**БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ**

 **ХАНТЫ-МАНСИЙСКОГО АВТОНОМНОГО ОКРУГА - ЮГРЫ**

 **«СУРГУТСКИЙ МУЗЫКАЛЬНЫЙ КОЛЛЕДЖ»**

Утверждено:

Директором

БУ «Сургутский музыкальный колледж»

приказом от 07 мая 2019г. № 09/01-ОД-151

С изменениями:

Утверждено:

Директором

БУ «Сургутский музыкальный колледж»

приказом от 28 июня 2019г. № 09/01-ОД-195

С изменениями:

Утверждено:

Директором

БУ «Сургутский музыкальный колледж»

приказом от 27 ноября 2020г. № 09/01-ОД-395

**Положение об обработке и защите персональных данных**

**в БУ «Сургутский музыкальный колледж»**

г. Сургут, 2020

1. **Общие положения**

1.1. Положение об обработке и защите персональных данных в БУ «Сургутский музыкальный колледж» (далее — Положение) определяет цели сбора персональных данных, объем и категории обрабатываемых персональных данных, категории субъектов персональных данных, порядок и условия обработки персональных данных, принимаемые меры к защите персональных данных.

1.2. В настоящем Положении используются следующие основные понятия:

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

- **биометрические персональные данные** - сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных;

- **Оператор** - БУ «Сургутский музыкальный колледж», 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;

- **обработка персональных данных** - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

- **автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники;

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

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

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

- **уничтожение персональных данных** - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

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

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

 1.3. **Конфиденциальность персональных данных** - Оператор и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено действующим законодательством Российской Федерации.

 1.4. Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - Федеральный закон № 152-ФЗ) и принятыми в соответствии с ним нормативными правовыми актами.

1.5. Оператор вправе:

- предоставлять персональные данные субъектов персональных данных третьим лицам, если это предусмотрено действующим законодательством Российской Федерации (правоохранительные, налоговые органы и др.);

- отказывать в предоставлении персональных данных в случаях, предусмотренных законодательством Российской Федерации;

- использовать персональные данные субъекта персональных данных без его согласия, в случаях, предусмотренных законодательством Российской Федерации.

1.6. Субъект персональных данных имеет право:

- на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

а) подтверждение факта обработки персональных данных Оператором;

б) правовые основания и цели обработки персональных данных;

в) цели и применяемые Оператором способы обработки персональных данных;

г) наименование и место нахождения Оператора, сведения о лицах (за исключением работников Оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Оператором или на основании федерального закона;

д) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

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

ж) порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом № 152-ФЗ;

з) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

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

к) иные сведения, предусмотренные Федеральным законом № 152-ФЗ или другими федеральными законами.

- требовать от Оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав,

- на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке;

- иные права, определенные Федеральным законом № 152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами.

1.7. Положение распространяется на персональные данные, полученные как до, так и после подписания настоящего Положения.

1**.8. В случае наличия противоречий между условиями настоящего Положения и требованиями действующего законодательства Российской Федерации к обработке и защите персональных данных, то применению подлежат требования действующего законодательства Российской Федерации.**

**1.9. Во всем, что не нашло отражения в настоящем Положении в отношении обработки и защиты персональных данных, Оператор руководствуется требованиями действующего законодательства Российской Федерации к обработке и защите персональных данных.**

2. **Цели обработки персональных данных**

2.1. Обработка и защита персональных данных осуществляется Оператором в целях:

- осуществления и выполнения возложенных законодательством Российской Федерации на Оператора функций, полномочий и обязанностей, в частности:

а) выполнение требований законодательства в сфере труда и налогообложения;

б) ведение бухгалтерского и налогового учета, формирование, изготовление и своевременная подача бухгалтерской, налоговой и статистической отчетности;

- выполнения требований законодательства Российской Федерации по определению порядка обработки и защиты персональных данных граждан, являющихся контрагентами Оператора, посетителей сайта Оператора;

- реализации прав и законных интересов Оператора в рамках осуществления видов деятельности, предусмотренных Уставом и иными локальными нормативными актами Оператора, либо достижения общественно значимых целей;

- обеспечения комплексной безопасности на объектах Оператора, организации контрольно-пропускного режима, контроля и учета рабочего времени;

- в иных законных целях.

3. **Правовое основание обработки персональных данных**

3.1. Правовым основанием обработки Оператором персональных данных являются:

- Трудовой кодекс Российской Федерации;

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

- Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;

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

- иные федеральные законы и принятые на их основе нормативные правовые акты, регулирующие отношения, связанные с деятельностью Оператора;

- заключаемые Оператором договоры гражданско-правового характера;

- согласие на обработку персональных данных.

4. **Объем и категории обрабатываемых персональных данных, категории субъектов персональных данных**

4.1. Оператором обрабатываются персональные данные следующих категорий субъектов персональных данных:

- работники, лица, ранее состоявшие в трудовых отношениях с Оператором, соискатели на замещение вакантных должностей, члены их семей и близкие родственники;

- абитуриенты, обучающиеся, выпускники, отчисленные студенты, их законные представители;

- физические лица по договорам гражданско-правового характера;

- физические лица, являющиеся работниками, представителями контрагентов (юридических лиц) по договорам гражданско-правового характера;

- физические лица, являющиеся стороной в гражданском судопроизводстве;

- физические лица – посетители сайта Оператора,

- физические лица – посетители БУ «Сургутский музыкальный колледж».

4.2. При реализации трудовых правоотношений Оператор осуществляет обработку следующих персональных данных:

- фамилия, имя, отчество (последнее - при наличии), в том числе прежние фамилии, имена, отчества (последнее - при наличии), в случае их изменения;

- число, месяц, год рождения;

- место рождения;

- сведения о гражданстве (в том числе прежние гражданства, иные гражданства);

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

- адрес и дата регистрации по месту жительства (месту пребывания), адрес фактического проживания;

- номер контактного телефона или сведения о других способах связи;

- реквизиты страхового свидетельства обязательного пенсионного страхования;

- идентификационный номер налогоплательщика;

- реквизиты полиса обязательного медицинского страхования;

- реквизиты свидетельства о государственной регистрации актов гражданского состояния;

- сведения о трудовом и общем стаже работника;

- сведения о воинском учете и реквизиты документов воинского учета;

- сведения об образовании и (или) о квалификации, обучении;

- сведения об ученой степени, ученом звании;

- сведения о владении иностранными языками, уровень владения;

- фотографии;

- видеоизображения;

- сведения, содержащиеся в трудовом договоре, дополнительных соглашениях к трудовому договору;

- сведения о наличии или отсутствии судимости;

- сведения о государственных наградах, иных наградах и знаках отличия (кем награжден и когда);

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

- сведения о ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения денежного содержания;

- номер расчетного (лицевого) счета;

- номер банковской карты;

- сведения о степени родства, фамилии, имени, отчестве, дате рождения близких родственников (отца, матери, братьев, сестер и детей), а также мужа (жены);

- сведения о месте рождения, месте работы и адресе фактического проживания близких родственников работника (отца, матери, братьев, сестер и детей), а также мужа (жены), номера их контактных телефонов или сведения о других способах связи;

- сведения о заработной плате работников, сведения о социальных льготах,

- результаты обязательных предварительных (при поступлении на работу) и периодических медицинских осмотров (обследований), сведения о прививках, а также психиатрического освидетельствования;

- сведения о специальности работника, занимаемой должности, подлинники и копии приказов по личному составу, личные дела и трудовые книжки работников, основания к приказам по личному составу, дела, содержащие материалы по повышению квалификации и переподготовке работников, их аттестации, служебным расследованиям; копии отчетов, направляемых в органы статистики; рекомендации, характеристики, другие документы и сведения, нахождение которых в личном деле будет признано целесообразным;

- биометрические персональные данные (дактилоскопические – отпечатки пальцев) для идентификации в комплексной информационно-сервисной системе биометрической идентификации «Школьное окно»).

4.3. Оператором создаются и хранятся следующие группы документов, содержащие данные о работниках Оператора, в единичном или сводном виде:

- документы, содержащие персональные данные работников (комплексы документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении; комплекс материалов по анкетированию, тестированию; проведению собеседований с кандидатом на должность; подлинники и копии приказов по личному составу; личные дела и трудовые книжки работников; дела, содержащие основания к приказу по личному составу; дела, содержащие материалы аттестации работников; служебных расследований; справочно-информационный банк данных по персоналу (картотеки, журналы); подлинники и копии отчетных, аналитических и справочных материалов, передаваемых Оператору, копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения);

- документация по организации работы (положения, должностные инструкции работников, приказы, распоряжения); документы по планированию, учету, анализу и отчетности в части работы с персоналом Оператора.

4.4. В отношении абитуриентов, обучающихся, выпускников, отчисленных студентов, Оператор осуществляет обработку следующих персональных данных при реализации образовательных правоотношений:

- фамилия, имя, отчество (последнее - при наличии), в том числе прежние фамилии, имена, отчества (последнее - при наличии), в случае их изменения;

- число, месяц, год рождения;

- место рождения;

- сведения о гражданстве (в том числе прежние гражданства, иные гражданства);

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

- адрес и дата регистрации по месту жительства (месту пребывания), адрес фактического проживания;

- номер контактного телефона или сведения о других способах связи;

- сведения о воинском учете и реквизиты документов воинского учета;

- сведения об образовании;

- фотографии;

- видеоизображения;

- сведения о состоянии здоровья, результаты медицинских осмотров (обследований);

- иные персональные данные, обработка которых потребуется Оператору в соответствии с законодательством Российской Федерации, регулирующим отношения, связанные с деятельностью Оператора;

- биометрические персональные данные (дактилоскопические – отпечатки пальцев) совершеннолетних субъектов персональных данных для идентификации в комплексной информационно-сервисной системе биометрической идентификации «Школьное окно»).

4.5. В отношении законных представителей абитуриентов, обучающихся, выпускников, отчисленных студентов, Оператор осуществляет обработку следующих персональных данных при реализации образовательных правоотношений:

- фамилия, имя, отчество (последнее - при наличии), в том числе прежние фамилии, имена, отчества (последнее - при наличии), в случае их изменения;

- число, месяц, год рождения;

- сведения о гражданстве (в том числе прежние гражданства, иные гражданства);

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

- адрес и дата регистрации по месту жительства (месту пребывания), адрес фактического проживания;

- номер контактного телефона или сведения о других способах связи;

- сведения о месте работы;

- сведения о составе семьи, о материальной обеспеченности семьи, при решении вопросов о выделении материальной помощи студентам;

- иные персональные данные, обработка которых потребуется Оператору в соответствии с законодательством Российской Федерации, регулирующим отношения, связанные с деятельностью Оператора.

4.6. При взаимодействии Оператора с физическими лицами по договорам гражданско-правового характера, физическими лицами являющимися работниками, представителями контрагентов (юридических лиц) по договорам гражданско-правового характера, Оператор осуществляет обработку следующих персональных данных:

- фамилия, имя, отчество (последнее - при наличии), в том числе прежние фамилии, имена, отчества (последнее - при наличии), в случае их изменения;

- число, месяц, год рождения;

- сведения о гражданстве (в том числе прежние гражданства, иные гражданства);

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

- адрес и дата регистрации по месту жительства (месту пребывания), адрес фактического проживания;

- номер контактного телефона или сведения о других способах связи;

- реквизиты страхового свидетельства обязательного пенсионного страхования;

- идентификационный номер налогоплательщика;

- сведения об образовании и (или) о квалификации необходимые для выполнения работ, оказания услуг по договорам гражданско-правового характера, требующих наличия специальных знаний или специальной подготовки;

- фотографии;

- видеоизображения;

- сведения о вознаграждении,

- иные персональные данные, обработка которых потребуется Оператору в соответствии с законодательством Российской Федерации, регулирующим отношения, связанные с деятельностью Оператора.

4.7. В отношении физических лиц, являющихся стороной в гражданском судопроизводстве, Оператор осуществляет обработку тех персональных данных, которые потребуется Оператору в соответствии с законодательством Российской Федерации.

4.8. В отношении физических лиц – посетителей сайта Оператора, Оператор осуществляет обработку следующих персональных данных: фамилия, имя, отчество, адрес электронной почты, номер телефона.

4.9. Оператор не осуществляет обработку персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни субъектов персональных данных.

5. **Порядок и условия обработки персональных данных**

5.1. Оператор осуществляет сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление и уничтожение персональных данных.

Обработка персональных данных осуществляется Оператором с соблюдением принципов и правил, предусмотренных Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных».

5.2. Обработка персональных данных осуществляется с согласия субъекта персональных данных, за исключением случаев, предусмотренных действующим законодательством Российской Федерации.

Письменное согласие субъектов на обработку своих персональных данных должно включать в себя, в частности, сведения, указанные в ч. 4 ст. 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

Согласие субъектов на обработку персональных данных составляется по типовой форме, согласно **приложению №1 к Положению**.

Согласие работника на обработку персональных данных получают начальник отдела кадров и документационного обеспечения управления, специалист по документационному обеспечению персонала получают от работника на этапе приема на работу. Сведения о персональных данных работника начальник отдела кадров и документационного обеспечения управления, специалист по документационному обеспечению персонала получают из следующих документов: паспорт, трудовая книжка, страховое свидетельство государственного пенсионного страхования, документы воинского учета, документ об образовании, о квалификации или наличии специальных знаний, анкета, заполняемая работником при приеме на работу. Биометрические персональные данные (дактилоскопические – отпечатки пальцев) для использования в комплексной информационно-сервисной системе биометрической идентификации «Школьное окно» получает системный администратор после письменного согласия работника.

Согласие на обработку персональных данных абитуриентов, обучающихся, выпускников, отчисленных студентов, их законных представителей получают работники учебной части (специалист учебной части, методист). Сведения о персональных данных абитуриентов, обучающихся, выпускников, отчисленных студентов, их законных представителей работники учебной части получают из следующих документов: паспорт, документ об образовании, документы воинского учета, анкета, заполняемая абитуриентом, обучающимся при приеме на обучение, иные документы и сведения, предоставляемые абитуриентом, обучающимся при приеме на обучение и в процессе обучения. Биометрические персональные данные (дактилоскопические – отпечатки пальцев) совершеннолетних обучающихся для использования в комплексной информационно-сервисной системе биометрической идентификации «Школьное окно» получает системный администратор после письменного согласия совершеннолетнего обучающегося.

Согласие на обработку персональных данных субъектов – посетителей сайта Оператора, осуществляется путем нажатия кнопки «Даю согласие на обработку данных» под текстом: «При посещении сайта БУ «Сургутский музыкальный колледж» (Колледж) даю согласие на обработку (любое действие (операцию) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение (размещение на сайте Колледжа), предоставление, доступ), обезличивание, блокирование, удаление, уничтожение) своих персональных данных (фамилия, имя, отчество, адрес электронной почты, номер телефона), даю согласие на обработку файлов cookie, пользовательских данных (сведения о местоположении; тип и версия ОС; тип и версия браузера; тип устройства и разрешение его экрана; источник: откуда пришел на сайт пользователь; с какого сайта или по какой рекламе; язык ОС и браузера; какие страницы открывает и на какие кнопки нажимает пользователь; ip-адрес) в целях функционирования сайта, проведения ретаргетинга и проведения статистических исследований и обзоров. В случае отказа от обработки данных я проинформирован о необходимости прекратить использование сайта или отключить файлы cookie в настройках браузера [(требование ФЗ №152. Статья 9 «Согласие субъекта персональных данных на обработку его персональных данных»)](http://www.consultant.ru/document/cons_doc_LAW_61801/6c94959bc017ac80140621762d2ac59f6006b08c/).

5.3. Оператор обязан не допускать обработку персональных данных, не совместимую с целями сбора персональных данных. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей.

5.4. При обработке персональных данных Оператор обязан не допускать объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

5.5. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных.

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

5.7. Сбор и уточнение персональных данных осуществляются путем:

- получения оригиналов необходимых документов;

- копирования оригиналов документов;

- получение персональных данных через сайт Оператора, информационные системы;

- внесения сведений в учетные формы (на бумажных и электронных (машинных) носителях);

- внесения персональных данных в информационные системы.

Сбор персональных данных осуществляется путем получения их непосредственно от субъекта персональных данных.

В случае возникновения необходимости получения персональных данных у третьей стороны следует заранее известить об этом субъекта персональных данных, получить его письменное согласие и сообщить о целях, предполагаемых источниках и способах получения персональных данных (за исключением случаев, установленных действующим законодательством Российской Федерации).

Согласие субъекта на получение его персональных данных у третьей стороны составляется по типовой форме, согласно **приложению № 2 к Положению**.

При сборе персональных данных, лицо осуществляющее сбор персональных данных, обязано разъяснить субъектам персональных данных юридические последствия отказа предоставить их персональные данные.

Типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные Оператору приведена **в приложении №3 к Положению**.

5.8. Сроки обработки персональных данных определяются в соответствии с законодательством Российской Федерации.

5.9. При обработке персональных данных, осуществляемой без использования средств автоматизации, выполняются требования, установленные действующим законодательством Российской Федерации.

Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации, если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Обработка персональных данных без использования средств автоматизации осуществляется как на бумажных носителях, так и в электронном виде на материальных носителях информации.

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

При использовании форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, должны соблюдаться следующие условия:

- форма документа 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;

- форма документа 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;

- форма документа 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;

- форма документа должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

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.

5.10. При передаче персональных данных субъектов, должностные лица Оператора, владеющие персональными данными в силу своих должностных обязанностей должны соблюдать следующие требования:

- не сообщать персональные данные третьей стороне без письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью физического лица, а также в других случаях, предусмотренных законодательством Российской Федерации;

- персональные данные могут быть использованы лишь в целях, для которых они сообщены, должностные лица осуществляющие обработку персональных данных несут персональную ответственность за соблюдение требований законодательства Российской Федерации при обработке персональных данных. Лица, получающие персональные данные, обязаны соблюдать режим секретности (конфиденциальности персональных данных);

5.11. По мотивированному запросу исключительно для выполнения возложенных законодательством функций и полномочий персональные данные субъекта персональных данных без его согласия могут быть переданы:

- в судебные органы в связи с осуществлением правосудия;

- в органы федеральной службы безопасности;

- в органы прокуратуры;

- в органы полиции;

- в иные органы и организации в случаях, установленных нормативными правовыми актами Российской Федерации, обязательными для исполнения.

Сведения о субъекте персональных данных могут быть предоставлены другой организации только с письменного запроса на бланке организации с приложением письменного разрешения самого субъекта персональных данных.

Персональные данные субъекта могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого субъекта персональных данных.

Внешний доступ к персональным данным работников, обучающихся имеют контрольно-ревизионные органы при наличии документов, на основании которых они проводят проверку. Дистанционно персональные данные работников, обучающихся, могут быть представлены контрольно-надзорным органам только по письменному запросу и по защищенным каналам связи.

5.12. В целях обеспечения антитеррористических мер защищённости здания Оператора, профилактики нарушений правил внутреннего распорядка, в здании Оператора установлена система видеонаблюдения. В местах осуществления видеосъемки размещена информация о возможной фото-, видеосъемке соответствующими текстовыми и/или графическими предупреждениями.

5.13. Для однократного пропуска субъекта персональных данных на территорию, на которой находится Оператор, или в иных аналогичных целях, ведутся журналы, в которых заносятся следующие персональные данные посетителей:

- фамилия, имя, отчество (последнее - при наличии);

- вид, серия, номер документа, удостоверяющего личность, дата выдачи, наименование органа, выдавшего его.

Необходимость ведения такого журнала связана с обеспечением мер безопасности и антитеррористической защищённости в зданиях, находящихся у Оператора на праве оперативного управления.

Ответственным за ведение и сохранность журнала в общежитии Оператора является старший воспитатель.

Ответственным за ведение и сохранность журнала в здании Оператора является заведующий хозяйством.

Копирование содержащейся в таких журналах информации не допускается.

Персональные данные каждого субъекта персональных заносятся в такой журнал не более одного раза в каждом случае пропуска субъекта персональных данных на территорию Оператора.

5.14. Оператор прекращает обработку персональных данных в следующих случаях:

– достигнуты цели обработки персональных данных;

– истек срок действия согласия на обработку персональных данных;

– отозвано согласие на обработку персональных данных;

– обработка персональных данных неправомерна.

5.15. Сбор, защита и обработка персональных данных и файлов «cookie» на сайте Оператора <https://surgutmusic.ru> (далее – сайт).

5.15.1. Посещая сайт Оператора или просматривая его содержимое, пользователь подтверждает, что прочитал, полностью уяснил и принимает без ограничений или оговорок политику в отношении управления персональными данными и файлами «cookie», главной целью которой является доведение до пользователя информации о правах и свободах, которые он может реализовать в отношении использования сайтом его персональных данных, а также о средствах, используемых сайтом для защиты этих данных.

5.15.2. Оставляя свои данные на сайте путем заполнения полей онлайн-форм, при регистрации на страницах сайта или в любом другом разделе сайта,
пользователь:

подтверждает, что указанные им персональные данные принадлежат лично ему;

признает и подтверждает, что внимательно и в полном объеме ознакомился с условиями обработки персональных данных, указываемых пользователем в соответствующих полях при использовании на сайте, и дальнейшем их использовании;

признает и подтверждает, что все положения и условия обработки персональных данных пользователю понятны;

дает согласие на обработку сайтом предоставленных персональных данных в целях регистрации на сайте, получения доступа к сайту и дополнительному функционалу сайта и подтверждает, что действует свободно, по своей воле и в своих интересах, согласен с условиями обработки персональных данных в соответствии с требованиями Федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных» без каких-либо оговорок и ограничений.

5.15.3. Оператор является контроллером данных, отвечающим за обработку и защиту персональных данных, использующихся с целью управления работой сайта. Указанные операции по обработке персональных данных осуществляются в соответствии с действующим законодательством.

5.15.4. Управление файлами «Cookie».

«Сookie» являются файлами, позволяющими сайту сохранять информацию относительно просмотра данных сайта с компьютера пользователя (количество посещений, количество просмотренных станиц и т.д.) с целью сделать посещения сайта более удобными и бесперебойными.

Пользователь может удалить файлы «cookie», хранящиеся на его компьютере, в любой момент, запретить сохранение новых файлов «cookie», либо получать уведомление перед сохранением новых файлов «cookie» путем изменения настроек браузера.

Файлы «cookie» используются для улучшения качества взаимодействия пользователя с сайтом, позволяя «запоминать» посетителей на время их первого или во время повторных посещений. Оператор использует файлы «cookie», которые необходимы для перемещения посетителей по сайту или работы определенных основных функций (за счет сохранения настроек пользователя).

Файлы «cookie», которые могут сохраняться на сервере пользователя при просмотре сайта, являются файлами, предназначенными исключительно для обеспечения или поддержания электронных коммуникаций или необходимыми для предоставления запрошенной услуги (имя учетной записи и т.д.), статистическими файлами «cookie» или другими файлами «cookie», в зависимости от условий, приведенных ниже:

|  |  |  |
| --- | --- | --- |
| **Название** | **Описание** | **Период** |
| BITRIX\_CONVERSION\_CONTEXT\_s1 | Используется для целей внутренней аналитики | ~1 год |
| BITRIX\_SM\_GUEST\_ID | Хранит информацию об уникальном идентификаторе авторизированного пользователя сайта | ~1 год |
| BITRIX\_SM\_LAST\_SETTINGS | Устанавливается системой управления сайтом для корректной работы сервисов на сайте | до закрытия браузера |
| BITRIX\_SM\_LAST\_VISIT | Хранит время последнего посещения пользователем сайта | ~1 год |
| BITRIX\_SM\_LOGIN | Хранит информацию о логине пользователя сайта | ~1 год |
| BITRIX\_SM\_SOUND\_LOGIN\_PLAYED | Звук при авторизации пользователя (да или нет) | до закрытия браузера |
| BITRIX\_SM\_menumode | Хранит информацию о навигации по сайту | ~5 лет |
| BX\_USER\_ID | Хранит информацию об уникальном идентификаторе неавторизированного пользователя сайта | ~10 лет |
| COOKIE\_AGREEMENT | Хранит информацию о согласии на обработку файлов cookies | ~1 год |
| PHPSESSID | Хранит информацию об уникальном идентификаторе сессии пользователя сайта | до закрытия браузера |
| \_ym\_d | Сохраняет дату начала работы с сайтом | ~1 год |
| \_ym\_isad | Используется для определения, установлен ли у пользователя блок от рекламы | ~1 день |
| \_ym\_uid | Позволяет различать пользователей | ~1 год |
| sputnik\_session | Используются для отслеживания поведения пользователей на сайте | ~1 час |

Сайт может собирать следующие данные:

источник захода на сайт и информация поискового или рекламного запроса;

данные о пользовательском устройстве (среди которых разрешение, версия и другие атрибуты, характеризующие пользовательское устройство);

пользовательские клики, просмотры страниц, заполнения полей, показы и просмотры баннеров и видео;

данные, характеризующие аудиторные сегменты;

параметры сессии;

данные о времени посещения;

идентификатор пользователя, хранимый в cookie.

Статистические сookie-файлы используются для измерения количества посещений, количества просмотренных страниц, активности пользователей на сайте и количества возвращений пользователей на сайте. Используемый статистический инструмент генерирует сookie-файл с уникальным идентификатором, который хранится не дольше выше указанного периода. IP-адрес пользователя анонимизируется сразу после обработки, поэтому никто не сможет определить пользователя как реально существующее лицо. Статистические данные по посещениям сайта собираются рассматриваемым провайдером телекоммуникационных услуг и в последующем передаются Оператору в статистической и анонимизированной форме через веб-интерфейс, к которому имеет доступ только Оператор. Собранные данные не передаются третьим сторонам и не используются в целях, отличающихся от указанных выше. Пользователь можете заблокировать cookie-файлы в любое время, отказавшись от их использования.

Раздел помощи каждого браузера предоставляет инструкции о том, как отказаться от использования cookie-файлов или получать уведомления об их установке или как их деактивировать. Ниже приведены наиболее часто используемые браузеры:

|  |  |
| --- | --- |
| **Браузер** | **Ссылка на раздел «Помощь»** |
| Internet Explorer™ | <https://support.microsoft.com/ru-ru/topic/%D1%83%D0%B4%D0%B0%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5-%D1%84%D0%B0%D0%B9%D0%BB%D0%BE%D0%B2-cookie-%D0%B8-%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5-%D0%B8%D0%BC%D0%B8-168dab11-0753-043d-7c16-ede5947fc64d> |
| Safari™ | <http://support.apple.com/kb/PH5042> |
| Chrome™ | <https://support.google.com/chrome/answer/95647?hl=ru&hlrm=en> |
| Firefox™ | <https://support.mozilla.org/ru/kb/blokirovanie-veb-sajtov-ot-hraneniya-nastroek-sajt> |
| Opera™ | <https://help.opera.com/ru/latest/web-preferences/> |

5.15.5. Сайт может содержать ссылки на другие сайты, находящиеся вне контроля Оператора и вне действия настоящего Положения. Операторы этих сайтов могут собирать информацию о посетителях и использовать ее в соответствии с их политикой, которая может отличаться от настоящего Положения.

5.15.6. Оператор сайта не несет ответственности за использование (как правомерное, так и неправомерное) третьими лицами информации, размещенной пользователем на сайте, включая её воспроизведение и распространение, осуществленные всеми возможными способами

**6. Доступ к персональным данным**

6.1. Право доступа к персональным данным обрабатываемым Оператором имеют работники Оператора исключительно в объеме, необходимом для выполнения своих должностных обязанностей.

 6.2. Список должностей (подразделений) работников Оператора обрабатывающих персональные данные без использования средств автоматизации:

| **Подразделение/ должность** | **Обрабатываемые персональные данные**  |
| --- | --- |
| Директор,заместитель директора по учебной работе,заместитель директора по воспитательной работе,заместитель директора по административно-хозяйственной деятельности | Персональные данные: - работников, лиц, ранее состоявших в трудовых отношениях с Оператором, соискателей на замещение вакантных должностей, членов их семей и близких родственников;- абитуриентов, обучающихся, выпускников, отчисленных студентов, их законных представителей; - физических лиц по договорам гражданско-правового характера; - физических лиц, являющихся работниками, представителями контрагентов (юридических лиц) по договорам гражданско-правового характера;- физических лиц, являющихся стороной в гражданском судопроизводстве;- физических лиц – посетителей сайта Оператора,- физических лиц – посетителей Оператора |
| Работники финансово экономической службы:- главный бухгалтер, - заместитель главного бухгалтера, - бухгалтеры, - главный экономист | Персональные данные: - работников, лиц, ранее состоявших в трудовых отношениях с Оператором, соискателей на замещение вакантных должностей, членов их семей и близких родственников;- абитуриентов, обучающихся, выпускников, отчисленных студентов, их законных представителей; - физических лиц по договорам гражданско-правового характера; - физических лиц, являющихся работниками, представителями контрагентов (юридических лиц) по договорам гражданско-правового характера;- физических лиц, являющихся стороной в гражданском судопроизводстве |
| Работники отдела кадров и документационного обеспечения управления: - начальник отдела кадров и документационного обеспечения управления, - специалист по документационному обеспечению персонала, - документовед, - секретарь руководителя | Персональные данные: - работников, лиц, ранее состоявших в трудовых отношениях с Оператором, соискателей на замещение вакантных должностей, членов их семей и близких родственников;- физических лиц по договорам гражданско-правового характера |
| Работники юридического отдела:- начальник юридического отдела, - юрисконсульт, - специалист по закупкам | Персональные данные: - работников, лиц, ранее состоявших в трудовых отношениях с Оператором, соискателей на замещение вакантных должностей, членов их семей и близких родственников;- абитуриентов, обучающихся, выпускников, отчисленных студентов, их законных представителей; - физических лиц по договорам гражданско-правового характера; - физических лиц, являющихся работниками, представителями контрагентов (юридических лиц) по договорам гражданско-правового характера;- физических лиц, являющихся стороной в гражданском судопроизводстве |
| Работники музыкального отделения: - преподаватели, - концертмейстеры, - заведующие производственной практикой | Персональные данные: - абитуриентов, обучающихся, выпускников, отчисленных студентов, их законных представителей |
| Работники учебной части:- специалист учебной части, - методист | Персональные данные: - абитуриентов, обучающихся, выпускников, отчисленных студентов, их законных представителей |
| Работники методической и информационно-аналитической службы:- начальник методической и информационно-аналитической службы, - заместитель начальника методической и информационно-аналитической службы,- методист, - фонотекарь,  | Персональные данные: - работников, лиц, ранее состоявших в трудовых отношениях с Оператором, соискателей на замещение вакантных должностей, членов их семей и близких родственников;- абитуриентов, обучающихся, выпускников, отчисленных студентов, их законных представителей; - физических лиц по договорам гражданско-правового характера; - физических лиц, являющихся работниками, представителями контрагентов (юридических лиц) по договорам гражданско-правового характера;- физических лиц, являющихся стороной в гражданском судопроизводстве;- физических лиц – посетителей сайта Оператора |
| Работники методической и информационно-аналитической службы:- специалист по связям с общественностью | Персональные данные: - работников, лиц, ранее состоявших в трудовых отношениях с Оператором, соискателей на замещение вакантных должностей, членов их семей и близких родственников;- абитуриентов, обучающихся, выпускников, отчисленных студентов, их законных представителей; - физических лиц – посетителей сайта Оператора |
| Работники методической и информационно-аналитической службы:- заведующий библиотекой, - библиотекарь | Персональные данные: - работников, лиц, ранее состоявших в трудовых отношениях с Оператором, соискателей на замещение вакантных должностей, членов их семей и близких родственников;- абитуриентов, обучающихся, выпускников, отчисленных студентов |
| Работники службы психолого-педагогического сопровождения обучающихся:- социальный педагог, - педагог-психолог,  | Персональные данные: - абитуриентов, обучающихся, выпускников, отчисленных студентов, их законных представителей;  |
| Работники службы психолого-педагогического сопровождения обучающихся:- старший воспитатель, - воспитатель | Персональные данные: - абитуриентов, обучающихся, выпускников, отчисленных студентов, их законных представителей; - посетителей общежития |
| - Системный администратор  | Персональные данные: - работников, лиц, ранее состоявших в трудовых отношениях с Оператором, соискателей на замещение вакантных должностей, членов их семей и близких родственников;- абитуриентов, обучающихся, выпускников, отчисленных студентов, их законных представителей; - физических лиц по договорам гражданско-правового характера; - физических лиц, являющихся работниками, представителями контрагентов (юридических лиц) по договорам гражданско-правового характера;- физических лиц, являющихся стороной в гражданском судопроизводстве;- физических лиц – посетителей сайта Оператора,- физических лиц – посетителей Оператора |
| Заведующий хозяйством | Персональные данные посетителей здания Оператора |
| Специалист по охране труда | Персональные данные: - работников, лиц, ранее состоявших в трудовых отношениях с Оператором, соискателей на замещение вакантных должностей, членов их семей и близких родственников;- абитуриентов, обучающихся, выпускников, отчисленных студентов, их законных представителей,- физических лиц, являющихся работниками, представителями контрагентов (юридических лиц) по договорам гражданско-правового характера |

Список должностей (подразделений) работников Оператора обрабатывающих персональные данные с использованием средств автоматизации:

| **Подразделение/ должность** | **Обрабатываемые персональные данные**  |
| --- | --- |
| - Системный администратор  | Персональные данные: - работников, лиц, ранее состоявших в трудовых отношениях с Оператором;- обучающихся, отчисленных обучающихся. |

6.3. Права и обязанности работников Оператора, обрабатывающих персональные данные без использования средств автоматизации устанавливаются:

- в Инструкции должностных лиц Оператора, обрабатывающих персональные данные без использования средств автоматизации (**приложение № 5 к Положению**);

- в Инструкции пользователя персональных данных по обеспечению безопасности обработки персональных данных при возникновении внештатных ситуаций (**приложение № 6 к Положению**), ознакомление с которыми работники Оператора осуществляют под роспись.

6.4. От работников, участвующих в обработке персональных данных, работниками отдела кадров и документационного обеспечения управления берутся письменные обязательства о неразглашении конфиденциальной информации о персональных данных субъектов.

Типовая форма обязательства лица непосредственно осуществляющего обработку персональных данных о неразглашении конфиденциальной информации о персональных данных субъектов приведена **в приложении № 4 к Положению**.

6.5. Оператор осуществляет обработку персональных данных в следующих информационных системах:

- «1С: Предприятие 8.3»;

- «1С: КолледжПроф»;

- УРМ АС «Бюджет»;

- «ФИС ГИА и прием»;

- «Контур-экстерн»;

- программа «Spu-orb»;

- программа «Перечень льготных профессий организации»;

- «Кибер – диплом»;

- информационные системы по зарплатным проектам с ПАО Сбербанк и ПАО Банк «ФК Открытие»;

- программная система «SONDA Школьное окно»;

- «Дело-WEB»;

- сайт «zakupki.gov.ru»;

- сайт ГИС «Государственный заказ»;

- сайт БУ «Сургутский музыкальный колледж».

6.6. Доступ к информационным системам имеют:

- «1С: Предприятие 8.3»: главный бухгалтер, заместитель главного бухгалтера, бухгалтеры, главный экономист, начальник отдела кадров и документационного обеспечения управления, специалист по документационному обеспечению персонала, системный администратор;

- «1С: КолледжПроф»: специалист учебной части, системный администратор;

- «Контур-экстерн»: главный бухгалтер, заместитель главного бухгалтера, бухгалтеры, главный экономист, начальник отдела кадров и документационного обеспечения управления, специалист по документационному обеспечению персонала, системный администратор;

- программа «Spu-orb»: начальник отдела кадров и документационного обеспечения управления, специалист по документационному обеспечению персонала, системный администратор;

- «ФИС ГИА и прием»: заместитель директора по учебной работе, специалист учебной части, системный администратор;

- программа «Перечень льготных профессий организации»: начальник отдела кадров и документационного обеспечения управления, специалист по документационному обеспечению персонала, системный администратор;

- программная система «SONDA Школьное окно»: системный администратор;

- «Кибер – диплом»: работники учебной части (специалист учебной части, методист), системный администратор;

- информационные системы по зарплатным проектам с ПАО Сбербанк и ПАО Банк «ФК Открытие»: главный бухгалтер, заместитель главного бухгалтера, бухгалтеры, главный экономист, системный администратор;

- УРМ АС «Бюджет»: главный бухгалтер, заместитель главного бухгалтера, бухгалтеры, главный экономист, специалист по закупкам, системный администратор;

- «Дело-WEB»: директор, руководители, специалист по закупкам, работники отдела кадров и документационного обеспечения управления, системный администратор;

- сайт «zakupki.gov.ru»: юрисконсульт, специалист по закупкам, системный администратор;

- ГИС «Государственный заказ»: юрисконсульт, специалист по закупкам, системный администратор;

- сайт БУ «Сургутский музыкальный колледж» (электронный журнал успеваемости): заместитель директора по учебной работе, заместитель директора по воспитательной работе, преподаватели, концертмейстеры, заведующие производственной практикой, педагог-психолог;

- сайт БУ «Сургутский музыкальный колледж»: специалист по связям с общественностью.

Доступ пользователей к указанным информационным системам осуществляется с применением логинов и паролей.

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

6.7. Помещения, в которых хранятся персональные данные работников, обучающихся, оборудуются надежными замками, сейфами.

Нахождение в помещениях, в которых ведется обработка персональных данных лиц, не являющихся лицом, уполномоченным на обработку персональных данных, возможно только в присутствии лица, уполномоченного на обработку персональных данных, на время, ограниченное необходимостью решения вопросов, связанных с деятельностью Оператора, предоставлением персональных данных.

Список лиц ответственных за соблюдение порядка доступа в помещения, в которых ведется обработка персональных данных, утверждается приказом Оператора.

 Персональные компьютеры, в которых содержатся персональные данные субъектов, должны быть защищены паролями доступа.

Для исключения возможности бесконтрольного проникновения в помещения и к установленному в них оборудованию посторонних лиц, двери в отсутствие штатных сотрудников запираются на ключ, окна закрываются на запирающие устройства.

Оборудование в помещении должно размещаться таким образом, чтобы исключить возможность бесконтрольного доступа к нему посторонних лиц. Мониторы компьютеров должны быть ориентированы таким образом, чтобы исключить возможность просмотра отображаемой на них информации лицами, не имеющими допуска к обработке персональных данных.

 6.8. Список помещений, в которых ведется обработка персональных данных

|  |  |  |
| --- | --- | --- |
| № п/п | Наименование помещения | Адрес и место расположения |
| 1 | Финансово экономическая служба | город Сургут, улица Энтузиастов, дом 28, помещение № 101 |
| 2 | Отдел кадров и документационного обеспечения управления | город Сургут, улица Энтузиастов, дом 28, помещение № 213 |
| 3 | Юридический отдел | город Сургут, улица Энтузиастов, дом 28, помещение № 318,  |
| 4 | Музыкальное отделение | город Сургут, улица Энтузиастов, дом 28, помещения № 107, 109, 111, 112, 201, 202, 203, 204, 205, 209, 210, 211, 215, 216, 301, 302, 303, 304, 305, 306, 307, 308, 309, 310, 311, 312, 313, 314, 316, 317  |
| 5 | Учебная часть | город Сургут, улица Энтузиастов, дом 28, помещение № 102 |
| 6 | Методическая и информационно-аналитическая служба | город Сургут, улица Энтузиастов, дом 28, помещение № 206 |
| 7 | Служба психолого-педагогического сопровождения обучающихся | город Сургут, улица Энтузиастов, дом 28, помещение № 31 |
| 8 | Служба психолого-педагогического сопровождения обучающихся | город Сургут, улица Губкина, дом 7, помещение № 42 |
| 9 | Кабинет заместителя директора по административно-хозяйственной деятельности и специалиста по охране труда | город Сургут, улица Энтузиастов, дом 28, помещение № 7 |
| 10 | Кабинет общего отдела (рабочее место специалиста по закупкам) | город Сургут, улица Энтузиастов, дом 28, помещение № 6 |
| 11 | Фонотека (кабинет системного администратора) | город Сургут, улица Энтузиастов, дом 28, помещение № 208 |
| 12 | Приемная директора  | город Сургут, улица Энтузиастов, дом 28, помещение № 213 |
| 13 | Кабинет директора | город Сургут, улица Энтузиастов, дом 28, помещение № 214 |
| 14 | Кабинет заместителя директора по учебной работе | город Сургут, улица Энтузиастов, дом 28, помещение № 212 |
| 15 | Кабинет заместителя директора по воспитательной работе, специалиста по связям с общественностью | город Сургут, улица Энтузиастов, дом 28, помещение №217 |
| 16 | Контрольно-пропускной пункт | город Сургут, улица Энтузиастов, дом 28, помещение контрольно-пропускного пункта |

6.9. Перечень машинных носителей содержащих персональные данные, номера помещений (кабинетов) мест использования и хранения машинных носителей, содержащих персональные данные, указываются в журнале учета машинных носителей персональных данных (форма журнала приведена **в приложении № 7 к Положению**). Ответственным за ведение и хранение журнала является системный администратор.

Перечень мест хранения материальных носителей информационных систем персональных данных, номера помещений (кабинетов) мест хранения, должностные лица имеющие доступ к материальным носителям информационных систем персональных данных, указываются в журнале мест хранения материальных носителей ИСПДн (форма журнала приведена **в приложении № 8 к Положению**). Ответственным за ведение и хранение журнала является системный администратор.

Должностные лица Оператора, обрабатывающие персональные данные в силу своих должностных обязанностей, системный администратор при использовании машинных носителей персональных данных обязаны соблюдать инструкцию по учету машинных носителей персональных данных и другой конфиденциальной информации (**приложение № 9 к Положению**).

**7. Лица ответственные за организацию обработки персональных данных, за обеспечение безопасности персональных данных, комиссия по осуществлению внутреннего контроля соответствия обработки**

**персональных данных законодательству о персональных**

**данных, требованиям к защите персональных данных**

7.1. Ответственным за обеспечение безопасности персональных данных субъектов при их обработке на машинных носителях, сервере Оператора, в информационных системах является системный администратор Оператора (далее – Администратор информационных систем персональных данных), обеспечивающий:

- своевременное обнаружение фактов несанкционированного доступа к персональным данным и немедленное доведение этой информации до директора;

- применение сертифицированного антивирусного программного обеспечения с регулярно обновляемыми данными (инструкция по антивирусной защите –приведена **в приложении № 10 к Положению**);

- установление индивидуальных паролей доступа к персональным данным субъектов;

- определение уровня защищенности персональных данных в информационных системах персональных данных (**приложение № 11 к Положению)**;

- постоянный контроль за обеспечением уровня защищенности персональных данных;

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

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

- принимать меры по своевременному восстановлению работоспособности технических средств и программного обеспечения элементов информационных систем персональных данных, в том числе средств защиты персональных данных и выявлению причин, приведших к отказу работоспособности. Инструкция по резервному копированию и восстановлению персональных данных, обрабатываемых в информационных системах персональных данных (**приложение № 12 к Положению**).

Права и обязанности Администратора информационных систем персональных данных устанавливаются в Инструкции Администратора информационных систем персональных данных (**приложение № 13 к Положению**).

В случае выявления нарушений порядка обработки персональных данных на персональных компьютерах, сервере, в информационных системах, системный администратор Оператора принимает меры по установлению причин нарушений и их устранению.

7.2. Лицом ответственным за организацию обработки персональных данных у Оператора является заместитель директора по административно-хозяйственной деятельности.

Ответственный за организацию обработки персональных данных обязан осуществлять внутренний контроль за соблюдением Оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных.

Права и обязанности ответственного за организацию обработки персональных устанавливаются в Инструкции ответственного за организацию обработки персональных данных (**приложение № 14 к Положению**).

7.3. В целях осуществления внутреннего контроля соответствия обработки персональных данных требованиям законодательства о персональных данных Оператором организовывается проведение проверок условий обработки персональных данных.

Проверки обработки персональных данных проводятся комиссией по осуществлению внутреннего контроля соответствия обработки персональных данных законодательству о персональных данных, требованиям к защите персональных данных.

Состав, полномочия комиссии по осуществлению внутреннего контроля соответствия обработки персональных данных законодательству о персональных данных, требованиям к защите персональных данных устанавливаются в Инструкции комиссии по осуществлению внутреннего контроля соответствия обработки персональных данных законодательству о персональных данных, требованиям к защите персональных данных (**приложение № 16 к Положению**).

**8. Хранение персональных данных**

8.1. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

8.2. Использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения.

9. **Актуализация, исправление, удаление и уничтожение**

**персональных данных, ответы на запросы субъектов**

 **персональных данных**

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

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

9.2. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных Оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения указанного запроса на период проверки.

9.3. В случае выявления неправомерной обработки персональных данных, осуществляемой Оператором, Оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных. В случае, если обеспечить правомерность обработки персональных данных невозможно, Оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных Оператор обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

9.4. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных Оператор обязан прекратить их обработку и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Оператором и субъектом персональных данных либо если Оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных действующим законодательством Российской Федерации.

9.5. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в пунктах 9.3., 9.4. настоящего Положения, Оператор осуществляет блокирование таких персональных данных и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

9.6. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки персональных данных, в случае утраты необходимости в достижении этих целей, а также в случае истечения срока согласия на обработку персональных данных или отзыва субъектом персональных данных согласия на обработку персональных данных, если иное не предусмотрено действующим законодательством Российской Федерации.

Уничтожение и обезличивание персональных данных осуществляются согласно Инструкции по порядку уничтожения и обезличивания персональных данных (**приложение № 17 к Положению**).

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

Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с Оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

Сведения, должны быть предоставлены субъекту персональных данных Оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положения нормативно-правовых актов Российской Федерации, являющихся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

9.8. Оператор обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение тридцати дней с даты получения такого запроса.

10. **Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных**

10.1. За нарушение норм, регулирующих получение, обработку и защиту персональных данных физических лиц, виновные лица в соответствии с действующим законодательством Российской Федерации несут: дисциплинарную, материальную, административную, гражданско-правовую, уголовную ответственность.

Приложение № 1

к Положению об обработке и

защите персональных данных в

БУ «Сургутский музыкальный колледж»

 **Типовая форма согласия субъектов на обработку персональных данных**

**Согласие**

**на обработку персональных данных**

Я, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

 (фамилия, имя, отчество)

зарегистрированный(ная) по адресу \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, документ, удостоверяющий личность (серия, номер, дата выдачи, выдавший орган) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

свободно, своей волей и в своем интересе даю согласие уполномоченным должностным лицам БУ «Сургутский музыкальный колледж» (ИНН 8602020182, место нахождения: ул. Энтузиастов, д. 28, г. Сургут, Ханты-Мансийский автономный округ-Югра, 628404) на обработку (любое действие (операцию) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение) следующих персональных данных:

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (перечень обрабатываемых персональных данных)

Вышеуказанные персональные данные предоставляю для обработки в целях осуществления и выполнения возложенных законодательством Российской Федерации на БУ «Сургутский музыкальный колледж» функций, полномочий и обязанностей.

Я ознакомлен(а) с тем, что согласие на обработку персональных данных действует с даты подписания настоящего согласия до дня отзыва согласия в письменной форме.

Отзыв согласия может быть произведен мной в виде заявления, поданного в письменной форме на имя директора БУ «Сургутский музыкальный колледж», с указанием причины отзыва.

\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (подпись) (ФИО субъекта персональных данных (последнее - при наличии))

"\_\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_\_ г.

Приложение № 2

 к Положению об обработке и

защите персональных данных в

БУ «Сургутский музыкальный колледж»

**Согласие**

**субъекта на получение его персональных данных у третьей стороны**

Я, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

 (фамилия, имя, отчество)

зарегистрированный(ная) по адресу \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, документ, удостоверяющий личность (серия, номер, дата выдачи, выдавший орган) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

свободно, своей волей и в своем интересе даю согласие уполномоченным должностным лицам БУ «Сургутский музыкальный колледж» (ИНН 8602020182, место нахождения: ул. Энтузиастов, д. 28, г. Сургут, Ханты-Мансийский автономный округ-Югра, 628404) на получение моих персональных данных, а именно:

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (перечень персональных данных)

для обработки в целях \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

у следующих лиц \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(указать Ф.И.О. физического лица или наименование организации, которыми сообщаются данные)

Я также утверждаю, что ознакомлен с возможными последствиями моего отказа дать письменное согласие на их получение.

\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (подпись) (ФИО субъекта персональных данных (последнее - при наличии))

"\_\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_\_ г.

Приложение № 3

к Положению об обработке и

защите персональных данных в

БУ «Сургутский музыкальный колледж»

**Типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные**

Мне, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

 (фамилия, имя, отчество (последнее - при наличии)

разъяснены юридические последствия отказа предоставить свои персональные данные уполномоченным на обработку персональных данных лицам БУ «Сургутский музыкальный колледж»

\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (подпись) (фамилия, имя, отчество (последнее - при наличии)

"\_\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_\_ г.

Приложение № 4

 к Положению об обработке и

защите персональных данных в

БУ «Сургутский музыкальный колледж»

**Типовая форма обязательства лица непосредственно осуществляющего**

**обработку персональных данных о неразглашении конфиденциальной информации о персональных данных субъектов**

Я, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

 (фамилия, имя, отчество (при наличии)

документ, удостоверяющий личность, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

 (вид документа) (серия, номер)

выдан \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

 (кем и когда)

зарегистрированный(ая) по адресу: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

обязуюсь:

- соблюдать конфиденциальность персональных данных субъектов, ставших мне известными в связи с исполнением должностных обязанностей в БУ «Сургутский музыкальный колледж» (ИНН 8602020182);

- в случае попытки третьих лиц получить от меня сведения о персональных данных, сообщать об этом непосредственному руководителю;

- прекратить обработку персональных данных, ставших мне известными в связи с исполнением должностных обязанностей в БУ «Сургутский музыкальный колледж» (ИНН 8602020182), в случае расторжения со мной трудового договора.

Я уведомлен(а) о том, что персональные данные являются конфиденциальной информацией и я обязан(а) не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных.

Положения законодательства Российской Федерации, предусматривающие ответственность за нарушение требований Федерального закона от 27 июля 2006 г. N 152-ФЗ, мне разъяснены.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (подпись) (фамилия, имя, отчество (последнее - при наличии)

"\_\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_\_ г.

Приложение № 5

 к Положению об обработке и

защите персональных данных в

БУ «Сургутский музыкальный колледж»

**Инструкция должностных лиц Оператора, обрабатывающих**

**персональные данные без использования средств автоматизации**

**1.  Общие положения**

1.1. Должностным лицом Оператора, обрабатывающим персональные данные без использования средств автоматизации (далее – Пользователь) является каждый работник Оператора, участвующий в рамках своих функциональных обязанностей в процессах обработки персональных данных.

1.2. Пользователь несет персональную ответственность за свои действия.

1.3. Пользователь в своей работе руководствуется настоящей инструкцией, руководящими и нормативными документами Российской Федерации и локальными нормативными актами Оператора.

**2.  Пользователь обязан:**

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите персональных данных и распоряжений, регламентирующих порядок действий по защите персональных данных.

2.2. Выполнять на рабочем месте только те процедуры, которые определены для него должностной инструкцией.

2.3. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности персональных данных, а также руководящих и организационно-распорядительных документов.

2.4. Соблюдать требования парольной политики.

2.5. Соблюдать правила при работе в сетях общего доступа и (или) международного обмена – Интернет и других.

2.6. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами.

2.7. Соблюдать режим секретности (конфиденциальности персональных данных).

2.8. При отсутствии визуального контроля за рабочей станцией доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>.

2.9. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в пределах возложенных на него функций.

2.10. Не сообщать персональные данные третьей стороне без письменного согласия субъекта персональных данных, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью физического лица, а также в других случаях, предусмотренных законодательством Российской Федерации.

**3.  Пользователям запрещается:**

- разглашать обрабатываемые персональные данные третьим лицам;

- копировать персональные данные на внешние носители без прямой служебной необходимости, делать выписки персональных данных, распечатывать документы с персональными данными;

- хранение или оставление бумажных документов и съемных носителей, содержащих персональные данные, в виде, позволяющем осуществить визуальный просмотр содержащихся в них персональных данных, их фотографирование или несанкционированное создание копий;

- самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;

- несанкционированно открывать общий доступ к папкам на своем рабочем месте (рабочей станции, компьютере);

- запрещено подключать к рабочей станции (компьютеру) и корпоративной информационной сети личные внешние носители и мобильные устройства;

- отключать (блокировать) средства защиты информации;

- сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам информационных систем персональных данных;

- привлекать посторонних лиц для производства ремонта или настройки рабочего места (рабочей станции, компьютера).

**4.  Организация парольной защиты**

4.1. Личные пароли доступа к рабочей станции (компьютеру), элементам информационных систем персональных данных выдаются Пользователям Администратором информационных систем персональных данных.

4.2. Правила формирования пароля:

- пароль не может содержать имя учетной записи пользователя или какую-либо его часть;

- пароль должен состоять не менее чем из 8 символов;

- в пароле должны присутствовать символы трех категорий из числа следующих четырех:

1) прописные буквы английского алфавита от A до Z;

2) строчные буквы английского алфавита от a до z;

3) десятичные цифры (от 0 до 9);

4) символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #, %).

- запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а также имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе;

- запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;

- запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);

-  запрещается выбирать пароли, которые уже использовались ранее.

4.3. Правила ввода пароля:

- ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан;

- во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

4.4. Правила хранение пароля:

- запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах;

- запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

4.5. Лица, использующие паролирование, обязаны:

- четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по паролированию;

- своевременно сообщать Администратору информационных систем персональных данных об утере, компрометации, несанкционированном изменении паролей.

**5. Правила работы в сетях общего доступа и (или) международного обмена**

5.1. Работа в сетях общего доступа и (или) международного обмена (сети Интернет и других) (далее – Сеть) на рабочем месте (рабочей станции, компьютере), должна проводиться при служебной необходимости.

5.2. При работе в Сети запрещается:

- осуществлять работу при отключенных средствах защиты (антивирус и других);

- передавать по Сети защищаемую информацию без использования средств шифрования;

- запрещается скачивать из Сети программное обеспечение и другие файлы;

- запрещается посещение сайтов сомнительной репутации (сайты, содержащие нелегально распространяемое ПО и другие);

- запрещается нецелевое использование подключения к Сети.

6**.  Права и ответственность Пользователей**

6.1. Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к персональным данным.

6.2. Пользователи, виновные в несоблюдении Настоящей инструкции несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Приложение № 6

к Положению об обработке и

защите персональных данных в

БУ «Сургутский музыкальный колледж»

**Инструкция пользователя персональных данных по обеспечению безопасности обработки персональных данных при возникновении внештатных ситуаций**

**1.     Назначение и область действия**

1.1.  Настоящая инструкция определяет возможные аварийные ситуации, связанные с функционированием информационных систем персональных данных (ИСПДн) Оператора, меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн после аварийных ситуаций.

1.2. Целью настоящего документа является превентивная защита элементов ИСПДн от прерывания в случае реализации рассматриваемых угроз.

1.3.  Задачей настоящей Инструкции является:

* определение мер защиты от прерывания;
* определение действий восстановления в случае прерывания.

1.4. Действие настоящей Инструкции распространяется на всех пользователей, имеющих доступ к ресурсам ИСПДн, а также на основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

* системы жизнеобеспечения;
* системы обеспечения отказоустойчивости;
* системы резервного копирования и хранения данных;
* системы контроля физического доступа.

**2.     Порядок реагирования на аварийную ситуацию**

**2.1. Действия при возникновении аварийной ситуации**

2.1.1. В настоящем документе под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн. Аварийная ситуации становится возможной в результате реализации одной из угроз, приведенных в таблице «Источники угроз».

**Источники угроз**

|  |  |
| --- | --- |
|   | **Технологические угрозы** |
| 1 | Пожар в здании |
| 2 | Повреждение водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения) |
| 3 | Взрыв (бытовой газ, теракт, взрывчатые вещества или приборы, работающие под давлением) |
| 4 | Химический выброс в атмосферу |
|   | **Внешние угрозы** |
| 5 | Массовые беспорядки |
| 6 | Сбои общественного транспорта |
| 7 | Эпидемия |
| 8 | Массовое отравление персонала |
|   | **Стихийные бедствия** |
| 9 | Удар молнии |
| 10 | Сильный снегопад |
| 11 | Сильные морозы |
| 12 | Просадка грунта (подмыв грунтовых вод, подземные работы) с частичным обрушением здания |
| 13 | Затопление водой в период паводка |
| 14 | Наводнение, вызванное проливным дождем |
| 15 | Подтопление здания (воздействие подпочвенных вод, вызванное внезапным и непредвиденным повышением уровня грунтовых вод) |
|   | **Телекоммуникационные и ИТ угрозы** |
| 16 | Сбой системы кондиционирования |
| 17 | Сбой ИТ – систем |
|   | **Угроза, связанная с человеческим фактором** |
| 18 | Ошибка персонала, имеющего доступ к серверной |
| 19 | Нарушение конфиденциальности, целостности и доступности конфиденциальной информации |
|   | **Угрозы, связанные с внешними поставщиками** |
| 20 | Отключение электроэнергии |
| 21 | Сбой в работе Интернет-провайдера |
| 22 | Физический разрыв внешних каналов связи |

2.1.2. В кратчайшие сроки, не превышающие одного рабочего дня, Администратор информационных систем персональных данных и пользователи ИСПДн, предпринимают меры по восстановлению работоспособности системы.

**2.2. Уровни реагирования на инцидент**

При реагировании на инцидент, важно, чтобы пользователь правильно классифицировал критичность инцидента. Критичность оценивается на основе следующей классификации:

* **Уровень 1 – Незначительный инцидент.** Незначительный инцидент определяется как локальное событие с ограниченным разрушением, которое не влияет на общую доступность элементов ИСПДн и средств защиты. Эти инциденты решаются ответственными за реагирование сотрудниками.
* **Уровень 2 – Авария.** Любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов ИСПДн и средств защиты. Эти инциденты выходят за рамки управления ответственными за реагирование сотрудниками.

К авариям относятся следующие инциденты:

1. Отказ элементов ИСПДн и средств защиты из-за:

- повреждения водой (провыв системы водоснабжения, канализационных труб, систем охлаждения), а также подтопления в период паводка или проливных дождей;

- сбоя системы кондиционирования.

* **Уровень 3 – Катастрофа.** Любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИСПДн и средств защиты, а также к угрозе жизни пользователей ИСПДн, классифицируется как катастрофа. Обычно к катастрофам относятся обстоятельства непреодолимой силы (пожар, взрыв), которые могут привести к неработоспособности ИСПДн и средств защиты на сутки и более.

К катастрофам относятся следующие инциденты:

- пожар в здании;

- взрыв;

- просадка грунта с частичным обрушением здания;

- массовые беспорядки в непосредственной близости от объекта.

 **3.     Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций**

**3.1.         Технические меры**

3.1.1.  К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения и возникновения аварийных ситуаций, такие как:

* системы жизнеобеспечения;
* системы обеспечения отказоустойчивости;
* системы резервного копирования и хранения данных;
* системы контроля физического доступа.

Системы жизнеобеспечения ИСПДн включают:

* пожарные сигнализации и системы пожаротушения;
* системы вентиляции и кондиционирования;
* системы резервного питания.

3.1.2.  Все критические помещения (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации.

Приложение № 7

 к Положению об обработке и

защите персональных данных в

БУ «Сургутский музыкальный колледж»

**Журнал учета машинных носителей персональных данных**

Начат \_\_.\_\_.20\_\_\_ г.

Окончен \_\_\_\_\_\_\_\_\_\_\_\_\_\_ г.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| № п/п | Учётный номер машинного носителя | Вид (тип, модель) машинного носителя | Дата постановки на учёт машинного носителя | Место использования и хранения машинного носителя | ФИО лица, регистрирующего носитель | Подпись лица, регистрирующего носитель | Сведения об уничтожении носителя (№ акта, дата) |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

Приложение № 8

к Положению об обработке и

защите персональных данных в

БУ «Сургутский музыкальный колледж»

**Журнал мест хранения материальных носителей ИСПДН**

Начат \_\_.\_\_.20\_\_\_ г.

Окончен \_\_\_\_\_\_\_\_\_\_\_\_\_\_ г.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Вид (тип, модель) машинного носителя | Название или номер помещения | Место хранения  |  Лица имеющие доступ |
|  |  |  |  |  |
|   |  |   |   |   |
|  |  |  |  |  |

Приложение № 9

к Положению об обработке и

защите персональных данных в

БУ «Сургутский музыкальный колледж»

**Инструкция**

**по учету машинных носителей персональных данных и другой конфиденциальной информации**

1. **Общие положения**
	1. Инструкция определяет порядок учета машинных носителей персональных данных и другой конфиденциальной информации предназначенных для работы в информационных системах.
	2. Под использованием машинных носителей персональных данных и другой конфиденциальной информации в информационных системах понимается их подключение к инфраструктуре информационных систем с целью обработки, приема, передачи информации между ресурсами информационной системы и машинными носителями информации.
	3. Администратор информационных систем персональных данных (далее – Администратор) обеспечивает учет машинных носителей персональных данных и другой конфиденциальной информации, используемых в информационных системах для хранения и обработки информации.

Учету подлежат:

* + Съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства);
	+ портативные вычислительные устройства, имеющие встроенные носители информации (ноутбуки, нетбуки, планшеты, цифровые камеры, звукозаписывающие устройства и иные аналогичные по функциональности устройства);
	+ машинные носители информации, встроенные в корпус средств вычислительной техники (накопители на жестких дисках).
	1. Все находящиеся на хранении и в обращении носители конфиденциальной информации подлежат регистрации в «Журнале учета машинных носителей персональных данных». Каждый носитель должен иметь уникальный учетный номер.
	2. Журнал учета машинных носителей персональных данных ведется Администратором в печатном виде.
1. **Порядок работы с машинными носителями**
2. В информационной системе запрещается использование не входящих в ее состав **(**находящихся в личном использовании**)** машинных носителей информации.
	1. В информационной системе допускается использование только учтенных машинных носителей информации.
3. Допуск должностного лица Оператора, обрабатывающего персональные данные в силу своих должностных обязанностей к машинным носителям персональных данных определяется на основании имеющих у пользователей прав доступа и служебных обязанностей.
4. Должностные лица Оператора, обрабатывающие персональные данные в силу своих должностных обязанностей получают учтенный машинный носитель от Администратора. При получении делаются соответствующие записи в журнале учета машинных носителей персональных данных.
5. При использовании должностными лицами Оператора, обрабатывающими персональные данные в силу своих должностных обязанностей машинных носителей персональных данных необходимо:
* соблюдать требования настоящей инструкции;
* использовать носители информации исключительно для выполнения служебных обязанностей;
* ставить в известность Администратора о любых фактах нарушения требований настоящей инструкции;
* бережно относиться к машинным носителям информации;
1. При использовании машинных носителей персональных данных запрещается:
* оставление машинных носителей персональных данных без присмотра или передача их на хранение другим лицам;
* вынос мащинных носителей персональных данных из служебных помещений для работы с ними на дому, в гостиницах и т. д.;
* использование для хранения и обработки персональных данных машинных носителей информации, не поставленных на учет в установленном порядке.
1. Любое взаимодействие (обработка, прием, передача информации), инициированное работниками Оператора, между информационной системой и неучтенным машинным носителем, рассматривается как несанкционированное. Администратор оставляет за собой право блокировать или ограничивать использование машинных носителей персональных данных.
2. В случае выявления фактов несанкционированного и/или нецелевого использовании машинных носителей персональных данных, проводится служебная проверка комиссией, состав которой определяется руководителем Оператора.
3. По факту выясненных обстоятельств составляется акт расследования инцидента и передается руководителю Оператора для принятия мер, согласно действующему законодательству Российской Федерации и локальным внутренним нормативным актам Оператора.
4. Информация, хранящаяся на учтенных машинных носителях, подлежит обязательной проверке на отсутствие вредоносного программного обеспечения.
5. О фактах утраты или уничтожения машинных носителей, содержащих персональные данные, либо разглашения содержащихся на них сведений, немедленно ставится в известность руководитель Оператора. О факте утраты машинного носителя составляется акт. Соответствующие отметки вносятся в журнал машинных носителей персональных данных.
6. Машинные носители персональных данных, пришедшие в негодность или отслужившие установленный срок, подлежат уничтожению. Уничтожение машинных носителей с персонифицированной информацией осуществляется комиссией, назначенной приказом руководителя Оператора. По результатам уничтожения носителей составляется акт об уничтожении носителей персональных данных по ниже приложенной форме.

**Акт об уничтожении носителей персональных данных**

Комиссия в составе:

Председатель: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Члены комиссии: *\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

 *\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

 *\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

провела отбор носителей персональных данных и установила, что в соответствии с требованиями руководящих документов по защите информации, информация записанная на них в процессе эксплуатации, подлежит уничтожению.

Указанные носители, содержащие персональные данные уничтожены путем (разрезания, сжигания, механического уничтожения и т.п. указать нужное)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № | Дата | Тип носителя | Рег. или инвент. № носителя ПНд | Способ уничтожения |
|  1 |  00.00.0000 | USB флеш 2Gb  |  | Физическое уничтожение без возможности восстановления  |
|  |  |  |  |  |

Председатель: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Члены комиссии: *\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

 *\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. При увольнении или переводе должностного лица Оператора, обрабатывающего персональные данные в силу своих должностных обязанностей в другое структурное подразделение, предоставленные машинные носители персональных данных изымаются.
2. Должностные лица Оператора, обрабатывающие персональные данные в силу своих должностных обязанностей, нарушившие требования настоящей инструкции, несут ответственность в соответствии с действующим законодательством Российской Федерации и внутренними нормативными актами Оператора.

Приложение № 10

к Положению об обработке и

защите персональных данных в

БУ «Сургутский музыкальный колледж»

**Инструкция по организации антивирусной защиты**

1. Настоящая Инструкция определяет требования к организации защиты от разрушающего воздействия компьютерных вирусов и устанавливает ответственность за их выполнение.
2. К использованию у Оператора допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.
3. Установка средств антивирусного контроля на компьютерах осуществляется Администратором информационных систем персональных данных. Настройка параметров средств антивирусного контроля в соответствии с руководствами по применению конкретных антивирусных средств.
4. Ежедневно в начале работы при загрузке компьютера в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов.
5. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, CD-ROM и т.п.).
6. Контроль входящей и исходящей информации на защищаемых серверах и персональных компьютерах (далее ПК) осуществляется непрерывно посредством постоянно работающего компонента антивирусного программного обеспечения («монитора»). Полная проверка информации, хранящейся на серверах и ПК должна осуществляться не реже одного раза в месяц.
7. Обновление баз вирусов антивирусного программного обеспечения, установленного на ПК и серверах, должно осуществляться еженедельно.
8. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера (локальной вычислительной сети), должна быть выполнена антивирусная проверка на защищаемом рабочем месте - Администратором информационных систем персональных данных.

9. 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.) Администратор информационных систем персональных данных должен провести внеочередной антивирусный контроль рабочей станции.

10. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники подразделений обязаны:

- приостановить работу;

- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов Администратора информационных систем персональных данных, владельца зараженных файлов, а также сотрудников, использующих эти файлы в работе;

- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

- провести лечение или уничтожение зараженных файлов.

11. Ответственность за антивирусный контроль у Оператора, за проведение мероприятий антивирусного контроля в подразделениях Оператора и соблюдение требований настоящей Инструкции возлагается на Администратора информационных систем персональных данных.

Приложение № 11

к Положению об обработке и

защите персональных данных в

БУ «Сургутский музыкальный колледж»

**Определение уровня защищенности персональных данных в информационных системах персональных данных**

Под уровнем защищенности персональных данных (УЗ) понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (ИСПДн).

Определение уровня защищенности персональных данных в ИСПДн проводится 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».

При обработке персональных данных в ИСПДн устанавливаются 4 уровня защищенности персональных данных (УЗ1, УЗ2, УЗ3, УЗ4). Самый низкий УЗ – четвертый, самый высокий – первый.

Уровни защищенности персональных данных при их обработке в ИСПДн определяются в зависимости от типа актуальных угроз безопасности персональных данных с учетом возможного вреда субъекту персональных данных, объема и содержания обрабатываемых персональных данных, вида деятельности, при осуществлении которого обрабатываются персональные данные (таблица 1).

Таблица 1. Уровни защищенности персональных данных в ИСПДн

|  |  |  |  |
| --- | --- | --- | --- |
| **Категории персональных данных** | **Категория субъектов** | **Количество субъектов** | **Тип актуальных угроз** |
| **1 тип** | **2 тип** | **3 тип** |
| Специальные   | не сотрудников оператора | более 100000 | УЗ1 | УЗ1 | УЗ2 |
| менее 100000 | УЗ1 | УЗ2 | УЗ3 |
| сотрудников оператора | любое | УЗ1 | УЗ2 | УЗ3 |
| Биометрические   | не сотрудников оператора | более 100000 | УЗ1 | УЗ2 | УЗ3 |
| менее 100000 | УЗ1 | УЗ2 | УЗ3 |
| сотрудников оператора | любое | УЗ1 | УЗ2 | УЗ3 |
| Иные   | не сотрудников оператора | более 100000 | УЗ1 | УЗ2 | УЗ3 |
| менее 100000 | УЗ1 | УЗ3 | УЗ4 |
| сотрудников оператора | любое | УЗ1 | УЗ3 | УЗ4 |
| Общедоступные   | не сотрудников оператора | более 100000 | УЗ2 | УЗ2 | УЗ4 |
| менее 100000 | УЗ2 | УЗ3 | УЗ4 |
| сотрудников оператора | любое | УЗ2 | УЗ3 | УЗ4 |

Определение уровня защищенности персональных данных в ИСПДн осуществляется в соответствии с требованиями Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» системным администратором БУ «Сургутский музыкальный колледж», на основании проведения постоянного анализа всех эксплуатируемыху Оператора информационных систем, где присутствуют и обрабатываются персональные данные.

Результаты определения уровня защищенности персональных данных в ИСПДн системный администратор отражает в Акте определения уровня защищенности персональных данных при их обработке в информационных системах персональных данных, согласно нижеуказанного образца.

|  |
| --- |
| ОбразецАКТопределения уровня защищенности персональных данных при их обработке в информационных системах персональных данныхв БУ «Сургутский музыкальный колледж»В ходе рассмотрения исходных данных об информационной системе персональных данных (далее - ИСПДн), необходимых для определения уровня защищенности персональных данных в «\_\_\_\_\_\_\_ **Наименование ИСПДн \_\_\_\_\_\_\_\_\_**» установлено следующее:- Категории персональных данных обрабатываемых в ИСПДн: в информационной системе персональных данных обрабатываются \_\_\_\_\_\_\_\_\_\_\_ (биометрические, специальные, общедоступные или иные) категории персональных данных;- Категории субъектов: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (субъектов персональных данных, являющихся сотрудниками оператора или субъектов персональных данных, не являющихся сотрудниками оператора);- Объем обрабатываемых персональных данных (количество субъектов): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (менее чем 100000, более чем 100000);- Тип актуальных угроз: для информационной системы актуальны угрозы \_\_\_\_\_ (первого, второго, третьего) типа;- Масштаб информационной системы: информационная система имеет \_\_\_\_\_\_\_\_\_\_ (федеральный, региональный или объектовый) масштаб;- Местонахождение технических средств: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.В соответствии с Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и на основании анализа исходных данных, необходимо обеспечить \_\_\_\_\_ уровень защищенности (УЗ\_\_\_\_) персональных данных.Системный администратор БУ «Сургутский музыкальный колледж» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_ г. |

Актуализация Акта определения уровня защищенности персональных данных при их обработке в информационных системах персональных данных производится системным администратором ежегодно до 01 марта текущего года, а также по мере необходимости по результатам анализа всех эксплуатируемыху Оператора информационных систем, где присутствуют и обрабатываются персональные данные.

Приложение № 12

к Положению об обработке и

защите персональных данных в

БУ «Сургутский музыкальный колледж»

**Инструкция по резервному копированию и восстановлению персональных данных, обрабатываемых в информационных**

**системах персональных данных**

1. Настоящая инструкция определяет порядок осуществления резервного копирования информационных ресурсов информационных систем персональных данных (ИСПДн)

2. Процесс резервного копирования обеспечивает сохранение на резервных носителях информации, с целью ее восстановления при потере или порче на основном носителе, и является ключевым элементом защиты от умышленной и неумышленной потери данных.

3. Резервное копирование защищаемой информации персональных данных, хранимое на серверах БУ «Сургутский музыкальный колледж», осуществляется автоматически ежедневно посредством создания бэкапов на специальных (дублирующих) системных блоках и хранится на жестких дисках, расположенных в них.

Резервное копирование защищаемой информации персональных данных системы СКУД производится вручную ежемесячно администратором информационных систем персональных данных (далее Администратор).

4. Перед выполнением задания резервного копирования Администратор проверяет доступность резервного носителя, а также наличие на нем свободного места для записи данных.

После завершения выполнения задачи резервного копирования Администратор должен извлечь резервный носитель и поместить на хранение.

5. Хранение резервных копий должно быть организовано в отдельном от копируемых информационных ресурсов помещении.

К резервному носителю персональных данных должна быть приложена учетная карточка, в которой делаются отметки о дате резервирования.

Резервные носители должны храниться на безопасном расстоянии от источников магнитных полей: блоков питания, телефонов, мониторов и т.п.

Доступ к хранилищу резервных копий должны иметь только Администратор.

6. Восстановление персональных данных из резервных копий и работоспособности ИСПДн осуществляется в случаях сбоев, отказов и аварий технических средств и систем ИСПДн, а также ее программного обеспечения.

Данные работы осуществляются Администратором в соответствии с эксплуатационной документацией на программное обеспечение до полного восстановления работоспособности.

В случае необходимости привлечения для восстановления работоспособности ИСПДн представителей сторонних организаций, должна быть обеспечена невозможность их ознакомления с персональными данными. Ответственность за выполнение данного требования возлагается на Администратора.

Приложение № 13

 к Положению об обработке и

защите персональных данных в

БУ «Сургутский музыкальный колледж»

**Инструкция Администратора информационных систем персональных данных**

**1.  Общие положения**

1.1. Администратором информационных систем персональных данных (далее – Администратор или Администратор ИСПДн) у Оператора является системный администратор БУ «Сургутский музыкальный колледж».

1.2. Администратор в своей работе руководствуется настоящей инструкцией, руководящими и нормативными документами Российской Федерации и локальными нормативными документами БУ «Сургутский музыкальный колледж».

1.4. Администратор отвечает за обеспечение устойчивой работоспособности элементов информационных систем персональных данных (далее – ИСПДн) и средств защиты при обработке персональных данных (ПДн).

**2.  Администратор обязан:**

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите персональных данных.

2.2. Обеспечивать установку, настройку и своевременное обновление элементов ИСПДн:

- программного обеспечения автоматизированных рабочих мест (АРМ) и серверов (операционные системы, прикладное и специальное программное обеспечение (ПО));

- аппаратных средств;

- аппаратных и программных средств защиты.

2.3. Обеспечивать работоспособность элементов ИСПДн и локальной вычислительной сети.

2.4. Осуществлять контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов.

2.5. Обеспечивать функционирование и поддерживать работоспособность средств защиты персональных данных, знать и соблюдать условия использования средств защиты персональных данных, предусмотренных эксплуатационной и технической документацией.

2.6. Вести учет применяемых средств защиты персональных данных, эксплуатационной и технической документации к ним, носителей персональных данных;

2.7. В случае отказа работоспособности технических средств и программного обеспечения элементов ИСПДн, в том числе средств защиты персональных данных, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

2.8. Проводить контроль принятых мер по защите ИСПДн, в пределах возложенных на него функций согласно плана внутренних проверок по обеспечению защиты ИСПДн (раздел 4. настоящей Инструкции).

2.9. Устанавливать индивидуальные пароли доступа к персональным данным субъектов, хранить, осуществлять прием и выдачу персональных паролей пользователям, осуществлять контроль за правильностью использования персональных паролей.

2.10. Обеспечивать постоянный контроль за выполнением пользователями установленного комплекса мероприятий по обеспечению безопасности персональных данных.

2.11. Информировать руководителя Оператора о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн.

2.12. Требовать прекращения обработки персональных данных, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн или средств защиты.

2.13. Обеспечивать строгое выполнение требований по обеспечению безопасности персональных данных при организации обслуживания технических средств и отправке их в ремонт. Техническое обслуживание и ремонт средств вычислительной техники, предназначенных для обработки персональных данных, проводятся организациями, имеющими соответствующие лицензии. При проведении технического обслуживания и ремонта запрещается передавать ремонтным организациям узлы и блоки с элементами накопления и хранения информации. Вышедшие из строя элементы и блоки средств вычислительной техники заменяются на элементы и блоки, прошедшие специальные исследования и специальную проверку.

2.14. Присутствовать при выполнении технического обслуживания элементов ИСПДн, сторонними физическими людьми и организациями.

2.15. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.

2.16. Применять сертифицированное антивирусное программное обеспечение с регулярно обновляемыми данными.

**3.  Права и ответственность Администратора**

3.1. Администратор имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн, в том числе производить установку и настройку элементов ИСПДн, контролировать и поддерживать работоспособность ИСПДн и выполнять прочие действия в рамках должностных обязанностей.

3.2. Администратор виновный в несоблюдении настоящей инструкции несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

**4. План внутренних проверок по обеспечению защиты ИСПДн**

План внутренних проверок по обеспечению защиты ИСПДн содержит необходимый перечень мероприятий для обеспечения контроля системы защиты персональных данных.

План внутренней проверки содержит следующую информацию:

- название проверяемого мероприятия;

- периодичность проведения проверки;

- исполнитель.

Проверки, предусмотренные настоящим планом, обязательны для проведения в отношении каждой ИСПДн во всех подразделениях обрабатывающих персональные данные.

Все результаты проверок заносятся в специальные журналы учёта проверок.

**План внутренних проверок состояния защиты ИСПДн**

|  |  |  |
| --- | --- | --- |
| **Мероприятие** | **Периодичность** | **Исполнитель** |
| Контроль над соблюдениемрежима защиты ИСПДн | Ежедневно | Администратор ИСПДн |
| Контроль над выполнениемантивирусной защиты ИСПДн | Еженедельно | Администратор ИСПДн |
| Контроль над соблюдением режима защиты при подключении к сетям общего пользования | Еженедельно | Администратор ИСПДн |
| Контроль за обеспечением резервного копирования информации | Ежемесячно | Администратор ИСПДн. |
| Контроль за обновлениями программного обеспечения и единообразия применяемогоПО на всех элементах ИСПДн | Ежеквартально | Администратор ИСПДн |
| Анализ и пересмотр имеющихся угроз безопасности ПДн в ИСПДн, предупреждение появления новых угроз | Ежегодно | Администратор ИСПДн |
| Проведение внутренних проверок на предмет выявленияизменений в режиме обработки и защиты ПДн в ИСПДн | Ежегодно | Администратор ИСПДн |

Приложение № 14

 к Положению об обработке и

защите персональных данных в

БУ «Сургутский музыкальный колледж»

**Инструкция ответственного за организацию обработки персональных данных**

**1.  Общие положения**

1.1. Ответственным за организацию обработки персональных данных у Оператора является заместитель директора по административно-хозяйственной деятельности

1.2. Ответственным за организацию обработки персональных данных в своей работе руководствуется настоящей инструкцией, руководящими и нормативными документами Российской Федерации и локальными нормативными документами БУ «Сургутский музыкальный колледж».

**2.  Ответственный за организацию обработки персональных данных обязан:**

2.1. Осуществлять контроль за сбором с должностных лиц Оператора, допущенных к обработке персональных данных, письменного обязательства о соблюдении режима конфиденциальности персональных данных и соблюдении правил их обработки (обязательство о неразглашении конфиденциальной информации о персональных данных субъектов).

2.2. Осуществлять прием субъектов персональных данных по вопросам обработки и защиты персональных данных указанных субъектов.

2.3. По запросу субъекта персональных данных сообщать ему сведения об обработке его персональных данных.

2.4. По запросу субъекта персональных данных организовать уточнение, блокирование или уничтожение персональных данных указанного субъекта.

2.5. Вести журнал учета обращений субъектов персональных данных по вопросам обработки персональных данных (приложение № 15 к Положению).

2.6. Осуществлять сопровождение и решение вопросов c органами, контролирующими обработку и защиту персональных данных, при проведении проверок.

2.7. Принимать меры по реагированию в случае возникновения внештатных и аварийных ситуаций с целью ликвидации их последствий.

**3. Ответственный за организацию обработки персональных данных имеет право:**

3.1. Указывать лицам, участвующим в обработке персональных данных, на необходимость осуществления уточнения, блокирования или уничтожения персональных данных по запросу субъекта.

3.2. Вносить на рассмотрение руководителю Оператора предложения по совершенствованию работы, связанной с обеспечением безопасности персональных данных.

**4. Ответственность**

4.1. За неисполнение (ненадлежащее исполнение) своих должностных обязанностей, предусмотренных настоящей инструкцией, ответственный за организацию обработки персональных данных несет персональную ответственность в соответствии с законодательством Российской Федерации.

Приложение № 15

 к Положению об обработке и

защите персональных данных в

БУ «Сургутский музыкальный колледж»

**Журнал**

**учета обращений субъектов персональных данных**

**по вопросам обработки персональных данных**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| №№ п/п | Дата обращения | ФИО обратившегося | Цель обращения | Отметка о предоставлении информации или отказе в ее предоставлении / дата предоставления или отказа в предоставлении информации | Подпись ответственного | Примечание |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Приложение № 16

 к Положению об обработке и

защите персональных данных в

БУ «Сургутский музыкальный колледж»

**Инструкция комиссии по осуществлению внутреннего контроля соответствия обработки персональных данных законодательству о персональных данных, требованиям к защите персональных данных**

**1.  Общие положения**

1.1. Настоящая Инструкция определяет состав, полномочия комиссии по осуществлению внутреннего контроля соответствия обработки персональных данных законодательству о персональных данных, требованиям к защите персональных данных (далее – Комиссия) обрабатываемых в БУ «Сургутский музыкальный колледж».

1.2. Комиссия в своей работе руководствуется настоящей инструкцией, руководящими и нормативными документами Российской Федерации и локальными нормативными документами БУ «Сургутский музыкальный колледж».

**2. Состав Комиссии:**

|  |  |
| --- | --- |
| Председатель комиссии | Заместитель директора по административно-хозяйственной деятельности |
| Члены комиссии | Главный бухгалтер |
| Начальник отдела кадров и документационного обеспечения управления |
| Начальник юридического отдела |
| Системный администратор |

**3. Порядок осуществления внутреннего контроля соответствия обработки персональных данных законодательству о персональных данных, требованиям к защите персональных данных**

3.1. Проверки соответствия обработки персональных данных законодательству о персональных данных, требованиям к защите персональных данных проводятся Комиссией в плановом порядке (плановые проверки) или на основании поступившей информации о нарушениях правил обработки персональных данных (внеплановые проверки).

 Плановые проверки проводятся два раза в год (июнь, декабрь).

Проведение внеплановой проверки организуется в течение трех рабочих дней со дня поступления информации о нарушениях правил обработки персональных данных.

3.2. Проверки соответствия обработки персональных данных законодательству о персональных данных, требованиям к защите персональных данных осуществляются непосредственно на месте обработки персональных данных путем опроса либо, при необходимости, путем осмотра служебных мест работников Оператора, осуществляющих обработку персональных данных.

3.3. При проведении проверки соответствия обработки персональных данных законодательству о персональных данных, требованиям к защите персональных данных проверяются:

- порядок и условия применения средств защиты информации;

- эффективность принимаемых мер по обеспечению безопасности персональных данных;

- состояние учета носителей персональных данных;

- соблюдение правил доступа к персональным данным;

- соблюдение порядка доступа в помещения, в которых ведется обработка персональных данных;

- наличие (отсутствие) фактов несанкционированного доступа к персональным данным.

3.4. Комиссия имеет право:

- запрашивать у работников Оператора осуществляющих обработку персональных данных, информацию, необходимую для реализации полномочий Комиссии;

- требовать от работников Оператора, осуществляющих обработку персональных данных, уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных.

3.5. Члены Комиссии должны обеспечивать конфиденциальность персональных данных ставших им известными в ходе проведения проверки.

3.6. По результатам проведенной проверки соответствия обработки персональных данных требованиям к защите персональных данных Комиссией составляется акт проверки соответствия обработки персональных данных законодательству о персональных данных, требованиям к защите персональных данных.

Приложение № 17

к Положению об обработке и

защите персональных данных в

БУ «Сургутский музыкальный колледж»

**Инструкция по порядку уничтожения**

**и обезличивания персональных данных**

**1. Общие положения**

1.1. Настоящая инструкция определяет порядок уничтожения и обезличивания информации, содержащей персональные данные, при достижении целей обработки или при наступлении иных законных оснований.

1.2. Инструкция разработана в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

**2. Условия и порядок уничтожения информации, содержащей персональные данные**

2.1. Оператор уничтожает информацию, содержащую персональные данные:

- по достижении целей обработки или в случае утраты необходимости в достижении этих целей;

- по достижении окончания срока хранения;

- при наступлении иных законных оснований.

2.2. Уничтожение информации, содержащей персональные данные, производится в случае достижения цели обработки в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных.

2.3. Уничтожение информации, содержащей персональные данные, производится в случае выявления неправомерной обработки в срок, не превышающий десяти дней с момента выявления неправомерной обработки персональных данных.

2.4. Ответственными за уничтожение информации, содержащей персональные данные, назначаются ответственный за организацию обработки персональных данных и Администратор информационных систем персональных данных. Ответственные лица подписывают соответствующий Акт об уничтожении персональных данных или физичеких носителей, содержащих персональные данные.

2.5. К персональным данным, хранимым в электронном виде, относятся файлы, папки, электронные архивы на жестком диске компьютера и съёмных машинных носителях, таких как компакт-диски CD-R/RW или DVD-R/RW, blue ray, дискеты 3,5”, флеш-накопители и любые устройства, оснащённые флеш-памятью.

2.6. Съёмные машинные носители по истечению сроков обработки и хранения на них персональных данных подлежат уничтожению с целью невозможности восстановления и дальнейшего использования. Это достигается путем деформирования - нарушения единой целостности носителя.

2.7. В случае допустимости повторного использования съёмного машинного носителя применяется программное удаление («затирание») содержимого путём его форматирования с последующей записью новой информации на данный носитель.

2.8. Подлежащие уничтожению файлы с персональными данными, расположенные на жестком диске информационной системы персональных данных, удаляются средствами операционной системы компьютера с последующим «очищением корзины».

2.9. Черновики документов, испорченные листы, варианты и неподписанные проекты документов уничтожаются путём их сожжения или измельчения или другим путем, исключающим восстановление текста документов.

**3. Условия и порядок обезличивания информации, содержащей персональные данные**

3.1. Оператор может обезличивать персональные данные в статистических или иных исследовательских целях, по достижении целей обработки персональных данных или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством Российской Федерации.

3.2. Способы обезличивания при условии дальнейшей обработки персональных данных:

- замена части данных идентификаторами;

- обобщение, изменение или удаление части данных;

- деление данных на части и обработка в разных информационных системах;

- перемешивание данных;

- другие способы.

3.3. В случае достижения целей обработки персональных данных или в случае утраты необходимости в достижении этих целей способом обезличивания является уменьшение перечня обрабатываемых данных.

3.4. Ответственный за организацию обработки персональных данных назначается ответственным за проведение мероприятий по обезличиванию персональных данных.

3.5. Решение о необходимости обезличивания персональных данных и способе обезличивания принимает ответственный за организацию обработки персональных данных.

3.6. Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

3.7. Обезличенные персональные данные могут обрабатываться с использованием и без использования средств автоматизации.

3.8. При использовании процедуры обезличивания не допускается совместное хранение персональных данных и обезличенных данных.

3.9. Обработка персональных данных до осуществления процедур обезличивания и после выполнения операции должна осуществляться в соответствии с законодательством Российской Федерации с применением мер по обеспечению безопасности персональных данных.

**4. Ответственность**

4.1. Ответственность за осуществление контроля выполнения требований настоящей инструкции несет ответственный за организацию обработки персональных данных Оператора.

4.2. Ответственность за выполнение настоящей инструкции возлагается на Администратора информационных систем персональных данных и всех работников Оператора, допущенных к обработке обезличенных персональных данных, в соответствии с действующим законодательством Российской Федерации.

Приложение № 18

к Положению об обработке и

защите персональных данных в

БУ «Сургутский музыкальный колледж»

**Инструкция по обработке персональных данных**

**в комплексной информационно-сервисной системе биометрической идентификации «Школьное окно»**

Комплексная информационно-сервисная система биометрической идентификации «Школьное окно» (далее – информационно-сервисная система) используется в БУ «Сургутский музыкальный колледж» (далее – колледж, оператор) с целью обеспечения безопасности в здании колледжа, расположенном по адресу: Тюменская область, Ханты-Мансийский автономный округ – Югра, г. Сургут, ул. Энтузиастов, дом 28, организации контрольно-пропускного режима (предотвращения проникновения в здание колледжа посторонних лиц, ведения статистики количества лиц, находящихся в здании), а так же контроля и учета рабочего времени работников колледжа.

1. Вход в здание колледжа через информационно-сервисную систему осуществляется по магнитным картам или по идентификации биометрических персональных данных (дактилоскопических данных – отпечатков пальцев). Работники колледжа и совершеннолетние обучающиеся проходят по магнитным картам или по идентификации отпечатков пальцев, несовершеннолетние обучающиеся – только по магнитным картам.

2. Обработка персональных данных в информационно-сервисной системе осуществляется с письменного согласия субъекта персональных данных, либо с согласия родителя (законного представителя) несовершеннолетнего субъекта персональных данных.

2.1. Согласие работника на обработку персональных данных, в том числе биометрических (дактилоскопических), получают начальник отдела кадров и документационного обеспечения управления, специалист по документационному обеспечению персонала на этапе приема на работу.

2.2. Согласие совершеннолетних обучающихся на обработку персональных данных, в том числе биометрических (дактилоскопических), согласие родителей (законных представителей) несовершеннолетних обучающихся на обработку персональных данных получают работники учебной части (специалист учебной части, методист) на этапе приема на обучение.

3. Сбор персональных данных для их обработки в информационно-сервисной системе осуществляется путем получения их непосредственно от субъекта персональных данных или родителей (законных представителей) несовершеннолетних субъектов.

3.1. Сбор персональных данных, включая биометрические персональные данные (дактилоскопические данные – отпечатки пальцев), производится ответственным за обработку персональных данных в информационно-сервисной системе лицом – системным администратором колледжа.

3.2. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки; для совершеннолетних обучающихся и работников колледжа - это ФИО, число, месяц, год рождения и, по желанию, биометрические персональные данные (отпечатки пальцев); для несовершеннолетних обучающихся - ФИО, число, месяц, год рождения.

3.3. Сбор и обработка биометрических персональных данных производится с помощью сканера отпечатков пальцев и заносится в базу данных не в виде изображения отпечатков пальцев, а в виде математических шаблонов, по которым получить исходное изображение невозможно, что обеспечивает защиту таких персональных данных от несанкционированного использования.

4. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных.

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

5.1. Системный блок, на котором производится обработка персональных данных, включая биометрические, располагается в помещении контрольно-пропускного пункта колледжа (город Сургут, улица Энтузиастов, дом 28, 1 этаж). Доступ в помещение находится под контролем сотрудника охраны.

5.2. Доступ к компьютеру и к программному обеспечению обработки персональных данных имеет лицо, ответственное за обработку персональных данных в системе безопасности - системный администратор. Компьютер защищен паролями – на вход в систему, на вход в программное приложение обработки персональных данных.

5.3. Лицом, ответственным за обработку персональных данных в системе безопасности - системным администратором, один раз в месяц производится резервное копирование данных.

5.4. Для защиты от сбоев электроэнергии компьютер подключен через источник бесперебойного питания (ИБП).

6. Обработка персональных данных в информационно-сервисной системе осуществляется с использованием средств автоматизации в следующем порядке:

6.1. После внесения персональных данных (в том числе биометрических) в базу данных программного приложения информационно-сервисной системы, обработка персональных данных осуществляется автоматизированно.

6.2. Ядром информационно-сервисной системы является система контроля и управления доступом, включающая:

- сенсоры отпечатков пальцев и магнитных карт, соединённые с сервером по локальной сети;

- базу данных, содержащую записи с чётким соответствием набора зарегистрированных шаблонов отпечатков пальцев для каждого субъекта персональных данных;

- приложение, осуществляющее обработку отпечатков пальцев, сравнение с шаблоном, вызов модуля реакции на идентификационное событие;

- модули реакции на идентификационные события: управление турникетом.

6.3. Вход в здание колледжа оборудован турникетами, связанными с сенсорами отпечатков. При прикладывании магнитной карты или отпечатка пальца к сенсору происходит идентификация данных субъекта с базой данных на сервере и при совпадении происходит открытие турникета.

7. Прекращение обработки персональных данных и их удаление из системы осуществляется, когда достигнуты цели обработки персональных данных: при увольнении работника, отчислении обучающегося.