Работник или обучающийся имеет право на получение при обращении или при получении запроса информации, касающейся обработки его персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных в ШГПУ, а также цель такой обработки;

2) способы обработки персональных данных, применяемые в ШГПУ;

3) сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;

4) перечень обрабатываемых персональных данных и источник их получения;

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

6) сведения о том, какие юридические последствия для работника (обучающегося) может повлечь за собой обработка его персональных данных.

4.5. Право работника или обучающегося на доступ к своим персональным данным ограничивается в случае, если:

1) обработка персональных данных, в том числе персональных данных, полученных в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

2) обработка персональных данных осуществляется органами, осуществившими задержание работника или обучающегося по подозрению в совершении преступления, либо предъявившими работнику (обучающемуся) обвинение по уголовному делу, либо применившими к работнику (обучающемуся)

меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

3) предоставление персональных данных нарушает конституционные права и свободы других лиц.

4.6. Права при обработке их персональных данных в целях продвижения товаров, работ, услуг на рынке.

4.6.1 Обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи допускается только при условии предварительного согласия работника (обучающегося).

4.6.2. ШГПУ обязан немедленно прекратить по требованию работника (обучающегося) обработку его персональных данных, указанную в п.4.6.1.

4.7. Права работника (обучающегося) при принятии решений на основании исключительно автоматизированной обработки их персональных данных. Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении работника (обучающегося) или иным образом затрагивающих его права и законные интересы, за исключением случаев:

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

4.8. ШГПУ обязан разъяснить работнику или обучающемуся порядок принятия решения на основании исключительно автоматизированной обработки его

персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты работником (обучающимся) своих прав и законных интересов.

4.9. ШГПУ обязан рассмотреть возражение, указанное в п.4.8. в течение семи рабочих дней со дня его получения и уведомить работника или обучающегося о результатах рассмотрения такого возражения.

5. Сбор, обработка и хранение персональных данных

5.1. Всю информацию о персональных данных работник (обучающийся) предоставляет самостоятельно.

5.2. Если персональные данные работника (обучающегося) возможно получить только у третьей стороны, то работник (обучающийся) должен быть уведомлен об этом заранее и от него должно получено письменное согласие (Приложения № № 1 - 4). Письменное согласие работника (обучающегося) на обработку своих персональных данных включает:

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

2) сведения о ШГПУ;

3) цель обработки персональных данных;

4) перечень персональных данных, на обработку которых дается согласие работника (обучающегося);

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

6) срок, в течение которого действует согласие, а также порядок его отзыва.

5.3. В случае недееспособности работника (обучающегося) согласие на обработку его персональных данных в письменной форме дает его законный

представитель.

5.4. В случае смерти работника (обучающегося) согласие на обработку его персональных данных дают в письменной форме наследники работника или родственники, если такое согласие не было дано работником (обучающимся) при его жизни.

5.5. ШГПУ должен сообщать работнику (обучающемуся) о последствиях отказа работника (обучающегося) дать письменное согласие на их получение.

5.6. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением если:

• работник (обучающийся) дал согласие в письменной форме на обработку своих персональных данных;

• персональные данные являются общедоступными;

• персональные данные относятся к состоянию здоровья работника (обучающегося) 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 (обучающегося) невозможно;

• обработка персональных данных необходима для осуществления правосудия;

• обработка персональных данных осуществляется в соответствии с законодательством РФ о безопасности, об оперативно-розыскной деятельности, а также в соответствии с уголовно-исполнительным законодательством РФ.

5.7. Обработка специальных категорий персональных данных должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась обработка.

5.8. Трансграничная передача персональных данных.

5.8.1. До начала осуществления трансграничной передачи персональных

данных ШГПУ обязан убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав работника или обучающегося.

5.8.2. Трансграничная передача персональных данных на территории иностранных государств, обеспечивающих адекватную защиту работника (обучающегося), осуществляется в соответствии с ФЗ «О 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.

5.8.3. Трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты работника (обучающегося), может осуществляться в случаях:

1) наличия согласия в письменной форме работника (обучающегося);

2) предусмотренных международными договорами Российской Федерации по вопросам выдачи виз, а также международными договорами Российской Федерации об оказании правовой помощи по гражданским, семейным и уголовным делам;

3) предусмотренных федеральными законами, если это необходимо в целях защиты основ конституционного строя Российской Федерации, обеспечения обороны страны и безопасности государства;

4) исполнения договора, стороной которого является работник (обучающийся);

5) защиты жизни, здоровья, иных жизненно важных интересов работника (обучающегося) или других лиц при невозможности получения согласия в письменной форме работника (обучающегося).

5.9. Работник (обучающийся) предоставляет в ШГПУ достоверные сведения о себе. ШГПУ проверяет достоверность сведений, сверяя данные предоставленные работником (обучающимся), с имеющимися у работника (обучающегося)

документами. Предоставление работником (обучающимся) подложных документов или ложных сведений при поступлении на работу является основанием для расторжения трудового договора.

5.10. При поступлении на работу или учебу работник (обучающийся) заполняет анкету и автобиографию.

5.11. Анкета представляет собой перечень вопросов о персональных данных работника (обучающегося).

5.12. Анкета заполняется работником (обучающимся) самостоятельно. При заполнении анкеты работник (обучающийся) должен заполнить все графы, на все вопросы давать полные ответы, не допускать исправлений или зачеркивании, прочерков, помарок.

5.13. Автобиография документ, содержащий описание в хронологической последовательности основных этапов жизни и деятельности работника или обучающегося.

5.14. Автобиография составляется в произвольной форме, без помарок и исправлений.

5.15. Анкета и автобиография работника (обучающегося) хранятся в личном деле работника (обучающегося), которое оформляется после издания приказа о приеме на работу или учебу.

5.16. Все документы личного дела работника (обучающегося) подшиваются в обложку образца, установленного в ШГПУ. На ней указывается фамилия, имя, отчество работника (обучающегося), номер личного дела.

5.17. Все документы, поступающие в личное дело, располагаются в хронологическом порядке. Листы документов, подшитых в личное дело, нумеруются.

5.18. Личное дело ведется на протяжении всей трудовой деятельности работника (обучающегося в период учебы). Изменения, вносимые в личное дело, должны быть подтверждены соответствующими документами.

5.19. Основная работа по обработке персональных данных возлагается на

начальника отдела кадров контроля и делопроизводства и начальника центра инновационных образовательных технологий, которые действуют на основании инструкции, предусматривающей:

• порядок защиты баз, размещенных на серверах и других электронных носителях от внешних и внутренних несанкционированных доступов;

• порядок передачи персональных данных в ШГПУ;

• порядок оформления и переоформления трудового договора и обязательства по неразглашению персональных данных работников и обучающихся. Обработка персональных данных по начислению заработной платы (стипендии) возлагается на сотрудников планово-экономического отдела и отдела бухгалтерии.

6. Передача персональных данных

6.1. При передаче персональных данных работника (обучающегося) ШГПУ должен соблюдать следующие требования:

• не сообщать персональные данные работника (обучающегося) третьей стороне без письменного согласия работника (обучающегося), за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника (обучающегося), а также в случаях, установленных федеральным законом;

• не сообщать персональные данные работника (обучающегося) в коммерческих целях без его письменного согласия;

• предупредить лиц, получающих персональные данные работника (обучающегося), о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это право соблюдено. Лица, получающие персональные данные работника (обучающегося), обязаны соблюдать конфиденциальность.

Данное Положение не распространяется на обмен персональными данными работников (обучающихся) в порядке, установленном федеральными законами;

• разрешать доступ к персональным данным работников (обучающихся) только специально уполномоченным лицам, при этом указанные лица должны иметь

право получать только те персональные данные, которые необходимы для выполнения конкретных функций;

• не запрашивать информацию о состоянии здоровья работника (обучающегося), за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции (обучающимся - учебы);

• передавать персональные данные работника представителям работников в порядке, установленном Трудовым кодексом РФ, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

7. Доступ к персональным данным работника или обучающегося

7.1. Внутренний доступ (доступ внутри ШГПУ).

Право доступа к персональным данным работника (обучающегося) имеют:

• ректор ШГПУ;

• проректоры ШГПУ;

• начальник Управления кадров;

• главный бухгалтер;

• начальник Управления по обеспечению безопасности образовательного учреждения;

• начальник планово-экономического отдела;

• ведущий юрисконсульт;

• специалист по охране труда;

• начальник отдела ГО;

• руководители структурных подразделений по направлению деятельности (доступ к личным данным только сотрудников своего подразделения) по согласованию с ректором ШГПУ (при переводе из одного структурного подразделения в другое доступ к персональным данным работника может иметь руководитель нового подразделения по согласованию с ректором ШГПУ);

• сотрудники бухгалтерии - к данным, которые необходимы им для выполнения должностных обязанностей;

• сотрудники управления кадров, осуществляющие обработку персональных данных работника (обучающегося) согласно должностных обязанностей;

• сам работник (обучающийся), носитель данных.

7.2. Внешний доступ.

К числу массовых потребителей персональных данных вне ШГПУ можно отнести государственные и негосударственные структуры:

• налоговые инспекции;

• правоохранительные органы;

• органы лицензирования и сертификации;

• органы прокуратуры и ФСБ;

• военкоматы;

• органы социального страхования;

• пенсионные фонды;

• подразделения муниципальных органов управления.

7.3. Другие организации.

Сведения о работающем работнике (об обучающемся) или уже уволенном могут быть предоставлены другой организацией только с письменного запроса на бланке организации с приложением копии заявления работника (обучающегося).

7.4. Родственники и члены семей.

Персональные данные работника (обучающегося) могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого работника (обучающегося), либо в случаях, установленных законодательством.

В случае развода, смерти бывшая супруга (супруг) имеет право обратиться в ШГПУ с письменным запросом о размере заработной платы работника без его согласия (ТК РФ).

8. Защита персональных данных работников и обучающихся

8.1. В целях обеспечения сохранности и конфиденциальности персональных данных работников (обучающихся) ШГПУ все операции по оформлению, формированию, ведению и хранению данной информации должны выполняться только работниками отдела кадров, контроля и делопроизводства, деканатов, приемной комиссии, осуществляющими данную работу в соответствии со своими служебными обязанностями, зафиксированными в их должностных инструкциях.

8.2. Ответы на письменные запросы других организаций и учреждений в пределах их компетенции и представленных полномочий даются в письменной форме на бланке ШГПУ и в том объеме, который позволяет не разглашать излишний объем персональных сведений о работниках ШГПУ.

8.3. Передача информации, содержащей сведения о персональных данных работников (обучающихся) ШГПУ, по телекоммуникационным сетям без их письменного согласия запрещается.

8.4. Внутренняя защита персональных данных

• 8.4.1. Персональные данные, содержащиеся на бумажных носителях, хранятся в запираемом шкафу или в запираемом сейфе.

• 8.4.2. Выдача ключей от сейфа (шкафа) производится руководителем структурного подразделения, в функции которого входит обработка определенных персональных данных (а на период его временного отсутствия - болезнь, отпуск и т.п. - лицом, исполняющим ее обязанности), только сотрудникам данного структурного подразделения. Сдача ключа осуществляется лично руководителю после закрытия сейфа (шкафа).

• 8.4.3. Персональные данные, содержащиеся на бумажных носителях, сдаются в архив после истечения установленного срока хранения.

• 8.4.4. Персональные данные, содержащиеся на электронных носителях информации, хранятся в памяти персональных компьютеров операторов. Доступ к указанным персональным компьютерам строго ограничен кругом лиц, ответственных за обработку персональных данных.

Информация на электронных носителях должна быть защищена паролем доступа, который подлежит смене не реже 1 (одного) раза в 6 (шесть) месяцев.

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

• определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

• разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

• проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

• установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

• обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

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

• учет лиц, допущенных к работе с персональными данными в информационной системе;

• контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

• анализ фактов 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, составление заключений по данным фактам, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

• описание системы защиты персональных данных.

8.5. Внешняя защита персональных данных

8.5.1. Помещения и территория ШГПУ охраняются, в том числе с помощью средств визуального наблюдения.

8.5.2. Персональные данные в зависимости от способа их фиксации (бумажный носитель, электронный носитель) подлежат обработке таким образом, чтобы исключить возможность ознакомления с содержанием указанной информации сторонними лицами.

9. Ответственность за разглашение информации, связанной с персональными данными работника или обучающегося

9.1. Лица, виновные в нарушении норм, регулирующих обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с федеральными законами.

9.2. Руководители структурных подразделений, в функции которых входит обработка персональных данных, несут персональную ответственность за нарушение порядка доступа работников данных структурных подразделений ШГПУ и третьих лиц к информации, содержащей персональные данные.

9.3. Должностные лица ШГПУ, обрабатывающие персональные данные, несут персональную ответственность за:

9.3.1. необеспечение конфиденциальности информации, содержащей персональные данные;

9.3.2. неправомерный отказ субъекту персональных данных в предоставлении собранных в установленном порядке персональных данных либо предоставление неполной или заведомо ложной информации.

10. Заключительные положения

10.1. В соответствии с Письмом Федерального агентства по образованию от 29 июля 2009 г. N 17-110 «Об обеспечении защиты персональных данных» в ШГПУ установлены следующие категории персональных данных (Классификация

информационных систем персональных данных осуществляется оператором в соответствии с Приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 N 55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных" в зависимости от категории обрабатываемых данных и их количества):

Категория 3 - персональные данные, позволяющие идентифицировать субъекта персональных данных;

Категория 4 - обезличенные и (или) общедоступные персональные данные.

10.2. Информационные системы персональных данных ШГПУ относятся к типовым, в которых требуется обеспечить только конфиденциальность персональных данных.

В зависимости от последствий нарушений заданной характеристики безопасности персональных данных типовой информационной системе ШГПУ присваивается класс:

класс 4 (К4) - информационные системы, для которых нарушения не приводят к негативным последствиям для субъектов персональных данных.

Приложение 1
к Положению по обработке и защите
персональных данных работников,
обучающихся и абитуриентов
Шадринского университета

СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ
РАБОТНИКА ШГПУ

Я (фамилия, имя, отчество)____,
Адрес регистрации (в том числе почтовый): _____,
Серия, номер паспорта: _____,
Дата выдачи паспорта: _____,
Орган выдавший паспорт: _____,

в соответствии со статьей 9 Федерального закона Российской Федерации от 26.07.2006 года № 152-ФЗ «О персональных данных» даю письменное согласие на обработку моих персональных данных **Федеральному государственному бюджетному образовательному учреждению высшего образования «Шадринский государственный педагогический университет» (ШГПУ, Шадринский университет) (юридический /почтовый адрес: 641870, Курганская область, г.Шадринск, ул. Карла Либкнехта, д.3)**, а именно:

фамилию, имя, отчество, пол, изображение лица (фотографию), дату рождения, место рождения, гражданство, документ удостоверяющий личность (серия, номер, дата выдачи паспорта, наименование органа, выдавшего паспорт, код подразделения), адрес регистрации/места проживания/почтовый, контактный номер телефона, данные по наличию образования в том числе: наличие диплома, профессиональной переподготовке, повышении квалификации, стажировки, присвоении ученой степени, ученого звания (если таковые имеются), аттестата их серия, номер, наименование органа или учреждения выдавшего, дата выдачи,

регистрационный номер, специальность, квалификация, форма обучения, данные страхового Свидетельства государственного пенсионного страхования, ИНН, личную подпись, данные документа воинского учета, анкетные данные, предоставленные мною при поступлении на работу или в процессе работы (в том числе - автобиография, сведения о семейном положении работника, перемене фамилии, наличии детей и иждивенцев), данные по стажу работы, сведения о предыдущих местах работы (службы), сведения о социальных льготах, доходах,

должности, подразделении, табельный номер, оклад, доплаты и надбавки, наличии судимостей, сведения о госнаградах, поощрениях, взысканиях, подлинниках и копиях приказов по личному составу, реквизиты трудового договора, реквизиты трудовой книжки, реквизиты водительского удостоверения, реквизиты медицинских справок, результаты медицинских обследований, реквизиты медицинского полиса, номер лицевого счёта в банке, реквизиты удостоверения сотрудника ШГПУ, реквизиты пропуска сотрудника, ШГПУ, рекомендации и характеристики

с целью:

- корректного документального оформления трудовых правоотношений между мною и Шадринским университетом;

- обеспечения выполнения мною должностных обязанностей (трудовой функции);

- предоставления информации в государственные органы Российской Федерации в порядке, предусмотренным действующим законодательством Российской Федерации.

Лицо, осуществляющее обработку персональных данных по поручению оператора (ШГПУ) – отсутствует.

Обработка персональных данных осуществляется как на бумажных носителях, так и с использованием средств автоматизации.

Обработка вышеуказанных персональных данных будет осуществляться путем смешанной обработки персональных данных (сбор, систематизация, накопление, хранение, уточнение (обновление, изменение использования, распространение), в том числе передача), обезличивание, блокирование, уничтожение персональных данных) в установленных федеральным законодательством случаях и формах.

Срок действия согласия на обработку персональных данных: с момента заключения мной трудового договора с Шадринским университетом или по письменному отзыву.

Данное согласие может быть отозвано в любой момент с обязательным направлением Оператору – Шадринскому университету письменного уведомления.

С момента получения уведомления об отзыве согласия на обработку персональных данных Оператор – Шадринский университет обязан прекратить обработку персональных данных, указанных в настоящем согласии, и (или) уничтожить персональные данные в течение трех дней с момента получения данного отзыва.

Обязанность уничтожения не распространяется на персональные данные, для которых нормативными правовыми актами предусмотрена обязанность их хранения, в том числе после прекращения отношений в области трудового законодательства.

Я ознакомлен с «Положением по обработке и защите персональных данных работников, обучающихся и абитуриентов Шадринского университета».

_____(подпись, расшифровка подписи и дата)

Приложение 2
к Положению по обработке и защите
персональных данных работников,
обучающихся и абитуриентов
Шадринского университета

СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ АБИТУРИЕНТА ШАДРИНСКОГОУНИВЕРСИТЕТА

Я (фамилия, имя, отчество)_____ _____,
Адрес регистрации (в том числе почтовый): _____,
Серия, номер паспорта: _____,
Дата выдачи паспорта: _____,
Орган выдавший паспорт: _____,

в соответствии со статьей 9 Федерального закона Российской Федерации от 26.07.2006 года № 152-ФЗ «О персональных данных» даю письменное согласие на обработку моих персональных данных **Федеральному государственному бюджетному образовательному учреждению высшего образования «Шадринский государственный педагогический университет» (ШГПУ, Шадринский университет) (юридический /почтовый адрес: 641870, Курганская область, г.Шадринск, ул. Карла Либкнехта, д.3)**, а именно:

фамилию, имя, отчество, пол, дату рождения, место рождения, гражданство, документ удостоверяющий личность (серия, номер, дата выдачи паспорта, наименование органа, выдавшего паспорт, код подразделения), адрес регистрации/места проживания/почтовый, адрес электронной почты, номер телефона, направление подготовки, профиль обучения, форма обучения, квоту (при наличии), форму обучения, результаты Единого государственного Экзамена (ЕГЭ), результаты вступительных испытаний, проводимых ШГПУ самостоятельно,

наименование (год окончания) образовательного учреждения, дающего право на прохождение обучения в высшем образовательном учреждении, серию, номер, регистрационный номер, дату выдачи, наименование учреждения выдавшего аттестат/диплом, страховых свидетельствах государственного пенсионного и медицинского страховании, ИНН, результаты медицинского обследования, сведения о льготах, изображение лица (фотографию), данные отпечатков пальцев, сведения о воинском учете, данные по успеваемости и выполнению учебного плана, данные о договоре (дополнения к нему) на получение образовательных услуг, данные по выданным документам о полученном в ШГПУ образовании, данные о трудоустройстве, сведения о поощрениях и наложенных дисциплинарных взысканиях, результаты посещения научной библиотеки ШГПУ, администрирование и контроль трафика сети Интернет, номер пропуска в общежитие (при наличии), личную подпись

с целью обеспечения обучения в Шадринском университете.

Обработка персональных данных осуществляется как на бумажных носителях, так и с использованием средств автоматизации.

Обработка вышеуказанных персональных данных будет осуществляться путем смешанной обработки персональных данных (сбор, систематизация, накопление, хранение, уточнение (обновление, изменение использования, распространение), в том числе передача), обезличивание, блокирование, уничтожение персональных данных) в установленных федеральным законодательством случаях и формах.

Лицо, осуществляющее обработку персональных данных по поручению оператора (ШГПУ) – отсутствует.

Я согласен(а) считать общедоступными следующие персональные данные в любых сочетаниях между собой: фамилия, имя, отчество, сведения о сдаче

вступительных испытаний, сведения о сдаче ЕГЭ (ГИА), сведения о наличии или отсутствии индивидуальных достижений, сведения о направлениях подготовки (специальности). Предоставляю университету право осуществлять с моими общедоступными персональными данными все вышеуказанные действия и применять вышеуказанные способы обработки, в том числе, раскрытие их неопределенному кругу лиц путем размещения в общедоступных источниках (официальный сайт университета в сети Интернет - http://shgpi.edu.ru/, информационные стенды, расположенные в помещениях ШГПУ).

Срок действия согласия на обработку персональных данных: на период обучения в ШГПУ или по письменному отзыву.

Данное согласие может быть отозвано в любой момент с обязательным направлением Оператору – Шадринскому университету письменного уведомления.

С момента получения уведомления об отзыве согласия на обработку персональных данных Оператор – Шадринский университет обязан прекратить обработку персональных данных, указанных в настоящем Согласии, и (или) уничтожить персональные данные в течение трех дней с момента получения данного отзыва.

Обязанность уничтожения не распространяется на персональные данные, для которых нормативными правовыми актами предусмотрена обязанность их хранения, в том числе после прекращения отношений в области образования.

Я ознакомлен с «Положением по обработке и защите персональных данных работников, обучающихся и абитуриентов Шадринского университета».

_____ (подпись, расшифровка подписи и дата)

СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ
АБИТУРИЕНТА (ПРЕДСТАВИТЕЛЬ АБИТУРИЕНТА)
В ШАДРИНСКОМ УНИВЕРСИТЕТЕ

Я (фамилия, имя, отчество)_____ _____,
Адрес регистрации (в том числе почтовый): _____,
Серия, номер паспорта: _____,
Дата выдачи паспорта:_____ _____,
Орган выдавший паспорт: _____,
Реквизиты доверенности или иного документа, подтверждающего полномочия в качестве представителя: _____,

являющийся представителем:
(фамилия, имя, отчество):_____,
Адрес регистрации (в том числе почтовый): _____,
Серия, номер паспорта: _____,
Дата выдачи паспорта: _____,
Орган выдавший паспорт: _____,

в соответствии со статьей 9 Федерального закона Российской Федерации от 26.07.2006 года № 152 -ФЗ «О персональных данных» даю письменное согласие на обработку моих (вышеуказанных) и моего _____ (*ребенка, доверителя – выбрать нужное*) персональных данных **Федеральному государственному бюджетному образовательному учреждению высшего образования «Шадринский государственный педагогический университет» (ШГПУ, Шадринский университет) (юридический /почтовый адрес: 641870, Курганская область, г.Шадринск, ул. Карла Либкнехта, д.3)**, а именно:

фамилию, имя, отчество, пол, дату рождения, место рождения, гражданство, документ удостоверяющий личность (серия, номер, дата выдачи паспорта,

наименование органа, выдавшего паспорт, код подразделения), адрес регистрации/места проживания/почтовый, адрес электронной почты, номер телефона, направление подготовки, профиль обучения, форма обучения, квоту (при наличии), форму обучения, результаты Единого государственного Экзамена (ЕГЭ), результаты вступительных испытаний, проводимых ШГПУ самостоятельно, наименование (год окончания) образовательного учреждения, дающего право на прохождение обучения в высшем образовательном учреждении, серию, номер, регистрационный номер, дату выдачи, наименование учреждения выдавшего аттестат/диплом, страховых свидетельствах государственного пенсионного и медицинского страховании, ИНН, результаты медицинского обследования, сведения о льготах, изображение лица (фотографию), данные отпечатков пальцев, сведения о воинском учете, данные по успеваемости и выполнению учебного плана, данные о договоре (дополнения к нему) на получение образовательных услуг, данные по выданным документам о полученном в ШГПУ образовании, данные о трудоустройстве, сведения о поощрениях и наложенных дисциплинарных взысканиях, результаты посещения научной библиотеки ШГПУ, администрирование и контроль трафика сети Интернет, номер пропуска в общежитие (при наличии), личную подпись

с целью обеспечения обучения в Шадринском университете.

Обработка персональных данных осуществляется как на бумажных носителях, так и с использованием средств автоматизации.

Обработка вышеуказанных персональных данных будет осуществляться путем смешанной обработки персональных данных (сбор, систематизация, накопление, хранение, уточнение (обновление, изменение использования, распространение), в том числе передача), обезличивание, блокирование, уничтожение персональных данных) в установленных федеральным законодательством случаях и формах.

Лицо, осуществляющее обработку персональных данных по поручению оператора (ШГПУ) – отсутствует.

Я согласен(а) считать общедоступными следующие персональные данные моего *(ребенка, доверителя – выбрать нужное*) (*указать фамилию, имя, отчество*): _____ в любых сочетаниях между собой: фамилия, имя, отчество, сведения о сдаче вступительных испытаний, сведения о сдаче ЕГЭ (ГИА), сведения о наличии или отсутствии индивидуальных достижений, сведения о направлениях подготовки (специальности). Предоставляю университету право осуществлять с моими общедоступными персональными данными все вышеуказанные действия и применять вышеуказанные способы обработки, в том числе, раскрытие их неопределенному кругу лиц путем размещения в общедоступных источниках (официальный сайт университета в сети Интернет - http://shgpi.edu.ru/, информационные стенды, расположенные в помещениях ШГПУ).

Срок действия согласия на обработку персональных данных: на период обучения в ШГПУ или по письменному отзыву.

Данное согласие может быть отозвано в любой момент с обязательным направлением Оператору – Шадринскому университету письменного уведомления.

С момента получения уведомления об отзыве согласия на обработку персональных данных Оператор – Шадринский университет обязан прекратить обработку персональных данных, указанных в настоящем Согласии, и (или) уничтожить персональные данные в течение трех дней с момента получения данного отзыва.

Обязанность уничтожения не распространяется на персональные данные, для которых нормативными правовыми актами предусмотрена обязанность их

хранения, в том числе после прекращения отношений в области образования.

Я ознакомлен с «Положением по обработке и защите персональных данных работников, обучающихся и абитуриентов Шадринского университета».

_____ (подпись, расшифровка подписи и дата)

Приложение 3
к Положению по обработке и защите
персональных данных работников,
обучающихся и абитуриентов
Шадринского университета

СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ
ОБУЧАЮЩЕГОСЯ В ШАДРИНСКОМ УНИВЕРСИТЕТЕ

Я (фамилия, имя, отчество)_____ ____,
Адрес регистрации (в том числе почтовый): _____,
Серия, номер паспорта: _____,
Дата выдачи паспорта:_____ _____,
Орган выдавший паспорт: _____,

в соответствии со статьей 9 Федерального закона Российской Федерации от 26.07.2006 года № 152 -ФЗ «О персональных данных» даю письменное согласие на обработку моих персональных данных **Федеральному государственному бюджетному образовательному учреждению высшего образования «Шадринский государственный педагогический университет» (ШГПУ, Шадринский университет) (юридический /почтовый адрес: 641870, Курганская область, г.Шадринск, ул. Карла Либкнехта, д.3)**, а именно:

фамилию, имя, отчество, пол, дату рождения, место рождения, гражданство, документ удостоверяющий личность (серия, номер, дата выдачи паспорта, наименование органа, выдавшего паспорт, код подразделения), адрес регистрации/места проживания/почтовый, адрес электронной почты, номер телефона, направление подготовки, профиль обучения, форма обучения, квоту (при наличии), форму обучения, результаты Единого государственного Экзамена (ЕГЭ),

результаты вступительных испытаний, проводимых ШГПУ самостоятельно, наименование (год окончания) образовательного учреждения, дающего право на прохождение обучения в высшем образовательном учреждении, серию, номер, регистрационный номер, дату выдачи, наименование учреждения выдавшего аттестат/диплом, страховых свидетельствах государственного пенсионного и медицинского страховании, ИНН, результаты медицинского обследования, сведения о льготах, изображение лица (фотографию), данные отпечатков пальцев, сведения о воинском учете, данные по успеваемости и выполнению учебного плана, данные о договоре (дополнения к нему) на получение образовательных услуг, данные по выданным документам о полученном в ШГПУ образовании, данные о трудоустройстве, сведения о поощрениях и наложенных дисциплинарных взысканиях, результаты посещения научной библиотеки ШГПУ, администрирование и контроль трафика сети Интернет, номер лицевого счёта в банке, номер читательского билета, номер студенческого билета, номер зачетной книжки, номер пропуска в общежитие (при наличии), личную подпись.

с целью обеспечения обучения в Шадринском университете.

Лицо, осуществляющее обработку персональных данных по поручению оператора (ШГПУ) – **Открытое акционерное общество «Сбербанк России»;** Юридический адрес: 117997 г. Москва, ул. Вавилова д.19; Почтовый адрес: 640022 г. Курган, ул. Гоголя, 98. **Цель обработки:** обеспечение обучающегося стипендиальной выплатой в соответствии со статьёй 36 Федерального закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации». **Перечень передаваемых персональных данных:** фамилия, имя, отчество, пол, дата рождения, место рождения, гражданство, документ удостоверяющий личность (серия, номер, дата выдачи паспорта, наименование органа, выдавшего паспорт, код подразделения), адрес регистрации/места проживания, ИНН, СНИЛС, реквизиты договора оказания образовательных услуг, размер стипендиального обеспечения.

Обработка персональных данных осуществляется как на бумажных носителях, так и с использованием средств автоматизации.

Обработка вышеуказанных персональных данных будет осуществляться путем смешанной обработки персональных данных (сбор, систематизация, накопление, хранение, уточнение (обновление, изменение использования, распространение), в том числе передача), обезличивание, блокирование, уничтожение персональных данных) в установленных федеральным законодательством случаях и формах.

Срок действия согласия на обработку персональных данных: на период обучения в ШГПУ или по письменному отзыву.

Данное согласие может быть отозвано в любой момент с обязательным направлением Оператору – Шадринскому университету письменного уведомления.

С момента получения уведомления об отзыве согласия на обработку персональных данных Оператор – Шадринский университет обязан прекратить обработку персональных данных, указанных в настоящем Согласии, и (или) уничтожить персональные данные в течение трех дней с момента получения данного отзыва.

Обязанность уничтожения не распространяется на персональные данные, для которых нормативными правовыми актами предусмотрена обязанность их хранения, в том числе после прекращения отношений в области образования.

Я ознакомлен с «Положением по обработке и защите персональных данных работников, обучающихся и абитуриентов Шадринского университета».

_____ (подпись, расшифровка подписи и дата)

СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ ОБУЧАЮЩЕГОСЯ (ПРЕДСТАВИТЕЛЬ ОБУЧАЮЩЕГОСЯ) В ШАДРИНСКОМ УНИВЕРСИТЕТЕ

Я (фамилия, имя, отчество)_____ _____,
Адрес регистрации (в том числе почтовый): _____,
Серия, номер паспорта: _____,
Дата выдачи паспорта:_____ _____,
Орган выдавший паспорт: _____,
Реквизиты доверенности или иного документа, подтверждающего полномочия в качестве представителя: _____,

являющийся представителем:
(фамилия, имя, отчество):_____,
Адрес регистрации (в том числе почтовый): _____,
Серия, номер паспорта: _____,
Дата выдачи паспорта: _____,
Орган выдавший паспорт: __,

в соответствии со статьей 9 Федерального закона Российской Федерации от 26.07.2006 года № 152 -ФЗ «О персональных данных» даю письменное согласие на обработку моих (вышеуказанных) и моего _____ (*ребенка, доверителя – выбрать нужное*) персональных данных **Федеральному государственному бюджетному образовательному учреждению высшего образования «Шадринский государственный педагогический университет» (ШГПУ, Шадринский университет) (юридический /почтовый адрес: 641870, Курганская область, г.Шадринск, ул. Карла Либкнехта, д.3)**, а именно:

фамилию, имя, отчество, пол, дату рождения, место рождения, гражданство, документ удостоверяющий личность (серия, номер, дата выдачи паспорта,

наименование органа, выдавшего паспорт, код подразделения), адрес регистрации/места проживания/почтовый, адрес электронной почты, номер телефона, направление подготовки, профиль обучения, форма обучения, квоту (при наличии), форму обучения, результаты Единого государственного Экзамена (ЕГЭ), результаты вступительных испытаний, проводимых ШГПУ самостоятельно, наименование (год окончания) образовательного учреждения, дающего право на прохождение обучения в высшем образовательном учреждении, серию, номер, регистрационный номер, дату выдачи, наименование учреждения выдавшего аттестат/диплом, страховых свидетельствах государственного пенсионного и медицинского страховании, ИНН, результаты медицинского обследования, сведения о льготах, изображение лица (фотографию), данные отпечатков пальцев, сведения о воинском учете, данные по успеваемости и выполнению учебного плана, данные о договоре (дополнения к нему) на получение образовательных услуг, данные по выданным документам о полученном в ШГПУ образовании, данные о трудоустройстве, сведения о поощрениях и наложенных дисциплинарных взысканиях, результаты посещения научной библиотеки ШГПУ, администрирование и контроль трафика сети Интернет, номер лицевого счёта в банке, номер читательского билета, номер студенческого билета, номер зачетной книжки, номер пропуска в общежитие (при наличии), личную подпись.

с целью обеспечения обучения в Шадринском университете

Лицо, осуществляющее обработку персональных данных по поручению оператора (ШГПУ) – **Открытое акционерное общество «Сбербанк России»;** Юридический адрес: 117997 г. Москва, ул. Вавилова д.19; Почтовый адрес: 640022 г. Курган, ул. Гоголя, 98. **Цель обработки:** обеспечение обучающегося стипендиальной выплатой в соответствии со статьёй 36 Федерального закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации». **Перечень передаваемых персональных данных:** фамилия, имя, отчество, пол, дата рождения, место рождения, гражданство, документ удостоверяющий личность

(серия, номер, дата выдачи паспорта, наименование органа, выдавшего паспорт, код подразделения), адрес регистрации/места проживания, ИНН, СНИЛС, реквизиты договора оказания образовательных услуг, размер стипендиального обеспечения.

Обработка персональных данных осуществляется как на бумажных носителях, так и с использованием средств автоматизации.

Обработка вышеуказанных персональных данных будет осуществляться путем смешанной обработки персональных данных (сбор, систематизация, накопление, хранение, уточнение (обновление, изменение использования, распространение), в том числе передача), обезличивание, блокирование, уничтожение персональных данных) в установленных федеральным законодательством случаях и формах.

Срок действия согласия на обработку персональных данных: на период обучения в ШГПУ или по письменному отзыву.

Данное согласие может быть отозвано в любой момент с обязательным направлением Оператору – Шадринскому университету письменного уведомления.

С момента получения уведомления об отзыве согласия на обработку персональных данных Оператор – Шадринский университет обязан прекратить обработку персональных данных, указанных в настоящем Согласии, и (или) уничтожить персональные данные в течение трех дней с момента получения данного отзыва.

Обязанность уничтожения не распространяется на персональные данные, для которых нормативными правовыми актами предусмотрена обязанность их хранения, в том числе после прекращения отношений в области образования.

Я ознакомлен с «Положением по обработке и защите персональных данных

работников, обучающихся и абитуриентов Шадринского университета».

_____ (подпись, расшифровка подписи и дата)

Приложение 4
к Положению по обработке и защите
персональных данных работников,
обучающихся и абитуриентов
Шадринского университета

В _____
от _____

Я,_____, занимающий (ая) должность в _____,
даю свое согласие на получение моих персональных данных, а именно:

1. _____
2. _____

у (в) _____

(указать источник - третье лицо, у которого могут быть получены сведения о работнике).

« »_____г. _____

(подпись работника)

Приложение 5
к Положению по обработке и
защите персональных данных
работников, обучающихся и
абитуриентов
Шадринского университета

Куда: _____

Кому: _____

УВЕДОМЛЕНИЕ

В связи с отсутствием согласия субъекта персональных данных на предоставление сведений инициатору обращения, в соответствии со статьями 7 и 9 Федерального закона «О персональных данных» сообщить запрашиваемую Вами информацию в отношении гр. (указать ФИО.) не представляется возможным.

Ректор ШГПУ _____

«_____»_____ 201____г.

Приложение 6
к Положению по обработке и
защите персональных данных
работников, обучающихся и
абитуриентов Шадринского
университета

Инструкция о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные

1.Общие положения

1.1. Настоящая инструкция регламентирует требования по обеспечению конфиденциальности документов содержащих персональные данные для всех структурных подразделений Шадринского государственного педагогического университета.

1.2. Персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, определяемая нормативно-правовыми актами Российской Федерации в области трудовых отношений и образования, нормативными и распорядительными документами Минобрнауки России, Рособразования и Рособрнадзора, положением об обработке и защите персональных данных и приказами ректора Шадринского университета.

1.3. Обеспечение конфиденциальности персональных данных не требуется в случае обезличивания персональных данных или в отношении общедоступных персональных данных. В общедоступные источники персональных данных (в том числе справочники, адресные книги) в целях информационного обеспечения с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер,

сведения о профессии и иные персональные данные, предоставленные субъектом персональных данных.

1.4. Конфиденциальность персональных данных предусматривает обязательное согласие субъекта персональных данных или наличие иного законного основания на их обработку.

1.5. Согласие субъекта персональных данных не требуется на обработку данных:

- в целях исполнения обращения, запроса субъекта персональных данных, трудового или иного договора с ним;

- адресных данных, необходимых для доставки почтовых отправлений организациями почтовой связи;

- данных, включающих в себя только фамилии, имена и отчества; в целях однократного пропуска на территорию, или в иных аналогичных целях; персональных данных, обрабатываемых без использования средств автоматизации.

1.6. В структурных подразделениях университета формируются и ведутся перечни конфиденциальных данных с указанием регламентирующих документов, мест хранения и ответственных за хранение и обработку данных по форме (Приложение 1 к настоящей инструкции).

1.7. Осуществлять обработку и хранение конфиденциальных данных, не внесенных в перечень, запрещается.

1.8. Основные требования и мероприятия по обеспечению безопасности при обработке и хранении персональных данных должны соответствовать постановлениям Правительства Российской Федерации от 17 ноября 2007 г. № 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных" и от 15 сентября 2008 г. № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации".

1.9. 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).

1.10. Запрещается оставлять материальные носители с персональными данными без присмотра в незапертом помещении. Все сотрудники, постоянно работающие в помещениях, в которых ведется обработка персональных данных, должны быть допущены к работе с соответствующими видами персональных данных.

1.11. Сотрудникам, работающим с персональными данными, запрещается сообщать их устно или письменно кому бы то ни было, если это не вызвано служебной необходимостью. После подготовки и передачи документа в соответствии с резолюцией, файлы черновиков и вариантов документа переносятся подготовившим их сотрудником на маркированные носители, предназначенные для хранения персональных данных. Без согласования с руководителем структурного подразделения формирование и хранение баз данных (картотек, файловых архивов и др.), содержащих конфиденциальные данные, запрещается.

1.12. Передача персональных данных допускается только в случаях, установленных Федеральными законами Российской Федерации «О персональных данных», «О порядке рассмотрения обращений граждан Российской Федерации», действующими инструкциями по работе со служебными документами и обращениями граждан, а также по письменному поручению (резолюции) вышестоящих должностных лиц.

1.13. Запрещается передача персональных данных по телефону, факсу, электронной почте за исключением случаев, установленных законодательством и действующими инструкциями по работе со служебными документами и обращениями граждан. Ответы на запросы граждан и организаций даются в том объеме, который позволяет не разглашать в ответах конфиденциальные данные, за исключением данных, содержащихся в материалах заявителя или опубликованных в общедоступных источниках.

1.14. Лица, виновные в нарушении норм, регулирующих обработку и хранение конфиденциальных данных, несут дисциплинарную, административную или уголовную ответственность в соответствии с законодательством и ведомственными нормативными актами.

1.15. Сотрудники структурных подразделений университета и лица, выполняющие работы по договорам и контрактам, имеющие отношение к работе с персональными данными, должны быть в обязательном порядке ознакомлены под расписку с настоящей Инструкцией.

2. Порядок обеспечения безопасности при обработке и хранении персональных данных, осуществляемой без использования средств автоматизации

2.1. 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.

2.2. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки.

2.3. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

2.4. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть

приняты меры по обеспечению раздельной обработки персональных данных, исключающее одновременное копирование иных персональных данных, не подлежащих распространению и использованию.

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, имя (наименование) и адрес Оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых Оператором способов обработки персональных данных;

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

в) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

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

2.6. При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию, на которой находится Оператор, или в иных аналогичных целях, должны соблюдаться следующие условия:

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

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

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

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). Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях, либо путем изготовления нового материального носителя с уточненными персональными данными.

3. Порядок обеспечения безопасности при обработке и хранении персональных данных, осуществляемой с использованием средств автоматизации

3.1. Безопасность персональных данных при их обработке в

информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации, а также используемые в информационной системе информационные технологии.

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

3.3. Размещение информационных систем, специальное оборудование и организация работы с персональными данными должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого пребывания в этих помещениях посторонних лиц.

3.4. Компьютеры и (или) электронные папки, в которых содержатся файлы с персональными данными, для каждого пользователя должны быть защищены индивидуальными паролями доступа, состоящими из 6 и более символов. Работа на компьютерах с персональными данными без паролей доступа, или под чужими или общими (одинаковыми) паролями, запрещается.

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

3.6. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации. Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия.

3.7. При обработке персональных данных в информационной системе пользователями должно быть обеспечено:

а) использование предназначенных для этого разделов (каталогов) носителей информации, встроенных в технические средства, или съемных маркированных носителей;

б) недопущение физического воздействия на технические средства автоматизированной обработки персональных данных, в результате которого

может быть нарушено их функционирование;

в) постоянное использование антивирусного обеспечения для обнаружения зараженных файлов и незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

г) недопущение несанкционированных выноса из помещений, установки, подключения оборудования, а также удаления, инсталляции или настройки программного обеспечения.

3.8. При обработке персональных данных в информационной системе разработчиками и

администраторами систем должны обеспечиваться:

а) обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

б) учет лиц, допущенных к работе с персональными данными в информационной системе, прав и паролей доступа;

в) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;

г) контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

д) описание системы защиты персональных данных).

3.9. Специфические требования по защите персональных данных в отдельных автоматизированных системах устанавливаются инструкциями по их использованию и эксплуатации.

4. Порядок учета, хранения и обращения со съемными носителями персональных данных, твердыми копиями и их утилизации

4.1. Все находящиеся на хранении и в обращении съемные носители с персональными данными подлежат учёту. Каждый съемный носитель с записанными на нем персональными данными должен иметь этикетку, на которой указывается его учетный номер.

4.2. Учет и выдачу съемных носителей персональных данных по форме

(Приложение 2 к настоящей инструкции) осуществляют сотрудники структурных подразделений, на которых возложены функции хранения носителей персональных данных. Сотрудники университета получают учтенный съемный носитель от уполномоченного сотрудника для выполнения работ на конкретный срок. При получении делаются соответствующие записи в журнале учета. По окончании работ пользователь сдает съемный носитель для хранения уполномоченному сотруднику, о чем делается соответствующая запись в журнале учета.

4.3. При работе с носителями персональных данных запрещается:

- хранить съемные носители с персональными данными вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

- выносить съемные носители с персональными данными из служебных помещений для работы с ними на дому, в гостиницах и т. д.

4.4. При отправке или передаче персональных данных адресатам на съемные носители записываются только предназначенные адресатам данные. Отправка персональных данных адресатам на съемных носителях осуществляется в порядке, установленном для документов для служебного пользования. Вынос съемных носителей персональных данных для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя структурного подразделения).

4.5. О фактах утраты съемных носителей, содержащих персональные данные, либо разглашения содержащихся в них сведений немедленно ставится в известность руководителя соответствующего структурного подразделения. На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы персонального учета съемных носителей персональных данных.

4.6. Съемные носители персональных данных, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с конфиденциальной информацией осуществляется «уполномоченной комиссией». По результатам уничтожения носителей составляется акт по форме (Приложение 3).

Приложение 1
к Инструкции о порядке обеспечения
конфиденциальности при обращении с
информацией, содержащей
персональные данные

ПЕРЕЧЕНЬ
персональных данных, обрабатываемых в структурных подразделениях

_____
наименование учреждения

_____
наименование структурного подразделения

№ п/п	Наименование (вид, типовая форма) документов с персональными данными	Регламен-тирующие документы (Наименование, дата, номер)	Наименование информационной системы/ без использо-вания средств автоматизации	Отдел	Место хранения (комната)	ФИО ответ-ственных за обработку и хранение
1						
2						
3						

_____ _____
Должность и ФИО начальника структурного подразделения Подпись

Приложение 2
к Инструкции о порядке обеспечения
конфиденциальности при обращении с
информацией, содержащей
персональные данные

ЖУРНАЛ
учета съемных носителей персональных данных

_____

наименование структурного подразделения

Начат « » _____ _____ на листах
Окончен « » _____ _____

_____ _____
Должность и ФИО ответственного за хранение Подпись

№ п/п	Метка съемного носителя (учетный номер)	Фамилия исполнителя	(Получил, вернул, передал)	Дата записи информации	Подпись исполнителя	Примечание*
1						
2						
3						
4						
5						

* Причина и основание окончания использования (№ и дата отправки адресату или распоряжения о передаче, № и дата акта утраты, неисправность, заполнение подлежащими хранению данными)

Приложение 3
к Инструкции о порядке обеспечения
конфиденциальности при обращении
с информацией, содержащей
персональные данные

«УТВЕРЖДАЮ»
Ректор ФГБОУ ВО
«Шадринский государственный
педагогический университет»
« » _____ ____ года

АКТ
уничтожения съемных носителей персональных данных

Комиссия, наделенная полномочиями приказом от « »_____ ____ года № _____
в составе: _____
(должности, ФИО)

провела отбор съемных носителей персональных данных, не подлежащих дальнейшему хранению:

№ п/п	Дата	Учетный номер съемного носителя	Пояснения
1	2	3	4

Всего съемных носителей:
_____
(цифрами и прописью)

На съемных носителях уничтожена конфиденциальная информация путем стирания ее на устройстве гарантированного уничтожения информации (механического уничтожения, сжигания и т.п.).

Перечисленные съемные носители уничтожены
_____
путем (разрезания, демонтажа и т.п.),

_____
измельчены и сданы для уничтожения предприятию по утилизации вторичного сырья
_____
(наименование предприятия)

_____ _____ _____
Председатель комиссии Подпись Дата

Члены комиссии:
_____ _____ _____

Приложение 7
к Положению по обработке и защите
персональных данных работников,
обучающихся и абитуриентов
Шадринского университета

Инструкция пользователя при обработке персональных данных на объектах вычислительной техники

1. Общие положения

1.1. Инструкция регламентирует основные обязанности, права и ответственность пользователя, допущенного к автоматизированной обработке персональных данных и иной конфиденциальной информации на объектах вычислительной техники (ПЭВМ) Шадринского государственного педагогического университета.

1.2. Для выполнения работ с персональными данными пользователь должен быть допущен к обработке соответствующих категорий персональных данных и иметь навыки работы на ПЭВМ.

1.3. Пользователь при выполнении работ в пределах своих функциональных обязанностей, обеспечивает безопасность персональных данных, обрабатываемых и хранимых в ПЭВМ и несет персональную ответственность за соблюдение требований руководящих документов по защите информации.

2. Обязанности пользователя

2.1. Пользователь при работе с персональными данными обязан:

- выполнять общие требования по обеспечению режима конфиденциальности проводимых работ, установленные в настоящей Инструкции;

- при работе с персональными данными не допускать присутствие в помещении, где расположены средства вычислительной техники, не допущенных к обрабатываемой информации лиц или располагать во время работы экран

видеомонитора так, чтобы исключалась возможность просмотра, отображаемой на нем информации посторонними лицами;

- соблюдать правила работы со средствами защиты информации и установленный режим разграничения доступа к техническим средствам, программам, данным, файлам с персональными данными при ее обработке;

- после окончания обработки персональных данных в рамках выполнения одного задания, а также по окончании рабочего дня, произвести стирание остаточной информации с жесткого диска ПЭВМ;

- оповещать обслуживающий ПЭВМ персонал, а также непосредственного начальника о всех фактах или попытках несанкционированного доступа к информации, обрабатываемой в ПЭВМ;

- не допускать "загрязнение" ПЭВМ посторонними программными средствами;

- знать способы выявления нештатного поведения используемых операционных систем и пользовательских приложений, последовательность дальнейших действий,

- знать и соблюдать правила поведения в экстренных ситуациях, последовательность действий при ликвидации последствий аварий;

- помнить личные пароли, персональные идентификаторы не оставлять без присмотра и хранить в запирающемся ящике стола или сейфе;

- знать штатные режимы работы программного обеспечения, знать пути проникновения и распространения компьютерных вирусов;

- при применении внешних носителей информации перед началом работы провести их проверку на предмет наличия компьютерных вирусов.

2.2. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь должен провести внеочередной антивирусный контроль своей рабочей станции.

2.3. В случае обнаружения при проведении антивирусной проверки

зараженных компьютерными вирусами файлов пользователь обязан:

- приостановить работу;

- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов своего непосредственного начальника, администратора системы, а также смежные подразделения, использующие эти файлы в работе;

- оценить необходимость дальнейшего использования файлов, зараженных вирусом;

- провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта следует привлечь администратора системы).

3. Запрещаемые действия

3.1. Пользователю при работе с персональными данными запрещается:

- записывать и хранить персональные данные на неучтенных установленным порядком машинных носителях информации;

- удалять с обрабатываемых или распечатываемых документов грифы конфиденциальности;

- самостоятельно подключать к ПЭВМ какие-либо устройства и вносить изменения в состав, конфигурацию, размещение ПЭВМ;

- самостоятельно устанавливать и/или запускать (выполнять) на ПЭВМ любые системные или прикладные программы, загружаемые по сети Интернет или с внешних носителей;

- осуществлять обработку персональных данных в условиях, позволяющих осуществлять их просмотр лицами, не имеющими к ним допуска, а также при несоблюдении требований по эксплуатации ПЭВМ;

- сообщать кому-либо устно или письменно личные атрибуты доступа к ресурсам ПЭВМ;

- отключать (блокировать) средства защиты информации;

- производить какие-либо изменения в подключении и размещении технических средств;

- производить иные действия, ограничения на исполнение которых

предусмотрены утвержденными регламентами и инструкциями;

- оставлять бесконтрольно ПЭВМ с загруженными персональными данными, с установленными маркированными носителями, электронными ключами, а также распечатываемыми бумажными документами с персональными данными.

4. Права и ответственность пользователя ПЭВМ

4.1. Пользователь имеет право:

- обрабатывать (создавать, редактировать, уничтожать, копировать, выводить на печать) информацию в пределах установленных ему полномочий;

- обращаться к обслуживающему ПЭВМ персоналу с просьбой об оказании технической и методической помощи при работе с общесистемным и прикладным программным обеспечением, установленным в ПЭВМ, а также со средствами защиты информации.

4.2. Пользователь несет ответственность за:

- надлежащее выполнение требований настоящей инструкции;

- соблюдение требований нормативных документов и инструкций, определяющих порядок организации работ по защите информации и использования информационных ресурсов;

- сохранность и работоспособное состояние средств вычислительной техники ПЭВМ;

- сохранность персональных данных.

4.3. Особенности обработки персональных данных пользователями отдельных автоматизированных систем могут регулироваться дополнительными инструкциями.

Приложение 8
к Положению по обработке и защите
персональных данных работников,
обучающихся и абитуриентов
Шадринского университета

Инструкция по проведению мониторинга информационной безопасности и антивирусного контроля при обработки персональных данных

1. Общие положения

1.1. Инструкция регламентирует порядок планирования и проведения мониторинга информационной безопасности автоматизированных систем, обрабатывающих персональные данные, от несанкционированного доступа, распространения, искажения и утраты информации Федерального государственного бюджетного образовательного учреждения высшего образования «Шадринского государственного педагогического университет».

1.2. Мониторинг работоспособности аппаратных компонент автоматизированных систем, обрабатывающих персональные данные, осуществляется в процессе их администрирования и при проведении работ по техническому обслуживанию оборудования. Наиболее существенные компоненты системы, имеющие встроенные средства контроля работоспособности (серверы, активное сетевое оборудование) должны контролироваться постоянно в рамках работы администраторов соответствующих систем.

1.3. Мониторинг парольной защиты и контроль надежности пользовательских паролей предусматривают:

- установление сроков действия паролей (не более 3 месяцев);

- периодическую (не реже 1 раза в месяц) проверку пользовательских паролей на количество символов и очевидность с целью выявления слабых паролей, которые легко угадать или дешифровать с помощью специализированных программных средств (взломщиков паролей).

1.4. Мониторинг целостности программного обеспечения включает следующие действия:

- проверка контрольных сумм и цифровых подписей каталогов и файлов сертифицированных программных средств при загрузке операционной системы;

- обнаружение дубликатов идентификаторов пользователей;

- восстановление системных файлов администраторами систем с резервных копий при несовпадении контрольных сумм.

1.5. Предупреждение и своевременное выявление попыток несанкционированного доступа осуществляется с использованием средств операционной системы и специальных программных средств, и предусматривает:

- фиксацию неудачных попыток входа в систему в системном журнале;

- протоколирование работы сетевых сервисов;

- выявление фактов сканирования определенного диапазона сетевых портов, в короткие промежутки времени с целью обнаружения сетевых анализаторов, изучающих систему и выявляющих ее уязвимости.

1.6. Мониторинг производительности автоматизированных систем, обрабатывающих персональные данные, производится по обращениям пользователей, в ходе администрирования систем и проведения профилактических работ для выявления попыток несанкционированного доступа, повлекших существенное уменьшение производительности систем.

2. Системный аудит

2.1. Системный аудит производится ежеквартально и в особых ситуациях. Он включает проведение обзоров безопасности, тестирование системы, контроль внесения изменений в системное программное обеспечение.

2.2. Обзоры безопасности проводятся с целью проверки соответствия текущего состояния систем, обрабатывающих персональные данные, тому уровню безопасности, удовлетворяющему требованиям политики безопасности. Обзоры безопасности имеют целью выявление всех несоответствий между текущим состоянием системы и состоянием, соответствующем специально составленному

списку для проверки.

2.3. Обзоры безопасности должны включать:

- отчеты о безопасности пользовательских ресурсов, включающие наличие повторяющихся пользовательских имен и идентификаторов, неправильных форматов регистрационных записей, пользователей без пароля, неправильной установки домашних каталогов пользователей и уязвимостей пользовательских окружений;

- проверку содержимого файлов конфигурации на соответствие списку для проверки;

- обнаружение изменений системных файлов со времени проведения последней проверки (контроль целостности системных файлов);

- проверку прав доступа и других атрибутов системных файлов (команд, утилит и таблиц);

- проверку правильности настройки механизмов аутентификации и авторизации сетевых сервисов;

- проверку корректности конфигурации системных и активных сетевых устройств (мостов, маршрутизаторов, концентраторов и сетевых экранов).

2.4. Активное тестирование надежности механизмов контроля доступа производится путем осуществления попыток проникновения в систему (с помощью автоматического инструментария или вручную).

2.5. Пассивное тестирование механизмов контроля доступа осуществляется путем анализа конфигурационных файлов системы. Информация об известных уязвимостях извлекается из документации и внешних источников. Затем осуществляется проверка конфигурации системы с целью выявления опасных состояний системы, т. е. таких состояний, в которых могут проявлять себя известные уязвимости. Если система находится в опасном состоянии, то, с целью нейтрализации уязвимостей, необходимо либо изменить конфигурацию системы (для ликвидации условий проявления уязвимости), либо установить программные коррекции, либо установить другие версии программ, в которых данная уязвимость отсутствует, либо отказаться от использования системного сервиса, содержащего

данную уязвимость.

2.6. Внесение изменений в системное программное обеспечение осуществляется администраторами систем, обрабатывающих персональные данные, с обязательным документированием изменений в соответствующем журнале; уведомлением каждого сотрудника, кого касается изменение; выслушиванием претензий в случае, если это изменение причинило кому-нибудь вред; разработкой планов действий в аварийных ситуациях для восстановления работоспособности системы, если внесенное в нее изменение вывело ее из строя.

3. Антивирусный контроль

3.1. Для защиты серверов и рабочих станций необходимо использовать антивирусные программы:

- резидентные антивирусные мониторы, контролирующие подозрительные действия программ;

- утилиты для обнаружения и анализа новых вирусов.

3.2. К использованию допускаются только лицензионные средства защиты от вредоносных программ и вирусов или сертифицированные свободно распространяемые антивирусные средства.

3.3. При подозрении на наличие не выявленных установленными средствами защиты заражений следует использовать Live CD с другими антивирусными средствами.

3.4. Установка и настройка средств защиты от вредоносных программ и вирусов на рабочих станциях и серверах автоматизированных систем, обрабатывающих персональные данные, осуществляется администраторами соответствующих систем в соответствии с руководствами по установке приобретенных средств защиты.

3.5. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено администратором системы на отсутствие вредоносных программ и компьютерных вирусов. Непосредственно после установки (изменения) программного обеспечения рабочей станции должна быть

выполнена антивирусная проверка.

3.6. Запуск антивирусных программ должен осуществляться автоматически по заданию, централизованно созданному с использованием планировщика задач (входящим в поставку операционной системы либо поставляемым вместе с антивирусными программами).

3.7. Антивирусный контроль рабочих станций должен проводиться ежедневно в автоматическом режиме. Если проверка всех файлов на дисках рабочих станциях занимает неприемлемо большое время, то допускается проводить выборочную проверку загрузочных областей дисков, оперативной памяти, критически важных инсталлированных файлов операционной системы и загружаемых файлов по сети или с внешних носителей. В этом случае полная проверка должна осуществляться не реже одного раза в неделю в период неактивности пользователя. Пользователям рекомендуется осуществлять полную проверку во время перерыва на обед путем перевода рабочей станции в соответствующий автоматический режим функционирования в запертом помещении.

3.8. Обязательному антивирусному контролю подлежит любая информация (исполняемые файлы, текстовые файлы любых форматов, файлы данных), получаемая пользователем по сети или загружаемая со съемных носителей (магнитных дисков, оптических дисков, флэш-накопителей и т.п.). Контроль информации должен проводиться антивирусными средствами в процессе или сразу после ее загрузки на рабочую станцию пользователя. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

3.9. Устанавливаемое (изменяемое) на серверы программное обеспечение должно быть предварительно проверено администратором системы на отсутствие компьютерных вирусов и вредоносных программ. Непосредственно после установки (изменения) программного обеспечения сервера должна быть выполнена антивирусная проверка.

3.10. На серверах систем, обрабатывающих персональные данные,

необходимо применять специальное антивирусное программное обеспечение, позволяющее:

- осуществлять антивирусную проверку файлов в момент попытки записи файла на сервер;

- проверять каталоги и файлы по расписанию с учетом нагрузки на сервер.

3.11. На серверах электронной почты необходимо применять антивирусное программное обеспечение, обеспечивающее проверку всех входящих сообщений. В случае если проверка входящего сообщения на почтовом сервере показала наличие в нем вируса или вредоносного кода, отправка данного сообщения должна блокироваться. При этом должно осуществляться автоматическое оповещение администратора почтового сервера, отправителя сообщения и адресата.

3.12. Необходимо организовать регулярное обновление антивирусных баз на всех рабочих станциях и серверах.

3.13. Администраторы систем должны проводить регулярные проверки протоколов работы антивирусных программ с целью выявления пользователей и каналов, через которых распространяются вирусы. При обнаружении зараженных вирусом файлов администратор системы должен выполнить следующие действия:

- отключить от компьютерной сети рабочие станции, представляющие вирусную опасность, до полного выяснения каналов проникновения вирусов и их уничтожения;

- немедленно сообщить о факте обнаружения вирусов непосредственному начальнику с указанием предположительного источника (отправителя, владельца и т.д.) зараженного файла, типа зараженного файла, характера содержащейся в файле информации, типа вируса и выполненных антивирусных мероприятий.

4. Анализ инцидентов

4.1. Если администратор системы, обрабатывающей персональные данные, подозревает или получил сообщение о том, что его система подвергается атаке или уже была скомпрометирована, то он должен установить:

- факт попытки несанкционированного доступа (НСД);

- продолжается ли НСД в настоящий момент;

- кто является источником НСД;

- что является объектом НСД;

- когда происходила попытка НСД;

- как и при каких обстоятельствах была предпринята попытка НСД;

- точка входа нарушителя в систему;

- была ли попытка НСД успешной;

- определить системные ресурсы, безопасность которых была нарушена;

- какова мотивация попытки НСД.

4.2. Для выявления попытки НСД необходимо установить, какие пользователи в настоящее время работают в системе, на каких рабочих станциях. Выявить подозрительную активность пользователей, проверить, что все пользователи вошли в систему со своих рабочих мест, и никто из них не работает в системе необычно долго. Кроме того, необходимо проверить что никто из пользователей не выполняет подозрительных программ и программ, не относящихся к его области деятельности.

4.3. При анализе системных журналов администратору необходимо произвести следующие действия:

- проверить наличие подозрительных записей системных журналов, сделанных в период предполагаемой попытки НСД, включая вход в систему пользователей, которые должны бы были отсутствовать в этот период времени, входы в систему из неожиданных мест, в необычное время и на короткий период времени;

- проверить не уничтожен ли системный журнал и нет ли в нем пробелов;

- просмотреть списки команд, выполненных пользователями в рассматриваемый период времени;

- проверить наличие исходящих сообщений электронной почты, адресованные подозрительным хостам;

- проверить наличие мест в журналах, которые выглядят необычно;

выявить попытки получить полномочия суперпользователя или другого

привилегированного пользователя;

- выявить наличие неудачных попыток входа в систему.

4.4. В ходе анализа журналов активного сетевого оборудования (мостов, переключателей, маршрутизаторов, шлюзов) необходимо:

- проверить наличие подозрительных записей системных журналов, сделанных в период предполагаемой попытки НСД;

- проверить не уничтожен ли системный журнал и нет ли в нем пробелов;

- проверить наличие мест в журналах, которые выглядят необычно;

- выявить попытки изменения таблиц маршрутизации и адресных таблиц;

- проверить конфигурацию сетевых устройств с целью определения возможности нахождения в системе программы, просматривающей весь сетевой трафик.

4.5. Для обнаружения в системе следов, оставленных злоумышленником, в виде файлов, вирусов, троянских программ, изменения системной конфигурации необходимо:

- составить базовую схему того, как обычно выглядит система;

- провести поиск подозрительных файлов, скрытые файлы, имена файлов и

- каталогов, которые обычно используются злоумышленниками;

проверить содержимое системных файлов, которые обычно изменяются злоумышленниками;

- проверить целостность системных программ;

- проверить систему аутентификации и авторизации.

4.6. В случае заражения значительного количества рабочих станций после устранения его последствий проводится системный аудит.

4.7. Особенности мониторинга информационной безопасности персональных данных в отдельных автоматизированных системах могут регулироваться дополнительными инструкциями.