МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ ЧЕЛЯБИНСКОЙ ОБЛАСТИ

государственное бюджетное образовательное учреждение
среднего профессионального образования
(среднее специальное учебное заведение)
«Челябинский радиотехнический техникум»

СОГЛАСОВАНО
Секретарь Совета техникума
_____ Н.М. Моторина
«30» августа 2013г.
Протокол №110

УТВЕРЖДАЮ
Директор ГБОУ СПО (ССУЗ) «ЧРТ»
_____ Е.Ю. Ломоносова
«01» сентября 2013г.

ПОЛОЖЕНИЕ

О ПОРЯДКЕ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ СОТРУДНИКОВ И СТУДЕНТОВ

Челябинск, 2013г.

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение об обработке персональных данных (далее — Положение) ГБОУ СПО (ССУЗ) «Челябинский радиотехнический техникум» (далее - техникум) разработано в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации (глава 14. Защита персональных данных работника), Гражданским кодексом Российской Федерации, Федеральным законом «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ, Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ, Постановлением Правительства РФ от 15.09.2008г. №687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», а также другими нормативно-правовыми актами, действующими на территории Российской Федерации.

1.2. Цели разработки Положения:

1.2.1. определение порядка обработки персональных данных сотрудников и студентов техникума, а также иных субъектов персональных данных, персональные данные которых подлежат обработке на основании полномочий техникума;

1.2.2. обеспечение защиты прав и свобод человека и гражданина, в т.ч. сотрудников и студентов техникума, при обработке их персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну;

1.2.3. установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.3. К любой информации, содержащей персональные данные субъекта, применяется режим конфиденциальности, за исключением:

1.3.1. обезличенных персональных данных;

1.3.2. общедоступных персональных данных.

1.4. Режим конфиденциальности персональных данных снимается в случаях их обезличивания и по истечении срока их хранения, или продлевается на основании заключения экспертной комиссии техникума, если иное не определено законом Российской Федерации.

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

1.5. **Блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных) *(ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).*

1.6. **Информационная система персональных данных (ИСПДн)** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств *(ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).*

1.7. **Документированная информация** - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель *(ст. 2 ФЗ РФ от 27.07.2006 г. N 149-ФЗ «Об информации, информационных технологиях и защите информации»).*

1.8. **Информация** - сведения (сообщения, данные) независимо от формы их представления *(ст. 2 ФЗ РФ от 27.07.2006 г. N 149-ФЗ «Об информации, информационных технологиях и защите информации»).*

1.9. **Обезличивание персональных данных** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных *(ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).*

1.10. **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 (*ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).*

1.11. **Обработка персональных данных без использования средств автоматизации** – обработка персональных данных, при которой такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека *(Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утв. постановлением Правительства РФ от 15.09.2008 N 687).*

1.12. **Оператор** – ГБОУ СПО (ССУЗ) «Челябинский радиотехнический техникум».

1.13. **Персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (*ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).*

1.14. **Распространение персональных данных** - действия, направленные на раскрытие персональных данных неопределенному кругу лиц (*ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).*

1.15. **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 (*ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).*

СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

1.16. Состав персональных данных, обрабатываемых в техникуме, определяется «Перечнем сведений, содержащих персональные данные» (Приложение 1).

1.17. Документы со сведениями, содержащими персональные данные, обрабатываются в следующих структурных подразделениях техникума:

1.17.1. бухгалтерия;

1.17.2. отдел кадров.

ПОРЯДОК ПОЛУЧЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

1.18. Персональные данные следует получать непосредственно у субъекта, либо у законного представителя.

1.19. Перед началом обработки персональных данных необходимо получить у субъекта согласие в письменной виде в соответствии с утвержденной в техникуме формой такого Согласия.

1.20. Комплекс документов, сопровождающий процесс взаимодействия с соискателями вакантной должности:

1.20.1. Соискатель направляет работодателю резюме в электронном виде или на бумажном носителе. Во время собеседования соискатель заполняет анкету кандидата, содержащую следующую информацию:

1.20.1.1. фамилия, имя, отчество;

1.20.1.2. дата рождения;

1.20.1.3. семейное положение;

1.20.1.4. количество и возраст детей;

1.20.1.5. фамилия, имя, отчество супруга(и) и родителей, их место работы и должность;

1.20.1.6. условия проживания;

1.20.1.7. адрес места жительства;

1.20.1.8. адрес регистрации;

1.20.1.9. контактные телефоны;

1.20.1.10. сведения об образовании;

1.20.1.11. сведения о предыдущих местах работы;

1.20.1.12. сведения об ограничениях в работе, связанных с состоянием здоровья.

1.20.2. В случае приема соискателя в техникум в качестве сотрудника резюме и анкета кандидата хранятся в его личном деле (в течение всего срока хранения личного дела). Если соискатель не явился на собеседование или не был принят на работу в техникум после собеседования, данные документы уничтожаются в течение 5 (Пяти) рабочих дней.

1.20.3. В случае если сотрудник отдела кадров техникума получил резюме в электронном виде, но в данный момент не существует вакантной должности для данного соискателя, сотрудник отдела кадров сохраняет резюме и помещает его в кадровый резерв сроком на 1 (Один) год.

1.21. Комплекс документов, сопровождающий процесс оформления трудовых отношений сотрудника техникума при его приёме, переводе и увольнении:

1.21.1. Информация, представляемая сотрудником при поступлении на работу в техникум, должна иметь документальную форму. При заключении трудового договора в соответствии со ст. 65 Трудового кодекса Российской Федерации лицо, поступающее на работу, предъявляет работодателю:

1.21.1.1. паспорт или иной документ, удостоверяющий личность;

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

1.21.1.3. страховое свидетельство государственного пенсионного страхования;

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

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

1.21.1.6. свидетельство о присвоении ИНН (при его наличии у сотрудника);

1.21.1.7. справку о наличии (отсутствии) судимости и (или) факта уголовного преследования по реабилитирующим основаниям, выданную в порядке и по форме, которые устанавливаются федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере внутренних дел,- при поступлении на работу, связанную с деятельностью, к осуществлению которой в соответствии с настоящим Кодексом, иным федеральным законом не допускаются лица, имеющие или имевшие судимость, подвергающиеся или подвергавшиеся уголовному преследованию.

1.21.2. При оформлении сотрудника в техникум начальником отдела кадров заполняется унифицированная форма Т-2 «Личная карточка сотрудника», в которой отражаются следующие анкетные и биографические данные сотрудника:

1.21.2.1. табельный номер, ИНН,СНИЛС;

1.21.2.2. общие сведения (Ф.И.О. дата рождения, место рождения, гражданство, образование, профессия, стаж работы, состояние в браке, паспортные данные);

1.21.2.3. сведения о воинском учете;

1.21.2.4. сведения о военно-учетной специальности;

1.21.2.5. данные о приеме на работу;

1.21.3. В дальнейшем в личную карточку вносятся:

1.21.3.1. сведения о переводах на другую работу;

1.21.3.2. сведения об аттестации;

1.21.3.3. сведения о повышении квалификации;

1.21.3.4. сведения о профессиональной переподготовке;

1.21.3.5. сведения о наградах (поощрениях), почетных званиях;

1.21.3.6. сведения об отпусках;

1.21.3.7. сведения о социальных гарантиях;

1.21.3.8. сведения о месте жительства и контактных телефонах.

1.21.4. Вся информация копируется в ИСПДн личное сотрудника.

1.21.5. В отделе кадров техникума создаются и хранятся следующие группы документов, содержащие персональные данные сотрудников в единичном или сводном виде:

1.21.5.1. документы, содержащие персональные данные сотрудников (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 сотрудников; дела, содержащие основания к приказу по личному составу; дела, содержащие материалы аттестации сотрудников; служебных расследований; справочно-информационный банк данных по персоналу (картотеки, журналы); подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству техникума, руководителям структурных подразделений; копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения);

1.21.5.2. документация по техникуму, работе отделов (положения, должностные инструкции сотрудников, приказы директора техникума);

1.21.5.3. документы по планированию, учету, анализу и отчетности в части работы с персоналом техникума.

1.22. Комплекс документов, сопровождающий процесс работы со студентами.

1.22.1. Информация, представляемая студентами, либо их представителями в структурные подразделения техникума, должна иметь документальную форму. Студенты, либо их представители предъявляют следующие документы:

1.22.1.1. паспорт или иной документ, удостоверяющий личность;

1.22.2. При обращении поступающего для обучения лица в техникум, ответственный секретарь приемной комиссии принимает от абитуриента заявление в электронном виде, в котором отражаются следующие анкетные и биографические данные:

1.22.2.1. фамилия, имя, отчество;

1.22.2.2. дата рождения;

1.22.2.3. место рождения;

1.22.2.4. гражданство;

1.22.2.5. паспортные данные;

1.22.2.6. адрес места жительства;

1.22.2.7. контактный телефон;

1.22.2.8. специальность;

1.22.2.9. Ф.И.О. законного представителя;

1.22.2.10. наименование образовательного учреждения;

1.22.2.11. серия, номер аттестата;

1.22.2.12. сведения о состоянии здоровья;

1.22.2.13. дополнительные сведения о себе.

1.22.3. Вся информация копируется в ИСПДн личное дело студента.

ПОРЯДОК ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

1.23. Хранение бумажных документов, электронных носителей (дискет, дисков и т.п.), содержащих персональные данные, должно осуществляться в специальных папках, закрытых шкафах или сейфах, в порядке, исключающем доступ к ним третьих лиц.

1.24. Безопасность персональных данных при их обработке с использованием технических и программных средств обеспечивается с помощью системы защиты персональных данных, включающей в себя организационные меры и средства защиты информации, удовлетворяющие устанавливаемым в соответствии с законодательством РФ требованиям, обеспечивающим защиту информации.

1.25. Обработка персональных данных в техникуме осуществляется до утраты правовых оснований обработки персональных данных. Перечень нормативно-правовых актов, определяющих основания обработки персональных данных в техникуме определяются «Перечнем сведений, содержащих персональные данные» (Приложение 1).

1.26. Срок хранения документов, содержащих персональные данные, определяется «Перечнем типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения», утвержденный Приказом Министерства культуры РФ от 25.08.2010 № 558.

1.27. По истечении срока хранения документы, либо иные материальные носители персональных данных должны быть уничтожены без возможности восстановления (например, в бумагорезательных машинах) с составлением акта. Для машинных носителей допускается гарантированное удаление информации методом многократной перезаписи с помощью специализированных программ (например, «Safe Erase», «Eraser», «FDelete») без уничтожения материального носителя.

1.28. Обезличивания персональных данных в техникуме не предполагается.

ПОРЯДОК ИСПОЛЬЗОВАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

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

1.30. Обработка персональных данных может осуществляться исключительно в целях предоставления:

-начального профессионального образования;

-среднего профессионального образования;

-услуги по содержанию и воспитанию;

-организации и проведения мероприятий в сфере образования,

принятия решения о трудоустройстве, кадрового планирования, осуществления трудовых отношений, и в случаях, установленных законодательством Российской Федерации.

1.31. Все персональные данные необходимо получать у субъекта персональных данных (либо у законных представителей). Если персональные данные возможно получить только у третьей стороны, то субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие.

1.32. Обработка персональных данных осуществляется с согласия в письменной форме субъекта персональных данных.

1.33. При определении объема и содержания, обрабатываемых персональных данных техникум должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ, Федеральным законом «Об образовании в Российской Федерации» от 29.12.2012 №273-ФЗ и иными нормативно-правовыми актами Российской Федерации, а также настоящим Положением.

ПОРЯДОК ПЕРЕДАЧИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1.34. Передавать персональные данные субъектов допускается только тем сотрудникам, которые имеют допуск к обработке персональных данных.

1.35. Предоставление персональных данных допускается в случаях передачи налоговой бухгалтерской и иной отчетности, передачи сведений о заработной плате в банковские и иные кредитные организации при официальном запросе, раскрытии данных правоохранительным органам при наличии законных оснований, а также в иных случаях, установленным законодательством РФ.

1.36. Не допускается распространение персональных данных субъекта.

ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

1.37. Защита персональных данных субъекта от неправомерного их использования или утраты обеспечивается техникумом.

1.38. В техникуме защите подлежат все сведения, содержащие персональные данные субъектов, в том числе:

1.38.1. зафиксированные в бумажных документах;

1.38.2. зафиксированные в электронных документах на технических средствах, включая внешние носители;

1.38.3. речевая (акустическая) информация, содержащая персональные данные;

1.38.4. текстовая и графическая видовая информация, содержащая персональные данные;

1.39. Защита персональных данных должна вестись по трём взаимодополняющим направлениям:

1.39.1. Проведение организационных мероприятий:

1.39.1.1. разработка и внедрение внутренних организационно-распорядительных документов, регламентирующих обработку и защиту персональных данных субъектов, в том числе порядок доступа в помещения и к персональным данным;

1.39.1.2. ознакомление сотрудников с законодательством Российской Федерации и внутренними нормативными документами, получение обязательств, касающихся обработки персональных данных;

1.39.1.3. проведение обучения сотрудников вопросам защиты персональных данных.

1.39.2. Программно-аппаратная защита:

1.39.2.1. разработка модели угроз безопасности персональным данным;

1.39.2.2. внедрение программно-аппаратных средств защиты информации, прошедших в соответствии с Федеральным законом №184 от 27.12.2002 г. «О техническом регулировании» оценку соответствия;

1.39.2.3. организация учёта носителей персональных данных.

1.39.3. Инженерно-техническая защита:

1.39.3.1. установка сейфов или запирающихся шкафов для хранения носителей персональных данных;

1.39.3.2. установка усиленных дверей, сигнализации, режима охраны здания и помещений, в которых обрабатываются персональные данные.

1.40. Определение конкретных мер, общую организацию, планирование и контроль выполнения мероприятий по защите персональных данных осуществляет ответственный за организацию обработки персональных данных в соответствии с законодательством в области защиты персональных данных и локальными нормативно-правовыми актами техникума.

1.41. Организацию и контроль защиты персональных данных в структурных подразделениях техникума осуществляют их непосредственные руководители.

ПОРЯДОК ПРЕДОСТАВЛЕНИЯ ДОСТУПА К ПЕРСОНАЛЬНЫМ ДАННЫМ

1.42. Допуск к персональным данным субъекта могут иметь только те сотрудники техникума, которым персональные данные необходимы в связи с исполнением ими своих трудовых обязанностей. Перечень таких сотрудников отражен в «Приказе об утверждении списка должностных лиц, которым необходим доступ к персональным данным, обрабатываемым в информационных системах».

1.43. Процедура оформления допуска к персональным данным представляет собой следующую строгую последовательность действий:

1.43.1. ознакомление сотрудника под роспись с настоящим Положением, «Инструкцией о порядке работы с персональными данными» и другими локальными нормативно-правовыми актами техникума, касающимися обработки персональных данных;

1.43.2. истребование с сотрудника «Обязательства о неразглашении конфиденциальной информации»;

1.44. Каждый сотрудник должен иметь доступ к минимально необходимому набору персональных данных субъектов, необходимых ему для выполнения служебных (трудовых) обязанностей.

1.45. Сотрудникам, не имеющим надлежащим образом оформленного допуска, доступ к персональным данным субъектов запрещается.

1.46. Специалисты техникума, которым доступ к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных обязанностей (далее – пользователи), для получения доступа к информационной системе направляют письменный запрос на имя ответственного за организацию обработки персональных данных.

ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

1.47. Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется сотрудниками техникума без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами техникума.

1.48. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

1.49. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

1.50. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются приказом директора техникума.

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

1.51. Состав информационных систем персональных данных техникума и их характеристика определяется «Перечнем информационных систем персональных данных» (Приложение 2).

1.52. Под техническими средствами, позволяющими осуществлять обработку персональных данных, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных, программные средства, средства защиты информации, применяемые в информационных системах.

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

1.54. Средства защиты информации, применяемые в информационных системах, в обязательном порядке проходят процедуру оценки соответствия в установленном законодательством РФ порядке.

1.55. Информационные системы классифицируются на основании приказа директора техникума, в соответствии с «Порядком проведения классификации информационных систем персональных данных», утвержденным приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20, в зависимости от объема обрабатываемых ими персональных данных и угроз безопасности жизненно важным интересам личности, общества и государства.

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

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

1.58. Безопасность персональных данных при их обработке в информационной системе персональных данных обеспечивает специалист, ответственный за организацию обработки информационных систем персональных данных (администратор безопасности ИСПДн).

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

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

1.59.2. своевременное обнаружение фактов несанкционированного доступа к персональным данным;

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

1.59.4. возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

1.59.5. постоянный контроль над обеспечением уровня защищенности персональных данных.

1.60. Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают:

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

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

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

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

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

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

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

1.60.8. контроль по соблюдению условий использования средств защиты информации, предусмотренных эксплуатационной и технической документации;

1.60.9. разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим

нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

1.60.10. описание системы защиты персональных данных.

1.61. Иные требования по обеспечению безопасности информации и средств защиты информации в техникуме выполняются в соответствии с требованиями федеральных органов исполнительной власти и органов исполнительной власти Челябинской области.

ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ОБРАБОТКУ И ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ

1.62. Ответственность за соблюдение требований по защите информации ограниченного доступа и надлежащего порядка проводимых работ возлагается на пользователей ИСПДн, администратора безопасности ИСПДн и ответственного за организацию обработки персональных данных техникума.

1.63. Руководитель структурного подразделения, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

1.64. Сотрудники техникума, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации. Разглашение персональных данных субъекта (передача их посторонним лицам, в том числе другим сотрудникам, не имеющим к ним допуск), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных настоящим Положением, локальными нормативно-правовыми актами (приказами, распоряжениями) техникума, влечет наложение на сотрудника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде: замечания, выговора, увольнения.

1.65. Сотрудник техникума, имеющий доступ к персональным данным субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба в соответствии с п.7 ст. 243 Трудового кодекса РФ.

1.66. Директор техникума за нарушение норм, регулирующих получение, обработку и защиту персональных данных субъектов, несет административную ответственность согласно ст. 5.27 и 5.39 Кодекса об административных правонарушениях Российской Федерации, а также возмещает субъекту ущерб, причиненный неправомерным использованием информации, содержащей персональные данные этого субъекта.

ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

1.67. Настоящее Положение утверждается директором техникума, согласовано на заседании Совета техникума и является обязательным для исполнения всеми сотрудниками, имеющими доступ к персональным данным.

1.68. Все сотрудники техникума, участвующие в обработке персональных данных, должны быть ознакомлены с настоящим Положением под роспись.

Приложения:

1. «Перечень сведений, содержащих персональные данные» на 5 л. в 1 экз.;
2. «Перечень информационных систем персональных данных» на 1 л. в 1 экз.;
3. Лист ознакомления с «Положением об обработке персональных данных» на 1 л. в 1 экз.