Министерство Культуры Челябинской области
Государственное бюджетное образовательное учреждение высшего образования
«Южно-Уральский государственный институт искусств имени П.И. Чайковского»
(ГБОУ ВО «ЮУрГИИ им. П.И. Чайковского»)

УТВЕРЖДАЮ
Ректор

_____ Е.Р. Сизова

« 18 » декабря 20 23 г.

приказ от 18.12.2023 № 02-10/03-47

ПОЛОЖЕНИЕ
ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ГБОУ ВО «ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ИНСТИТУТ ИСКУССТВ ИМЕНИ П. И. ЧАЙКОВСКОГО» И В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ ГБОУ ВО «ЮУРГИИ ИМ. П.И. ЧАЙКОВСКОГО»

Челябинск 2023

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение об обработке и защите персональных данных (далее – Положение) в государственном бюджетном образовательном учреждении высшего образования «Южно-Уральский государственный институт искусств имени П. И. Чайковского» (далее – институт) и в информационных системах персональных данных (далее – ИСПДн)института разработано в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Гражданским кодексом Российской Федерации, Федеральным законом Российской Федерации
от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом Российской Федерации от 27.07.2006 №152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом Федеральной службы по техническому и экспортному контролю Российской Федерации от 18.02.2013 №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и устанавливает порядок приема, учета, сбора, поиска, обработки, защиты, накопления и хранения документов, содержащих сведения, отнесенных к персональным данным института и ИСПДнинститута.

1.2. Цель разработки Положения – определение порядка обработки персональных данных работниковинститута и иных субъектов персональных данных (далее – субъекты ПДн), персональные данные которых подлежат обработке в ИСПДн института; защитыПДн от несанкционированного доступа, неправомерного их использования или утраты.

1.3. Институт является оператором персональных данных лиц, указанных в пункте 2.1. настоящего Положения. На основании письменного согласияна обработку персональных данных (далее – Согласие) институтвправе передавать персональные данные другим лицам с целью их обработки. Существенным условием Согласия является соблюдение другими лицами конфиденциальности персональных данных и обеспечение безопасности при их обработке.

1.4. Персональные данные, которые обрабатываются в информационных системах персональных данных института, подлежат защите от несанкционированного доступа и копирования. Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

1.5. Сведения о персональных данных работников относятся к числу конфиденциальных. Режим конфиденциальности в отношении персональных данных снимается:

1) в случае их обезличивания;

2) по истечении 75 лет срока их хранения;

3) в других случаях, предусмотренных законодательством Российской Федерации.

1.6. Настоящее Положение вступает в силу с момента его утверждения ректором института и действует бессрочно, до замены его новым Положением.

1.7. Все изменения в Положение вносятся приказом ректора института.

2. ОСНОВНЫЕ ПОНЯТИЯ И СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Основные понятия:

1) субъект персональных данных –физическое лицо (работник, абитуриент/обучающийся института, законный представитель абитуриента/обучающегося, участник Единого государственного экзамена и т.п.), которое прямо или косвенно определено или определяемо с помощьюперсональных данных;

2) оператор –юридическое лицо (институт), самостоятельно или совместно с другими лицами организующее и/или осуществляющее обработку персональных данных, а также определяющее цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными субъекта;

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

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

5) технические средства, позволяющие осуществлять обработку персональных данных, – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных, программные средства, средства защиты информации, применяемые в информационных системах;

6) уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и/или в результате которых уничтожаются материальные носители персональных данных;

7) распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

2.2. Обработка персональных данных осуществляетсябез использования средств автоматизации и/или с использованием средств информационных систем персональных данных в институте.

1) обработка персональных данных – действия (операции), совершаемые с использованием средств автоматизации или без использования таких средств.

Обработка персональных данных включает в себя следующие действия (операции):

1) сбор, хранение, уточнение (обновление, изменение);

2) систематизацию, накопление;

3) извлечение, использование, распространение (в том числе передачу);

4) обезличивание, блокирование, уничтожение.

2.3. Оператор (институт) с письменного согласия обрабатывает персональные данные работников, абитуриентов/обучающихся института, законных представителейабитуриентов/обучающихся, участников Единого государственного экзамена и т.п. (далее – субъекты ПДн).

2.4. Оператор (институт) определяет состав персональных данных субъектов ПДн (ФИО, пол, место и дата рождения, гражданство, адрес по прописке (проживания), паспортные данные, СНИЛС, ИНН и т.п.), обрабатываемых в информационных системах персональных данных института.

2.5. Комплексы АРМ ИСПДн, объединенные в локальную вычислительную сеть, подключены к защищенным сетям федеральных и региональных информационных систем.

3. СБОР, ОБРАБОТКА И ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1 Порядок получения персональных данных:

1) персональные данные субъектов ПДноператор (институт) получает и обрабатывает только с письменного согласия, либос письменного согласия их законных представителей;

2) письменное согласие субъекта ПДнна обработку персональных данных должно включать в себя следующие персональные данные:

а) работники института:

– фамилия, имя, отчество, информация о смене фамилии, имени, отчества;

– пол;

– место и дата рождения, Гражданство;

– адрес по прописке (проживания);

– паспортные данные (серия, номер паспорта, кем и когда выдан);

– личная подпись;

– СНИЛС (страховое свидетельство обязательного пенсионного страхования);

– ИНН (при наличии);

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

– информация об образовании (наименование образовательного учреждения, сведения о документах, подтверждающие образование: наименование, номер, дата выдачи, специальность);

– биометрические персональные данные (фотография) в общественных или иных интересах оператора, связанных с трудовой деятельностью с целью размещения на сайте: http://www.uyrgii.ru/, на информационных стендах, или получения при съемке в местах, открытых для посещения, или на публичных мероприятиях (концертах, спектаклях, выставках и подобных мероприятиях);

– информация о трудовой деятельности (стаже) до приема на работу;

– телефонный номер (домашний, мобильный), адрес электронной почты;

– семейное положение и состав семьи (муж/жена, дети);

– информация о знании иностранных языков;

– информация, образующаяся в результате трудовой деятельности у оператора о приеме на работу, трудовом договоре и соглашениях к нему, окладе, доплатах и надбавках, перемещениях по профессии (должности), отпусках, командировках, о трудовом стаже, об отсутствии по уважительной причине, увольнении и т.п.;

– данные об аттестации работников;

– данные о повышении квалификации;

– данные о наградах, поощрениях, ученых степенях и званиях, почетных званиях;

– информация о наличии (отсутствии) судимости;

– результаты обязательных предварительных (при поступлении на работу) и периодических медицинских осмотров (обследований), в порядке, установленном законодательством Российской Федерации, а также обязательного психиатрического и наркологического освидетельствования

– сведения о социальных гарантиях;

б) абитуриенты:

– фамилия, имя, отчество, информация о смене фамилии, имени, отчества;

– пол;

– место и дата рождения, гражданство;

– паспортные данные (серия, номер паспорта, кем и когда выдан) / данные свидетельства о рождении;

– личная подпись;

– информация об образовании (наименование образовательного учреждения, сведения о документах, подтверждающие образование: наименование, номер, дата выдачи, специальность);

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

– состав семьи;

– сведения о социальных гарантиях;

– адрес по прописке (проживания), телефонный номер (домашний, мобильный), адрес электронной почты;

– биометрические персональные данные (фотография) в общественных или иных интересах оператора, связанных с поступлением;

– информация о знании иностранных языков;

– информация о прохождении вступительных испытаний;Я

– информация, образующаяся в процессе поступления (приказы о зачислении, списки, протоколы коллоквиума, экзаменационные ведомости и т.п.);

– информация о научных, культурных и спортивных достижениях;

– сведения о миграционно-визовом учете;

– данные медицинской карты;

в) обучающиеся:

– фамилия, имя, отчество, информация о смене фамилии, имени, отчества;

– пол;

– место и дата рождения, гражданство;

– паспортные данные (серия, номер паспорта, кем и когда выдан);

– личная подпись;

– информация об образовании (наименование образовательного учреждения, сведения о документах, подтверждающие образование: наименование, номер, дата выдачи, специальность);

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

– состав семьи;

– сведения о социальных гарантиях;

– адрес по прописке (проживания), телефонный номер (домашний, мобильный), адрес электронной почты;

– биометрические персональные данные (фотография) в общественных или иных интересах оператора, связанных с обучением;

– информация о знании иностранных языков;

– сведения о стипендии и дополнительных выплатах;

– информация, образующаяся, в процессе учебной деятельности (о зачислении, переводе, академическом отпуске, отчислении в связи с окончанием обучения, поощрениях, взысканиях и т.п.);

– информация об отсутствии по уважительной причине;

– информация, о наличии пройденной флюорографии и прививках;

– информация о трудовой деятельности до зачисления на обучение;

– информация о профсоюзной и общественной деятельности;

– информация о научных, культурных и спортивных достижениях;

– данные договора об оказании платных образовательных услуг (при наличии);

– сведения о миграционно-визовом учете;

– данные медицинской карты;

– данные свидетельства о рождении;

г) оператор (институт) в письменном согласии информирует законных представителей абитуриентов/обучающихся о персональных данных их несовершеннолетних детей, которые оператор будет обрабатывать с целью осуществления идентификации личности, правового регулирования обучения, документирования факта, этапов, характера обучения и т.п.;

3) оператор обязан ознакомить субъекта ПДн, что:

– согласие на обработку персональных данных действует с момента его подписания в течение всего срока работы, поступления на обучение и/или обучения у оператора;

– субъект ПДн имеет право, по письменному запросу, на получение информации, касающейся обработки своих персональных данных;

– после увольнения с работы (прекращения трудовых отношений) / отчисления в связи с окончанием обучения персональные данные хранятся у оператора в течение срока хранения документов, предусмотренного законодательством Российской Федерации;

– согласие на обработку персональных данных может быть отозвано на основании письменного заявления в произвольной форме. В случае отзыва согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27 июля 2006г. №152-ФЗ «О персональных данных»;

– персональные данные, предоставляемые в отношении третьих лиц, обрабатываются только в целях осуществления и выполнения, возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

4) если персональные данные возможно получить только у третьей стороны, то субъект ПДн должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Должностное лицо учреждения должно сообщить о целях, предполагаемых источниках и способах получения персональных данных,а также о характере подлежащих получению персональных данныхи последствиях отказа субъекта дать письменное согласие на их получение;

5) оператор (далее – институт) не имеет права получать и обрабатывать персональные данные субъектов ПДн об их расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни;

6) согласие субъекта не требуется в следующих случаях:

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

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

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

г) обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве (далее – исполнение судебного акта);

д) обработка персональных данных необходима для предоставления государственной или муниципальной услуги в соответствии с Федеральным законом от 27.07.2010 №210-ФЗ «Об организации предоставления государственных и муниципальных услуг», для обеспечения предоставления такой услуги, для регистрации субъекта персональных данных на едином портале государственных и муниципальных услуг;

е) обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

ж) обработка персональных данных осуществляется в статистических или иных исследовательских целях, при условии обязательного обезличивания персональных данных;

з) обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц, либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

и) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов работника, если получение его согласия невозможно.

3.2. Порядок обработки, передачи и хранения персональных данных:

а) субъект ПДн предоставляет институту (оператору) достоверные сведения о себе. Оператор (уполномоченное должностное лицо) проверяет достоверность сведений, сверяя данные, предоставленные субъектом, с имеющимисяу субъекта документами.

3.3. Оператор при обработке персональных данных субъекта ПДн должен соблюдать следующие общие требования:

1) обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов Российской Федерации, при оформлении трудовых правоотношений между оператором и субъектом, при оказании образовательных услуг оператором и проведении Государственной итоговой аттестации;

2) при определении объема и содержания обрабатываемых персональных данных оператор должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ и иными нормативными правовыми актами Российской Федерации.

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

3.5. Защита персональных данных субъекта от неправомерного их использования или утраты обеспечивается оператором за счет собственных средств в порядке, установленном Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных».

4. ПЕРЕДАЧА И ХРАНЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. При передаче персональных данных субъекта ПДноператор должен соблюдать следующие требования:

1) не разглашать персональные данные субъекта ПДнтретьей стороне без письменного согласия субъектаПДн, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, установленных Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных»;

2) не сообщать персональные данные в коммерческих целях без письменного согласия субъекта ПДн;

3) предупреждатьуполномоченное должностное лицо, получающее персональные данные субъектаПДн, о том, что персональные данные могут быть использованы лишь в целях, для которых они переданы, и требовать от этого лица подтверждения того, что это правило соблюдается. Уполномоченное должностное лицо, получившее персональные данные субъектаПДн, обязано соблюдать режим конфиденциальности;

4) осуществлять передачу персональных данных субъектов ПДн в соответствии с локальными актами института (оператора), с которымисубъекты ПДндолжны быть ознакомлены под подпись.

4.2. Настоящее Положение не распространяется на обмен персональными данными субъектов ПДнв порядке, установленном Федеральными законами:

1) оператор осуществляет передачу персональных данных субъектовПДн в порядке, определенном настоящим Положением.

2) доступ к персональным данным субъектов ПДноператором разрешен только уполномоченным должностным лицам, при этом указанные лица должны иметь право получать только те персональные данные субъектовПДн, которые необходимы для выполнения конкретной функции.

3) оператор передает персональные данные субъектов ПДнтретьим лицам и/или их представителям в порядке, установленном законодательством Российской Федерации, и ограничивает эту информацию только теми персональными данными субъектаПДн, которые необходимы для выполнения указанными третьими лицами и/или представителями их функций.

4) не допускается предоставлять информацию, связанную с передачей персональныхданных субъектов ПДн, по телефону или факсу.

4.3. Хранение и использование персональных данных:

1) персональные данные субъектов ПДнобрабатываются и хранятся на бумажных и иных носителях в местах храненияматериальных носителей оператора, определенныхПеречнем мест хранения материальных носителей персональных данных;

2) полученные оператором, персональные данные субъектовПДн, могут проходить дальнейшую обработку и передаваться на хранение, как на бумажных носителях, так и в иных видах, таких как: локальная компьютерная сеть, компьютерные программы и электронные базы данных.

3) персональные данные субъектов ПДн подлежат уничтожению из информационных систем персональных данных оператора по достижении целей обработки (оператор составляет Акт уничтожения ПДн).

4.4. При получении персональных данных не от субъекта ПДн (за исключением случаев, если персональные данные были предоставлены оператору на основании федерального закона или если персональные данные являются общедоступными), оператор до начала обработки таких персональных данных обязан предоставить субъекту ПДнследующую информацию:

1) наименование (фамилия, имя, отчество) и адрес оператора или его представителя;

2) цель обработки персональных данных и ее правовое основание;

3) предполагаемых пользователей персональных данных;

4) установленные Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» права субъекта персональных данных.

4.5. Оператор (институт) обязан уведомить Роскомнадзор об изменениях представленных им ранее сведений об обработке ПДн, произошедших за месяц, в срок не позднее 15 числа следующего месяца.

5. ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ

5.1. Списокуполномоченных должностных лиц, которым необходим допуск к персональным данным при их обработке у оператора(институт) и в информационных системах персональных данных оператора (институт)определяется приказом ректором института.

5.2. Субъект ПДн, чьи персональные данные обрабатываются в информационной системе института, имеет право:

1) получать доступ к своим персональным данным и знакомиться с ними, включая право на безвозмездное получение копий любой записи, содержащей персональные данные этого субъекта;

2) требовать от оператора уточнения, исключения или исправления неполных, неверных, устаревших, недостоверных, незаконно полученных или не являющих необходимыми для оператора персональных данных.

3) от оператора:

а) получать сведения о лицах, которые имеют доступ к персональным даннымили которым может быть предоставлен такой доступ;

б) получать перечень обрабатываемых персональных данных и источник их получения;

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

г) получать сведения о том, какие юридические последствия для субъекта ПДнможет повлечь за собой обработка его персональных данных;

д) требовать извещения Оператором всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях.

5.3. Передача информации третьим лицам и/или их представителям возможна только при письменном согласии субъекта ПДн.

6. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Меры по обеспечению безопасности персональных данных принимаются для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

6.2. Безопасность персональных данных при их обработке в информационной системе персональных данных оператора (институт) обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы, определенные в соответствии с частью 5 статьи 19 Федерального закона от 27.07.2006 №152-ФЗ«О персональных данных». Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах персональных данных оператора (институт).

6.3. Меры по обеспечению безопасности персональных данных реализуются в том числе посредством применения в информационных системах персональных данных оператора (институт) средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия, в случаях, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности персональных данных.

6.4. В ИСПДнинститута устанавливаются уровни защищенности персональных данных в зависимости от угроз безопасности этих данных в соответствии с «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утвержденными Постановлением Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

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

6.6. Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

6.7. Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

6.8. Защита персональных данных представляет собой жестко регламентированный и динамически технологический процесс,

предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе профессиональной и управленческой деятельности института.

6.9. Защита персональных данных от неправомерного их использования или утраты должна быть обеспечена оператором (институтом) за счет собственных средств в порядке, установленном Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных»:

1) субъекты и/или их законные представители должны быть ознакомлены под подпись с документами оператора (институт), устанавливающими порядок обработки и защиты персональных данных, а также об их правах и обязанностях в этой области;

2) во всех случаях отказ субъекта ПДнот своих прав на сохранение и защиту персональных данных недействителен;

3) все меры конфиденциальности при сборе, обработке и хранении персональных данных распространяются как на бумажные, так и на электронные (автоматизированные) носители информации;

4) информация о субъектах ПДн, зафиксированная в информационных системах персональных данных института и на бумажных носителях должна храниться в условиях, исключающих несанкционированный доступ к ней.

6.10. «Внутренняя защита»:

1) основным виновником несанкционированного доступа к персональным данным является, как правило, уполномоченное должностное лицо, работающее с документами и базами, содержащими персональные данные субъектовПДн. Регламентация доступа уполномоченного должностного лица к персональным данным, документам и информационным системам персональных данных института входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководителем и уполномоченными должностными лицами института.

2) для обеспечения внутренней защиты персональных данных субъектов ПДннеобходимо соблюдать ряд мер:

а) ограничение и регламентация состава уполномоченных должностных лиц, функциональные обязанности которых требуют конфиденциальных знаний;

б) строгое избирательное и обоснованное распределение документов и информации между уполномоченными должностными лицами;

в) рациональное размещение рабочих мест уполномоченных должностных лиц, при котором исключалось бы бесконтрольное использование защищаемой информации;

г) знание уполномоченным должностным лицом требований нормативно-методических документов по защите информации и сохранении тайны;

д) наличие необходимых условий в помещении для работы с конфиденциальными документами и информационными системами персональных данных института;

е) определение и регламентация состава уполномоченных должностных лиц, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника, на которой обрабатываются персональные данные субъектов ПДн;

ж) организация порядка уничтожения информации, содержащей персональные данные;

з) своевременное выявление нарушения требований разрешительной системы доступа уполномоченными должностными лицами;

и) воспитательная и разъяснительная работа с уполномоченными должностными лицами по предупреждению утраты ценных сведений при работе с конфиденциальными документами.

6.11. Безопасность персональных данных при их обработке в информационных системах персональных данных института обеспечивают ответственный за обеспечение безопасности персональных данных и администратор безопасности персональных данных.

6.12. «Внешняя защита»:

1) для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией, содержащей персональные данные. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

2) под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности института, посетители, работники других организационных структур. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в Учреждении;

3) для обеспечения внешней защиты персональных данных необходимо соблюдать ряд мер:

а) порядок приема, учета и контроля деятельности посетителей;

б) пропускной режим организации;

в) учет и порядок выдачи удостоверений;

г) технические средства охраны, сигнализации;

д) порядок охраны территории, зданий, помещений, транспортных средств;

е) требования к защите информации при интервьюировании и собеседованиях.

6.13. В институте организован режим обеспечения безопасности помещений, в которых размещены ИСПДн, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.

6.14. Все уполномоченные должностные лица, связанные с получением, обработкойи защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных.

6.15. По возможности персональные данные обезличиваются.

6.16. Кроме мер защиты персональных данных, установленных законодательством, работодатель и уполномоченные должностные лица, их представители могут вырабатывать совместные меры защиты персональных данных.

7. СОХРАНЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОБРАЗОВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

7.1. В целях информационного обеспечения управления в системе образования и государственной регламентации образовательной деятельности уполномоченными органами государственной власти Российской Федерации и органами государственной власти субъектов Российской Федерации создаются, формируются и ведутся государственные информационные системы, в том числе государственные информационные системы, предусмотренные Федеральным законом от 29.12.2012 №27Э-ФЗ «Об образовании в Российской Федерации». Ведение государственных информационных систем осуществляется в соответствии с едиными организационными, методологическими и программно-техническими принципами, обеспечивающими совместимость и взаимодействие этих информационных систем с иными государственными информационными системами и информационно-телекоммуникационными сетями, включая информационно-технологическую и коммуникационную инфраструктуры, используемые для предоставления государственных и муниципальных услуг, с

обеспечением конфиденциальности и безопасности содержащихся в них персональных данных и с соблюдением требований законодательства Российской Федерации о государственной или иной охраняемой законом тайне.

7.2. Институт гарантирует безопасность и конфиденциальность персональных данных, используемыхв целях информационного обеспечения проведения государственной итоговой аттестации и приемаобучающихся в ГБОУ ВО «ЮУрГИИим. П.И. Чайковского» для получения среднего профессионального, высшего, дополнительного профессионального образования и дополнительного образования детей.

7.3. При реализации образовательных программ с применением дистанционных образовательных технологий институт также обеспечивает защиту персональных данных.

7.4. При поступлении в институт обучающиеся предоставляют достоверные сведения. Институт вправе проверять достоверность предоставленных сведений.

8. ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ

8.1. При обработке персональных данных в ИСПДнинститута должно быть обеспечено:

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

2) своевременное обнаружение фактов несанкционированного доступа к персональным данным;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

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

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

6) постоянный контроль над обеспечением уровня защищенности персональных данных.

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

1) определение угроз безопасности персональных данных при их обработке в ИСПДн;

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

3) оценку эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию ИСПДн;

4) учет машинных носителей персональных данных;

5) установление правил доступа к персональным данным, обрабатываемым в ИСПДн, а также обеспечение регистрации и учета всех действий, совершаемых с персональными данными в ИСПДн;

6) контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности ИСПДн;

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

8.3. Осуществление мероприятий по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных института возлагается на администратора безопасности.

8.4. Список лиц, имеющих право доступа к персональным данным, уполномоченных на обработку этих данных и несущих ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты персональных данных, утверждается ректором. (Убрать п.5.1.)

8.5. Работники института, которым необходим доступ к персональным данным, обрабатываемым в информационных системах персональных данных института, для выполнения ими трудовых обязанностей, направляют письменный запрос на имя ректора института или уполномоченного должностного лица, который отвечает за обеспечение безопасности персональных данных, для получения доступа к ИСПДн института.

8.6. При обнаружении нарушений порядка предоставления персональных данных уполномоченное должностное лицо незамедлительно приостанавливает предоставление персональных данных пользователям (работникам) информационной системы персональных данных до выявления причин нарушения порядка предоставления персональных данных и устранения данных причин.

8.7. Оператор (институт) уведомляет Роскомнадзор о фактах, повлекших неправомерную передачу (предоставление, распространение, доступ) ПДн, повлекших нарушение прав субъектов ПДн.

8.8. Иные требования по обеспечению безопасности информации и средств защиты информации института выполняются в соответствии с требованиями органов исполнительной власти Российской Федерации и соответствующего субъекта Российской Федерации, органов местного самоуправления.

9. РЕГИСТРАЦИЯ СОБЫТИЙ БЕЗОПАСНОСТИ ИСПДн

9.1. В ИСПДнинститута подлежат регистрации следующие события:

1) вход (выход), а также попытки входа субъектов доступа в ИСПДн и загрузки (останова) операционной системы;

2) подключение машинных носителей информации и вывод информации на носители информации;

3) запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации;

4) попытки доступа программных средств к определяемым оператором защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей) и иным объектам доступа;

5) попытки удаленного доступа.

9.2. Сроки хранения событий безопасности определяются заданными настройками средств защиты информации от несанкционированного доступа.

9.3. Состав и содержание информации о событиях безопасности:

1) тип события;

2) дата и время события;

3) идентификационной информации источника события безопасности;

4) результат события безопасности (успешно или неуспешно);

5) субъект доступа (пользователь и (или) процесс), связанный с данным событием безопасности.

9.4. Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения предусматривает:

1) возможность выбора администратором безопасности событий безопасности, подлежащих регистрации в текущий момент времени: обеспечивается возможностями операционной системы и средств защиты информации от несанкционированного доступа;

2) генерацию (сбор, запись) записей регистрации (аудита) для событий безопасности, подлежащих регистрации (аудиту) в соответствии с п. 9.1

настоящего Положения с составом и содержанием информации, определенными в соответствии с п. 9.3 настоящего Положения.

3) хранение информации о событиях безопасности в течение времени, установленного в соответствии с п. 9.2 настоящего Положения.

9.5. Доступ к записям регистрации событий и функциям управления механизмами регистрации предоставляется только администратору безопасности и уполномоченным должностным лицам под контролем администратора безопасности.

10. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ОБРАБОТКУ И ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ

10.1. Должностные лица учреждения, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с федеральными законами и иными нормативными правовыми актами Российской Федерации.

10.2. Ректор института(оператор) за нарушение норм, регулирующих получение, обработку и защиту персональных данных субъектов, несет административную ответственность согласно статьям 5.27 и 5.39 Кодекса об административных правонарушениях Российской Федерации, а также возмещает субъекту ущерб, причиненный неправомерным использованием информации, содержащей персональные данные этого субъекта.

РАЗРАБОТАНО:

Начальник СИ		А.А. Сериков
должность	подпись	расшифровка подписи

СОГЛАСОВАНО:

Проректор по АХР		П.П. Сундарев
должность	подпись	расшифровка подписи
Начальник ОУП		Е.А. Соломатова
должность	подпись	расшифровка подписи

Приложение №1 к Положению
об обработке и защите персональных
данных в ГБОУ ВО «ЮУрГИИ
им. П. И. Чайковского»
и в информационных системах
персональных данных
ГБОУ ВО «ЮУрГИИ
им. П.И. Чайковского»

ЛИСТ ОЗНАКОМЛЕНИЯ К ПОЛОЖЕНИЮ
об обработке и защите персональных данных в ГБОУ ВО «ЮУрГИИ
им. П. И. Чайковского» и в информационных системах персональных данных
ГБОУ ВО «ЮУрГИИ им. П.И. Чайковского»

Дата ознакомления	**ФИО работника, ознакомившегося с документом**	**Должность работника, ознакомившегося с документом**	**Подпись работника, ознакомившегося с документом**
