МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЮУрГГПУ»)
Профессионально-педагогический институт
Кафедра автомобильного транспорта, информационных технологий и методики обучения техническим дисциплинам

Организация режима защиты конфиденциальной информации в организации профессионального образования

Выпускная квалификационная работа
по направлению 44.04.04 Профессиональное обучение
Направленность программы магистратуры
«Управление информационной безопасности в профессиональном образовании»

Проверка на объём заимствований:
_____ % авторского текста

Выполнил:
студент гр. ЗФ-309/210-2-1
Муратов Руслан Рашитович

Работа рекомендована к защите
«___» _____2017 г.

Зав. кафедрой АТ,ИТиМОТД
_____В.В. Руднев

Научный руководитель:
к.п.н., доцент кафедры АТ, ИТ и МОТД
Диденко Галина Александровна

Челябинск, 2017

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное
учреждение высшего образования
Южно-Уральский государственный гуманитарно-педагогический университет
(ФГБОУ ВО «ЮУрГГПУ»)
Профессионально-педагогический институт
Кафедра автомобильного транспорта, информационных технологий
и методики обучения техническим дисциплинам

Направление подготовки: 44.04.04. «Профессиональное обучение»
Программа подготовки магистров «Управление информационной безопасностью в профессиональном образовании»

ЗАДАНИЕ
на выпускную квалификационную работу
(магистерскую диссертацию)

Магистранту Муратову Руслану Рашитовичу, обучающемуся в группе ЗФ-309/210-2-1 по направлению подготовки 44.04.04. «Профессиональное обучение (Управление информационной безопасностью в профессиональном образовании)»

Научный руководитель квалификационной работы: Диденко Г.А., к.п.н., доцент кафедры АТ, ИТ и МОТД.

1.Тема квалификационной работы: «Организация режима защиты конфиденциальной информации в организации профессионального образования», утверждена приказом Южно-уральского государственного гуманитарно-педагогического университета № 539-сз от «10» __03____ 2016 г.

2. Срок сдачи магистрантом законченной работы на кафедру « _» __2017 г.

3. Содержание и объем работы (пояснительной расчетной и экспериментальной частей, т.е. перечень подлежащих разработке вопросов):

– раскрыть сущность и содержание защиты персональных данных в организациях профессионального образования;

– раскрыть задачи, функции, организационную структуру ГБПОУ «Южноуральский энергетический техникум»;

– раскрыть методы предпроектного исследования и проектирования образовательной организации защиты персональных данных в ГБПОУ «Южноуральский энергетический техникум»

– проанализировать организацию защиты персональных данных в ГБПОУ «Южноуральский энергетический техникум»;

– разработать мероприятия по совершенствованию организации защиты персональных данных в ГБПОУ «Южноуральский энергетический техникум».

4. Материалы для выполнения квалификационной работы:

- Учебная, научно-техническая, педагогическая, методическая, нормативно-правовая литература по теме выпускной квалификационной работы (магистерской диссертации).
- Материалы научно-исследовательской работы, педагогической и

преддипломной практики.

5. Перечень графического материала (с точным указанием обязательных таблиц, чертежей или графиков, образцов и др.) Таблица, таблицы и диаграммы результатов экспериментальной проверки внедрения в организации СПО и экспертной проверки действующих педагогов и руководителей СПО и ВО, а также технических специалистов.

6. Консультанты по специальным разделам ВКР:

Раздел	Консультант	Отметка о

Дата выдачи задания «_____» _____ 2017 года

Задание выдал, зав. кафедрой АТ, ИТ и МОТД
к.т.н., доцент _____ Руднев В.В.

Задание принял _____ Муратов Р.Р.

КАЛЕНДАРНЫЙ ПЛАН
выполнения выпускной квалификационной работы
(магистерской диссертации)

№ п/п	Наименование этапов подготовки выпускной квалификационной работы	Срок выполнения этапов ВКР	Отметка о выполнении
1	Предзащита ВКР	21.11.2017г.	
2	Доработка ВКР после предзащиты		
3	Нормоконтроль		
4	Подписание ВКР научным руководителем		
5	Оформление пояснительной записки и презентации ВКР		
6	Подписание рецензии на ВКР		
7	Защита ВКР на заседании ГАК	14.12.2017г.	

Автор _____ Муратов Р.Р.

Научный руководитель,
к.п.н., доцент кафедры АТ, ИТ и МОТД _____ Диденко Г.А.

Заведующий кафедрой АТ, ИТ и МОТД
к.т.н., доцент _____ Руднев В.В.

Содержание

Введение

Защита персональных данных, приобретает все более важное значение, так как в XXI веке у человечества, появляется все больше новых объектов, нуждающихся в защите путем закрепления соответствующих норм в законе. Основной объект в настоящее время – это информация. В наше время общество всецело зависит от получаемых, обрабатываемых и передаваемых данных. По этой причине данные сами по себе приобретают высокую ценность. И тем больше цена полезной информации, чем выше ее сохранность.

В Трудовом кодексе Российской Федерации N 197 ФЗ от 30.12.2001 впервые появилась специальная глава, посвященная защите персональных данных работника в организации (от. 85-90).

Работодатель всегда собирал данные о личности работника. Для этой цели использовались «Личный листок» и различные анкеты, а также письменные характеристики и т.д. Однако официальная правовая регламентация обработки этих данных, доступная работнику, отсутствовала.

Персональные данные являются важнейшим активом любой современной организации и в то же время её серьезной проблемой. Утечка персональных данных не выгодна ни организации: она испытывает серьезные репутационные потери и получает конфликт с законом, ни владельцам этой информации, так как они испытывают как минимум беспокойство, а нередко становятся жертвами различных афер.

В виду вышесказанного, законодательными актами, как в России, так и зарубежных стран предусматривают немалое количество норм, направленных на регулирование создания, пользования, передачи и защиты информации во всех ее формах.

Особой ценностью обладает информация, несущая в себе данные о личной, индивидуальной или семейной жизни человека. Закрепляет основной принцип современного демократического общества: «Человек, его права и свободы являются высшей ценностью». Соответственно и информация, непосредственно

затрагивающая частные интересы человека должны уважаться и защищаться государством.

В повседневной жизни человека сохранность информации «о его жизни» зависит от него самого. Но совсем другая ситуация, когда мы обязаны предоставить данные о себе в соответствии с законом третьему лицу, а конкретно – работодателю. Работник в данной ситуации передает конфиденциальную информацию о себе на ответственное хранение. Далее за сохранность данных отвечает уже работодатель. Способы их защиты, а также ответственность работодателя за невыполнение обязательств по обеспечению сохранности персональных данных.

Проблемы функционирования систем обеспечения информационной безопасности нашли отражение в трудах А.А. Герасимова [27], А.А. Грушо [28], С.В. Дворянкина [31], В. А. Минаева [41], С.В. Скрыля [50], М.П. Сычева [51] и ряда других ученых.

Проблемы защиты персональных данных рассматривались в трудах российских ученых, таких как: А.В Меньшиковой [37], где она выделила некоторые проблемы защиты персональных данных работника и определила перспективы и пути их решения; проблемные вопросы понятия и сущности персональных данных в своих трудах рассмотрел А.В Минбалеев [38].

В настоящее время в образовательных учреждениях активно внедряются информационные системы, осуществляющие обработку персональных данных в образовательном учреждении, делопроизводство, бухгалтерские программы и др. Эти системы предназначены для ведения базы данных воспитанников, обучающихся, родителей и работников образовательных учреждений, оперативного управления учреждением. Образовательные учреждения должны отреагировать на требования законодательства о защите персональных данных участников образовательного процесса в первую очередь, т. к. речь идет о защите сведений, незаконное использование которых может серьезно отразиться на правах граждан.

Актуальность. Тема диссертации актуальна, так как лица, ответственные за

обработку персональных данных не всегда знают элементарных правил безопасности, доверенной им информации. Поэтому на специалистов по информационной безопасности возлагается не только ответственность за безопасность информационной системы, но система обучения персонала.

Гипотеза. Если будет реализован разработанный в диссертации комплекс мероприятий по защите персональных данных в ГБПОУ «Южноуральский энергетический техникум», то уровень защищенности персональных данных значительно повысится.

Объектом исследования является организация защиты данных в образовательном учреждении ГБПОУ «Южноуральский энергетический техникум».

Предмет – особенности организации защиты персональных данных.

Целью диссертации является анализ организации защиты персональных данных (на примере управления ГБПОУ «Южноуральский энергетический техникум»).

В соответствии с поставленной целью были выделены следующие **задачи**:

– раскрыть сущность и содержание защиты персональных данных в организациях профессионального образования;

– раскрыть задачи, функции, организационную структуру ГБПОУ «Южноуральский энергетический техникум»;

– раскрыть методы предпроектного исследования и проектирования образовательной организации защиты персональных данных в ГБПОУ «Южноуральский энергетический техникум»

– проанализировать организацию защиты персональных данных в ГБПОУ «Южноуральский энергетический техникум»;

– разработать мероприятия по совершенствованию организации защиты персональных данных в ГБПОУ «Южноуральский энергетический техникум».

В процессе написания выпускной квалификационной работы были использованы законодательные акты и нормативно-методические документы, регламентирующие организацию защиты персональных данных. Использование

законодательных актов и нормативно-методических документов было продиктовано темой исследования.

Основополагающие нормы, регулирующие отношения по поводу персональных данных, содержатся в Федеральном законе «О персональных данных» [6].

Федеральный закон «Об информации, информационных технологиях и защите информации» [5] определяет, процессы функционирования информации и документации в обществе, в системе государственного и хозяйственного управления. Настоящий закон регулирует отношения, возникающие при формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации; создании и использовании информационных технологий и средств их обеспечения; защите информации, прав субъектов, участвующих в информационных процессах и информатизации.

В качестве методического материала по защите персональных данных, использованы научные, учебные, практические материалы, подготовленные ведущими специалистами: Т. В. Кузнецовой [30], В.И. Петренко [42], О. В. Силакова [45]; регламентация работы с персональными данными – С. А. Борисова [25], М.А. Федосова [46] и др.

Для решения задач были использованы следующие методы исследования: анализ публикационного массива по теме, описание, наблюдение, изучение документов.

Научная новизна исследуемой проблемы заключается в том, что в диссертации предложен комплексный подход к вопросам организации защиты персональных данных в образовательной организации.

Практическая значимость данной работы заключается в создании эффективно действующей системы защиты персональных данных в образовательном учреждении.

Диссертация состоит из введения, трех глав, заключения, списка

использованных источников и литературы, приложений. Во введении обосновывается выбор темы исследования, ее актуальность, анализируется степень ее изученности, формулируются объект, предмет, цели, задачи, методологические основы исследования, структура работы.

В первой главе раскрываются теоретические основы организации защиты персональных данных системе управления организацией

Во второй главе рассматриваются цели, задачи, функции защиты персональных данных в образовательной организации.

В третьей главе разработаны мероприятия по совершенствованию организации защиты персональных данных в организации образования.

В заключении подводятся итоги проведенного исследования, формулируются основные выводы. Список использованной литературы содержит 55 источников по теме. Приложения дополняют текст выпускной квалификационной работы таблицами, рисунками.

Глава 1. Теоретические основы организации защиты персональных данных в системе управления организацией

1.1. Организация защиты персональных данных: основные понятия

В Федеральном законе № 197-ФЗ «Трудовой кодекс Российской Федерации» от 30.12.01 (с изменениями) (далее по тексту - ТК РФ) под персональными данными работника понимается информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника (ч.1 ст.85 ТК РФ) [19].

Легко заметить, что под указанное определение можно подвести любую информацию о работнике. И работодатели нередко собирают о сотруднике всю информацию, мотивируя это тем, что хотят иметь максимально полное представление о нем.

Довольно часто от работника требуют сообщить исчерпывающую информацию о его семейном положении и ближайших родственниках, о жилищных условиях, состоянии здоровья, о фактах привлечения к уголовной ответственности, о наличии постоянной регистрации по месту жительства и многое другое. Но такого рода информация никаким образом не относится к трудовой деятельности работника. Наоборот, тем самым работодатель переходит тонкую грань, отделяющую персональные данные от сведений, составляющих тайну частной жизни, личную или семейную тайну гражданина.

В.С. Плешенко, в учебном пособии «Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления», дает следующие определение персональным данным: «Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)» [45, с. 141].

В учебном пособии В.И. Аверченко дает такое определение персональным данным: «Персональные данные − любая информация, относящаяся к прямо или

косвенно определенному или определяемому физическому лицу (субъекту персональных данных)».

При поступлении на работу – это данные отдела кадров работодателя, которые работник указывает в личной карточке, автобиографии, других документах, заполняемых при заключении трудового договора.

При поступлении ребенка в детский сад, школу, институт, другие образовательные учреждения также заполняется множество анкет и форм, в которых указываются данные как ребенка (например, данные свидетельства о рождении), так и его родителей (вплоть до места работы, занимаемой должности).

При прохождении лечения в медицинских учреждениях необходимо указать не только паспортные данные, но и сведения о льготах, медицинских страховках, сведения о предыдущих лечениях, результаты анализов. Во многих медицинских учреждениях амбулаторные/стационарные карты дублируются в электронном виде. И все эти данные подлежат защите.

Персональные данные объективно присущи любому человеку, они подчеркивают правовой статус человека и гражданина. Персональные данные содержат необходимый объем информации о человеке, который участвует в соответствующих правоотношениях. Персональные данные принадлежат непосредственно человеку, и он в их несанкционированном распространении, как правило, не заинтересован, в этой связи неслучайно, что персональные данные охраняются различными правовыми средствами. Исходя из этого вполне логично, что доступ к персональным данным имеет весьма ограниченный круг лиц, работодатель, сотрудники кадровых служб и др. В этой связи значение персональных данных трудно переоценить. В настоящее время правовое регулирование персональных данных привлекает внимание ученых и специалистов-практиков.

В учебном пособии «Защита персональных данных в информационных системах В.И. Петренко определяет защиту персональных данных, как комплекс мероприятий технического, организационного и организационно-технического характера, направленных на защиту сведений, относящихся к определенному или

определяемому на основании такой информации физическому лицу (субъекту персональных данных)[46, с. 98].

Защита персональных данных представляет собой регламентированный технологический процесс, предупреждающий нарушение установленного порядка доступности, целостности, достоверности и конфиденциальности персональных данных и обеспечивающий безопасность информации в процессе управленческой и производственной деятельности компании[19, с. 114].

В процессе трудовой деятельности работника работодатель копит и хранит документы, содержащие персональные данные работника. Исходя из определения персональных данных, которое, такие сведения могут содержаться в следующих документах:

– трудовая книжка или ее копия со сведениями о трудовом стаже, предыдущих местах работы;

– копии свидетельств о заключении брака, рождении детей. Такие документы содержат сведения о составе семьи, которые могут понадобиться работодателю для предоставления работнику определенных льгот, предусмотренных трудовым и налоговым законодательством;

– копия документа, удостоверяющего личность работника. Здесь указываются фамилия, имя, отчество, дата рождения, адрес регистрации, семейное положение, состав семьи работника, а также реквизиты этого документа;

– анкета, автобиография, личный листок по учету кадров, которые заполняются работником при приеме на работу. В этих документах содержатся анкетные и биографические данные работника;

– личная карточка № Т-2. В ней указываются фамилия, имя, отчество работника, место рождения, состав семьи, образование, а также данные документа, удостоверяющего личность, и пр.;

– документы воинского учета с информацией об отношении работника к воинской обязанности и необходимы работодателю для осуществления в организации воинского учета работников;

– справка о доходах с предыдущего места работы. Нужна работодателю для предоставления работнику определенных льгот и компенсаций в соответствии с налоговым законодательством;

– документы об образовании с квалификацией работника;

– документы обязательного пенсионного страхования работника;

– трудовой договор со сведениями о должности работника, заработной плате, месте работы, рабочем месте, а также иные персональные данные работника;

– подлинники и копии приказов по личному составу. В них содержится информация о приеме, переводе, увольнении и иных событиях, относящихся к трудовой деятельности работника;

– при необходимости – иные документы, содержащие персональные данные работников.

Кроме того, работодатель в процессе своей деятельности собирает информацию о соискателях, необходимую для принятия решения о вступлении с ними в трудовые отношения. Если эта информация содержит персональные данные соискателей, к ней в полной мере относятся установленные законом требования о сборе, обработке, хранении, защите персональных данных.

Так же существует такое понятие как обработка персональных данных, что является неотъемлемой частью процесса защиты персональных данных.

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.

Можно выделить некоторые принципы обработки персональных данных.

Обработка персональных данных должна осуществляться на законной и справедливой основе.

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

Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

Обработке подлежат только персональные данные, которые отвечают целям их обработки.

Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

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. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

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

Существуют некоторые условия обработки персональных данных, которые перечислены ниже.

Обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных.

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

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

Обработка персональных данных необходима для предоставления государственной или муниципальной услуги в соответствии с Федеральным законом от 27 июля 2010 года N 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», для обеспечения предоставления такой услуги, для регистрации субъекта персональных данных на едином портале государственных и муниципальных услуг [12].

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

Обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно.

Обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных [30, с. 147].

Обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой

деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных.

Обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в статье 15 настоящего Федерального закона, при условии обязательного обезличивания персональных данных.

Осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее - персональные данные, сделанные общедоступными субъектом персональных данных).

Осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

Ниже кратко даны понятия, определяющие основные элементы системы защиты персональных данных:

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

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.

Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Таким образом, персональные данные – это, прежде всего, паспортные данные, сведения о семейном положении, сведения об образовании, номера ИНН, страхового свидетельства государственного пенсионного страхования, медицинской страховки, сведения о трудовой деятельности, социальное и имущественное положение, сведения о доходах. Такие данные есть практически в каждой организации.

Проведя теоретическое исследование основных понятий системы персональных данных можно дать следующее определение: «Защита персональных данных представляет собой регламентированный технологический процесс, предупреждающий нарушение установленного порядка конфиденциальности, целостности, доступности, достоверности персональных данных и обеспечивающий безопасность информации в процессе управленческой и производственной деятельности организации.

1.2.Нормативно-правовые основы работы с персональными данными в учреждении

Обработка персональных данных должна осуществляться на законной и справедливой основе, ограничиваться достижением конкретных заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных. Обрабатывать можно только те персональные, которые отвечают целям их обработки.

Федеральным законом от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации» установлены конкретные требования по обеспечению создания и ведения официального сайта образовательного учреждения в сети «Интернет», а так же требования к информационным системам в сфере образования.

В соответствии с новыми установленными законом требованиями образовательное учреждение обязано разместить на своём сайте сведения:

– о персональном составе педагогических работников с указанием уровня образования и квалификации;

– о доступе к информационным системам и информационно-телекоммуникационным сетям.

В этой связи нужно обратить внимание, что федеральным законом от 27 июля 2006 г. N 152-ФЗ «О персональных данных», установлены жёсткие требования к защите и обработке персональных данных. Обработка персональных данных преподавателей и обучающихся в большом объёме осуществляется в каждом образовательном учреждении, которое, как предусмотрено федеральным законом от 27 июля 2006 г. N 152-ФЗ «О персональных данных», обязаны принять меры по защите персональных данных. В свою очередь данные меры предусматривают, прежде всего, создание достаточно большого количества локальных нормативных актов образовательного учреждения.

Кроме того, статьёй 29 закона от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации» ещё более усилены требования к информационной

открытости образовательного учреждения. А статьёй 98 данного закона установлены требования к информационным системам в сфере образования, которые обязывают образовательные организации осуществлять обработку персональных данных указанных системах в строгом соответствии с законодательством.

Таким образом, обработка персональных данных должна осуществляться с соблюдением принципов и правил, предусмотренных Федеральным законом «О персональных данных» от 27.07.2006 года №152-ФЗ. Обработка персональных данных допускается в следующих случаях:

– обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

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

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

– обработка персональных данных необходима для предоставления государственной или муниципальной услуги в соответствии с Федеральным законом «Об организации предоставления государственных и муниципальных услуг» от 27.07. 2010 года № 210ФЗ, для обеспечения

– предоставления такой услуги, для регистрации субъекта персональных данных на едином портале государственных и муниципальных услуг;

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

– обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

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

– обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;

– обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в статье 15 Федерального закона «О персональных данных» от 27.07.2006 года №152-ФЗ, при условии обязательного обезличивания персональных данных;

– осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе;

– осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом;

– оператор имеет право поручить обработку персональных данных другому лицу при согласии субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, или путем принятия государственным или муниципальным органом соответствующего акта.

Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных предусмотренные Федеральным законом «О персональных данных» от

27.07.2006 года №152-ФЗ. В поручении оператора должны быть определены действия (операции) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, нужно установить обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона «О персональных данных» от 27.07.2006 года №152-ФЗ.

Лицо, осуществляющее обработку персональных данных по поручению оператора, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.

В случае, если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

Основополагающие нормы, регулирующие отношения по поводу персональных данных, содержатся в Федеральном законе «О персональных данных». В соответствии с п. 1 ст. 3 этого Закона персональными данными является любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация [7].

В соответствии с ч. 1 ст. 85 ГК РФ под персональными данными работника понимается информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника. Оценочный характер данного определения отражает лишь общий подход законодателя к категории персональных данных работника. Работодатель может собирать и обрабатывать не любую информацию о лице, являющемся его работником, а лишь ту, которая непосредственно связана с его трудовым правоотношением [3].

В 2012 году было принято новое Постановление Правительства №1119, а в 2013 году введён в действие новый Приказ ФСТЭК №21, а также очередные правки в Федеральном законе №152 от 27.07.2011. Данные документы предъявляют новые требования к оператору персональных данных.

Так же можно выделить еще три группы нормативных документов по защите персональных данных – это: методические материалы ФСТЭК России; Приказ ФСТЭК России о составе и содержании мер по обеспечению безопасности персональных данных в ИСПДн; Методические материалы ФСБ России [29, с. 89].

Методические материалы ФСТЭК России:

– «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 15 февраля 2008 года (При применении документа следует учитывать, что Постановлением Правительства РФ от 01.11.2012 N 1119 утверждены новые Требования к защите персональных данных при их обработке в информационных системах персональных данных).

– «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 14 февраля 2008 года (При применении документа следует учитывать, что Постановлением Правительства РФ от 01.11.2012 N 1119 утверждены новые Требования к защите персональных данных при их обработке в информационных системах персональных данных)..

Согласно Приказа ФСБ России от 10.07.2014 N 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» (Зарегистрировано в Минюсте России 18.08.2014 N 33620) методические материалы ФСБ России включают:

– состав и содержание организационных и технических мер, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для 4 уровня защищенности;

– состав и содержание организационных и технических мер, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для 3 уровня защищенности;

– состав и содержание организационных и технических мер, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для 2 уровня защищенности;

– состав и содержание организационных и технических мер, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для 1 уровня защищенности;

Требования[18]:

– являются обязательными для оператора, осуществляющего обработку персональных данных, а также лица, которому на основании договора оператор поручает обработку персональных данных и (или) лица, которому на основании договора оператор поручает оказание услуг по организации и обеспечению безопасности защиты персональных данных при их обработке в информационной системе с использованием криптосредств. При этом существенным условием договора является обязанность уполномоченного лица обеспечить конфиденциальность персональных данных и безопасность персональных данных при их обработке в информационной системе в случаях, предусмотренных действующим законодательством;

– распространяются на криптосредства, предназначенные для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, все технические средства которых находятся в пределах Российской Федерации, а также в системах, технические средства которых частично или целиком находятся за пределами Российской Федерации.

– не отменяют требования иных документов, регламентирующих порядок обращения со служебной информацией ограниченного распространения в

федеральных органах исполнительной власти.

Оператор с учетом особенностей своей деятельности может разрабатывать не противоречащие настоящим Требованиям методические рекомендации по их применению.

В соответствии с положениями федерального закона от 27 декабря 2009 года № 363-ФЗ «О внесении изменений в статьи 19 и 25 Федерального закона «О персональных данных», вступившего в силу 29 декабря 2009 года, в законе № 152-ФЗ в части 1 статьи 19 было исключено требование использования оператором

приhttps://ru.wikipedia.org/wiki/%D0%9E%D0%B1%D1%80%D0%B0%D0%B1%D0%BE%D1%82%D0%BA%D0%B0_%D0%BF%D0%B5%D1%80%D1%81%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D1%85_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85 обработке персональных данных шифровальных (криптографических) средств. Таким образом, требования методических материалов, разработанных ФСБ России и направленных на разъяснение требований по обеспечению безопасности ПД путем организации криптографической защиты данных, перестали носить обязательный характер [11].

В соответствии со ст. 24 лица ФЗ «О персональных данных», виновные в нарушении требований этого федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность Закона № 152-ФЗ «О персональных данных». Неисполнение требований Закона № 152-ФЗ «О персональных данных» операторами баз данных может повлечь: гражданские иски со стороны работников; репутационные риски; приостановление или прекращение обработки персональных данных в школе, осуществляемой с нарушением требований Закона № 152-ФЗ «О персональных данных»; направление в органы прокуратуры, другие правоохранительные органы материалов для решения вопроса о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов персональных данных; привлечение к административной и уголовной ответственности лиц, виновных в

нарушении соответствующих статей Уголовного кодекса РФ и Кодекса РФ об административных правонарушениях. В соответствии со ст. 90 ТК РФ, устанавливающей ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника, виновные в этом лица привлекаются к дисциплинарной, материальной, гражданско-правовой, административной и уголовной ответственности в порядке, установленном ТК РФ и иными федеральными законами.

1 июля 2017 года вступает в силу Федеральный закон от 07.02.2017 № 13-ФЗ, который вносит поправки в ст. 13.11 КоАП. В частности, он предусматривает расширение перечня оснований для привлечения к административной ответственности за незаконную обработку персональных данных (ПДн) и существенное увеличение штрафов.

Таким образом, нормативной основой защиты персональных данных являются нормы Конституции РФ, Федерального закона «О персональных данных», Указ Президента РФ «О перечне сведений конфиденциального характера», требования и другие нормативно-правовые акты Российской Федерации.

1.3. Технология защиты персональных данных в организации

Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. При обработке персональных данных должны быть обеспечены точность достаточность, а в необходимых случаях и актуальность персональных данных по отношению к целям обработки персональных данных.

Хранить персональные данные нужно в форме, которая позволяет определить субъект персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен Федеральным законом, договором, стороной которого получателем или поручителем является субъект персональных данных. После достижения

целей обработки, персональные данные необходимо уничтожить либо обезличить, если иное не предусмотрено федеральным законом.

В общих чертах защита персональных данных сводится к созданию режима обработки персональных данных, включающего:

– разработку внутренней документации по работе с персональными данными;

– создание организационной структуры системы защиты персональных данных;

– внедрение технических мер защиты персональных данных;

– получение сертификатов регулирующих органов (Федеральной службы безопасности и Федеральной службой по техническому и экспортному контролю) на средства защиты информации;

– при необходимости, получение лицензий регулирующих органов (Федеральной службы безопасности и Федеральной службой по техническому и экспортному контролю). Лицензия Федеральной службы по техническому и экспортному контролю России на Техническую защиту конфиденциальной информации, нужна только в случае если организация оказывает услуги по созданию системы защиты персональных данных для других лиц. При создании системы защиты персональных данных силами организации (для собственных нужд) как техническими средствами, так и организационными – данная лицензия не нужна.

Безопасность персональных данных при их обработке в информационной системе обеспечивает оператор этой системы, который обрабатывает персональные данные (далее – оператор), или лицо, осуществляющее обработку персональных данных по поручению оператора на основании заключаемого с этим лицом договора (далее – уполномоченное лицо). Договор между оператором и уполномоченным лицом должен предусматривать обязанность уполномоченного лица обеспечить безопасность персональных данных при их обработке в информационной системе.

Выбор средств защиты информации для системы защиты персональных

данных осуществляется оператором в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю во исполнение Федерального закона «О персональных данных».

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

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

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

Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится оператором с учетом оценки возможного вреда, проведенной во исполнение Федерального закона «О персональных данных», и в соответствии с нормативными правовыми актами, принятыми во исполнение Федерального закона «О персональных данных».

При обработке персональных данных в информационных системах устанавливаются 4 уровня защищенности персональных данных.

Необходимость обеспечения 1-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

– для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает либо специальные категории персональных данных, либо биометрические персональные данные, либо иные категории персональных данных;

– для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

Необходимость обеспечения 2-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

– для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает общедоступные персональные данные;

– для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

– для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает биометрические персональные данные;

– для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

– для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

– для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

Необходимость обеспечения 3-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при

наличии хотя бы одного из следующих условий:

– для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные сотрудников оператора или общедоступные персональные данные менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

– для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

– для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

– для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает биометрические персональные данные;

– для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

Необходимость обеспечения 4-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

– для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает общедоступные персональные данные;

– для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем

100000 субъектов персональных данных, не являющихся сотрудниками оператора.

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

– организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

– обеспечение сохранности носителей персональных данных;

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

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

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

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

Для обеспечения 1-го уровня защищенности персональных данных при их обработке в информационных системах помимо требований, предусмотренных правилами, необходимо выполнение следующих требований:

– автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе;

– создание структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности.

Контроль за выполнением настоящих требований организуется и проводится оператором (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанный контроль проводится не реже 1 раза в 3 года в сроки, определяемые оператором (уполномоченным лицом).

Таким образом, при создании системы защиты персональных данных в организациях, на современном этапе развития в РФ, можно выделить следующие последовательные этапы:

– выяснить и определить все случаи, когда необходимо проводить обработку персональных данных в организации;

– определить бизнес-процессы, в которых обрабатываются персональные данные;

– наметить обязательные (в том числе предварительные) этапы работ по защите персональных данных:

– выделить все возможные ситуации, когда необходимо проводить обработку персональных данных;

– отобрать определенное число бизнес-процессов для проведения анализа. (необходимо разработать перечень структурных подразделений и работников

организации, принимающих непосредственное участие в обработке персональных данных в рамках своих функциональных обязанностей);

– определить совокупность обрабатываемых персональных данных и круг информационных систем;

– провести ранжирование персональных данных по категориям и предварительную классификацию информационных систем.

– наметить меры по минимизации категорий обрабатываемых персональных данных;

– подготовить действующую модель угроз для информационной системы обработки персональных данных.

– разработать техническое задание по созданию необходимой системы защиты;

– провести уточнение соответствия классов информационных систем, с дальнейшей подготовкой предложений по использованию технических средств защиты персональных данных;

– подать уведомление о начале обработки персональных данных в уполномоченный орган по защите прав субъектов персональных данных (Роскомнадзор) для регистрации в качестве оператора персональных данных;

– подать заявку на получение экземпляров руководящих документов в Федеральную службу по техническому и экспортному контролю России по организации системы защиты персональных данных;

– разработать требования для конкретной системы обработки персональных данных, учитывая класс защиты информационной системы .

– для защиты информационной системы обработки персональных данных и помещений подготовить технический проект.

– для документов в информационной системе защиты персональных данных (регламенты, приказы, положения, инструкции) разработать пакет организационно-распорядительные документы;

– провести внедрение системы защиты персональных данных;

– с субъектов персональных данных взять согласие на обработку персональных данных;

– провести контрольные мероприятия по выявлению нарушений защиты персональных данных; физическому или юридическому лицу иностранного государства, при передаче оператором персональных данных через государственную границу Российской Федерации органу власти иностранного государства, проверить находится ли получатель персональных данных в стране, где осуществляется надлежащая защита персональных данных.

В случае необходимости, может привлекаться организация, для выбора и реализации методов и способов защиты информации в информационной системе обработки персональных данных, имеющая лицензию на осуществление деятельности по технической защите конфиденциальной информации оформленную в установленном законом порядке.

Применение системы защиты информации является не обязательным для всех типов информационных систем обработки персональных данных. Выбор системы защиты информации необходимо осуществлять учитывая, что конечный набор мер для защиты персональных данных должен отвечать требованиям, предъявляемым к информационной системе обработки персональных данных соответствующего класса, определение которых приведено в Приказе ФСТЭК России от 18.02.2013 N 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (Зарегистрировано в Минюсте России 14.05.2013 N 28375) (ред. от 23.03.2017).

В соответствии с Указом Президента РФ от 17.03.2008 N 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» осуществляется подключение информационных систем, обрабатывающих государственные информационные ресурсы, к информационно телекоммуникационным сетям международного информационного» (ред. от 22.05.2015).

Таким образом, для системы защиты персональных данных информационная система обработки персональных данных выбирается в зависимости от класса информационной системы с учетом: угроз безопасности персональным данным; структуры информационной системы; наличия межсетевого взаимодействия и режимов обработки персональных данных с использованием соответствующих методов и способов защиты информации от несанкционированного доступа (реализуются функции управления доступом, регистрации и учета); обеспечения целостности защиты персональных данных; анализа защищенности персональных данных; обеспечения безопасного межсетевого взаимодействия; обнаружения вторжений.

Система защиты персональных данных включает в себя меры организационного и технического характера, которые определяются с учетом актуальных угроз безопасности для персональных данных и информационных технологий, используемых в системе обработки информации организации.

Глава 2. Особенности организации защиты персональных данных ГБПОУ «Южноуральский энергетический техникум»

2.1. Общая характеристика ГБПОУ «Южноуральский энергетический техникум»

Южноуральский энергетический техникум создан в 1952 году Советом народного хозяйства Челябинского экономического административного района для подготовки специалистов для строящейся Южноуральской ГРЭС – одной из первых в Советском Союзе тепловых электростанций мощностью 1000 МВт. Техникум образовался как вечерний филиал Челябинского энергетического техникума и стал готовить специалистов двух направлений: теплотехников-котельников и электриков. В июне 1958 г. был преобразован в самостоятельный вечерний индустриальный техникум, который, кроме энергетиков, стал готовить техников-строителей и технологов по керамике – эти специалисты понадобились новостроящимся заводам молодого г. Южноуральска.

Место нахождения образовательной организации: 457040, Челябинская область, г.Южноуральск, ул.Строителей дом 3.

В приложении 1 представлена организационная структура ГБПОУ «Южноуральский энергетический техникум».

Непосредственное управление техникумом осуществляет директор. Представители педагогического коллектива и коллектива сотрудников, родительской общественности, работодателей вовлечены в процесс управления через систему административно-общественного управления.

Отдельными направлениями деятельности руководят заместители директора по:

- учебной работе (УР);
- методической работе (МР);
- воспитательной работе (ВР);
- учебно-производственной работе (УПР).

Руководство структурными подразделениями осуществляют:

- заведующие отделениями (очное и заочное обучение);
- заведующий библиотекой;
- начальник информационно-вычислительного центра;

В целях обеспечения эффективного решения вопросов, связанных с реализацией основных функций техникума, в соответствии с законодательством РФ и локальными нормативными актами в техникуме действуют экспертные комиссии (аттестационная комиссия по аттестации педагогических работников на соответствие занимаемой должности, комиссия по разрешению конфликтных ситуаций и др.)

Имеющаяся структура управления соответствует функциональным задачам и Уставу техникума.

В техникуме разрабатываются и внедряются элементы системы менеджмента качества (СМК) в соответствии с требованиями ГОСТ Р ИСО 9000-2001, которая ориентирована на выявление, сокращение, устранение и предупреждение предос-тавления образовательных услуг неудовлетворительного качества.

Политику в области качества формирует, утверждает и организует директор техникума.

При разработке политики в области качества учитываются:

- стратегические цели;
- характер улучшений в будущем;
- степень удовлетворённости потребителей;
- потребности и ожидания заинтересованных сторон.

На каждую должность штатного расписания разработаны и утверждены должностные инструкции.

Основным документом, определяющим направления развития и деятельности техникума, является Программа развития на 2014-2018гг. Основная цель Программы - обеспечение доступности и качества профессионального образования, отвечающего требованиям инновационного развития Челябинской

области, создание условий и реализация механизмов повышения эффективности профессионального образования в обеспечении социально-экономической сферы Челябинской области трудовыми ресурсами.

Программа содержит:

– анализ содержания проблемы и обоснование необходимости ее решения программными методами, включающий проблемно-ориентированный анализ состояния техникума по направлениям, определенными целевыми показателями;

– анализ факторов, оказывающих существенное влияние на деятельность техникума;

– оценку инновационного потенциала системы управления техникумом;

– основную цель и задачи программы;

– систему программных мероприятий,

– -ресурсное обеспечение программы;

– описание организации управления и механизма реализации программы;

– ожидаемые результаты реализации программы,

– целевые индикаторы и показатели эффективности реализации программы.

Программой определены объемы и источники финансирования, обеспечивающие ее реализацию.

Перспективный план работы на учебный год формируется по направлениям деятельности на основе планов работы структурных подразделений техникума. План работы обсуждается и принимается на заседании педагогического совета техникума в начале учебного года.

ГБПОУ «Южноуральский энергетический техникум» обладает автономией, под которой понимается самостоятельность в осуществлении образовательной, научной, административной, финансово-экономической деятельности, разработке и принятии локальных нормативных актов в соответствии с Федеральным законом «Об образовании в Российской Федерации», иными нормативными правовыми актами Российской Федерации и настоящим Уставом.

ГБПОУ «Южноуральский энергетический техникум» подотчетно и

подконтрольно в своей деятельности Учредителю.

В ГБПОУ «Южноуральский энергетический техникум» действуют следующие коллегиальные органы управления: Конференция работников Учреждения, Совет Учреждения, Педагогический совет, Совет обучающихся Учреждения, Попечительский совет, Совет родителей.

Конференция работников ГБПОУ «Южноуральский энергетический техникум» проводится не реже 1 раза в год. В состав конференции входят директор, представители всех категорий работников, представители родителей (законных представителей) несовершеннолетних обучающихся, представители обучающихся.

Председатель, секретарь Конференции Учреждения избираются Конференцией на срок 5 лет.

Конференция ГБПОУ «Южноуральский энергетический техникум»:

– решает вопросы о необходимости заключения с администрацией ГБПОУ «Южноуральский энергетический техникум» коллективного договора, внесения изменений и дополнении в него;

– избирает представителя для предоставления интересов всех работников в социальном партнерстве в порядке, установленном Трудовым кодексом Российской Федерации;

– избирает представителей работников в комиссию по трудовым спорам;

– избирает Совет ГБПОУ «Южноуральский энергетический техникум»;

– утверждает положение о Совете ГБПОУ «Южноуральский энергетический техникум»;

– заслушивает отчет Совета ГБПОУ «Южноуральский энергетический техникум» о выполненной работе;

– утверждает публичный отчет ГБПОУ «Южноуральский энергетический техникум»;

– рассматривает иные вопросы, отнесенные к его компетенции действующим законодательством, а также выносимые на обсуждение директором ГБПОУ «Южноуральский энергетический техникум», Советом ГБПОУ

«Южноуральский энергетический техникум».

Конференция работников ГБПОУ «Южноуральский энергетический техникум» считается правомочным, если на нем присутствует не менее половины от общего числа работников. Решение считается принятым, если за него проголосовало не менее половины работников, присутствующих на Конференции работников ГБПОУ «Южноуральский энергетический техникум».

Совет ГБПОУ «Южноуральский энергетический техникум» избирается на Конференции работников Учреждения в количестве 15 человек сроком на 3 года. В состав Совета ГБПОУ «Южноуральский энергетический техникум» входят директор, представители всех категорий работников, представители родителей (законных представителей) несовершеннолетних обучающихся, представители обучающихся, представители заинтересованных организаций в равных долях.

Совет ГБПОУ «Южноуральский энергетический техникум» собирается по мере необходимости, но не реже 4 раз в год. Решения Совета ГБПОУ «Южноуральский энергетический техникум» оформляются протоколами и вступают в силу с даты их подписания председателем Совета.

Члены Совета ГБПОУ «Южноуральский энергетический техникум» избираются Конференцией открытым голосованием. Председатель, секретарь Совета ГБПОУ «Южноуральский энергетический техникум»избираются членами Совета на первом заседании.

Решения Совета ГБПОУ «Южноуральский энергетический техникум» принимаются открытым голосованием и являются правомочными при участии на его заседаниях более половины членов Совета, и если за них проголосовало не менее двух третей присутствовавших.

Совет ГБПОУ «Южноуральский энергетический техникум»:

- принимает решение о созыве и проведении Конференции, определяет порядок его проведения;
- организует выполнение решений Конференции;
- разрабатывает изменения и дополнения в Устав;
- принимает локальные нормативные акты ГБПОУ «Южноуральский

энергетический техникум»;

– рассматривает сметы планирования и расходования денежных средств, получаемых от приносящей доход деятельности «Южноуральский энергетический техникум»;

– осуществляет контроль за расходованием привлеченных «Южноуральский энергетический техникум» дополнительных финансовых средств, в том числе от приносящей доход деятельности, в соответствии с утвержденными сметами;

– разрабатывает программы развития ГБПОУ «Южноуральский энергетический техникум»;

– участвует в работе ревизионной комиссии;

– решает вопросы, отнесенные к его компетенции коллективным договором;

– формирует предложения администрации (в лице директора, заместителей директора) ГБПОУ «Южноуральский энергетический техникум» о предоставлении материальной помощи работникам и обучающимся ГБПОУ «Южноуральский энергетический техникум»;

– выполняет иные функции в соответствии с положением о Совете ГБПОУ «Южноуральский энергетический техникум» и действующим законодательством.

В ГБПОУ «Южноуральский энергетический техникум» действует педагогический совет (Педсовет формируется директором ГБПОУ «Южноуральский энергетический техникум», в который входят все педагогические работники ГБПОУ «Южноуральский энергетический техникум», работающие по основному месту работы.

Решения педсовета принимаются открытым голосованием и являются правомочными при участии на его заседаниях более половины членов педсовета, и если за них проголосовало не менее двух третей присутствовавших. Решения педсовета оформляются протоколами. Решения педсовета являются рекомендательными для коллектива ГБПОУ «Южноуральский энергетический

техникум». Решения педсовета, утвержденные приказом ГБПОУ «Южноуральский энергетический техникум», являются обязательными для исполнения.

Педсовет собирается не реже одного раза в три месяца и решает все вопросы, относящиеся к образовательной деятельности ГБПОУ «Южноуральский энергетический техникум», в том числе:

– организации и совершенствования методического обеспечения образовательной деятельности;

– разработки и утверждения образовательных программ и учебных планов, годовых календарных учебных графиков;

– объема и качества знаний, умений, навыков обучающихся и компетенции, приобретения опыта деятельности, развития способностей, приобретения опыта применения знаний в повседневной жизни и формирования у обучающихся мотивации получения образования в течение всей жизни;

– учебной и производственной практики;

– инспектирования и контроля образовательной деятельности внутри В ГБПОУ «Южноуральский энергетический техникум»;

– содержания и качества дополнительных образовательных услуг, в том числе платных;

– разработки, апробации, экспертизы и применения педагогическими работниками новых педагогических и воспитательных технологий;

– разработки методик и средств профессионального отбора и ориентации;

– разработки новых форм и методических материалов, пособий, средств обучения; новых форм и методов теоретического и производственного обучения, производственной (профессиональной) практики обучающихся;

– осуществления текущего контроля успеваемости и промежуточной аттестации обучающихся в соответствии с Федеральным законом «Об образовании в Российской Федерации» и настоящим Уставом;

– принятия решения об исключении обучающихся из Учреждения других вопросов в соответствии с положением о Педагогическом совете.

Совет обучающихся формируется из представителей обучающихся — по одному представителю от группы сроком на 3 года.

Решения совета обучающихся принимаются открытым голосованием и являются правомочными при участии на его заседаниях более половины членов совета обучающихся, и если за них проголосовало не менее двух третей присутствовавших. Решения совета обучающихся оформляются протоколами.

Совет обучающихся:

– принимает участие в планировании и проведении учебно-воспитательной работы в ГБПОУ «Южноуральский энергетический техникум»;

– принимает участие в обсуждении программы развития ГБПОУ «Южноуральский энергетический техникум»;

– подводит итоги соревнования между группами по учебной, учебно-производственной и воспитательной работе;

– вносит предложения администрации ГБПОУ «Южноуральский энергетический техникум» о поощрении победителей;

– участвует по вопросам управления ГБПОУ «Южноуральский энергетический техникум» и при принятии локальных нормативных актов, затрагивающих права и законные интересы обучающихся;

– решает иные вопросы в соответствии с положением о совете обучающихся.

Попечительский совет ГБПОУ «Южноуральский энергетический техникум» действует в соответствии с законодательством Российской Федерации и Челябинской области, настоящим Уставом и Положением о Попечительском совете.

В попечительский совет могут входить физические и юридические лица, в том числе представители администрации и работники ГБПОУ «Южноуральский энергетический техникум», обучающиеся и их родители (законные представители), представители органов государственной власти и местного самоуправления, представители работодателей, социальных партнеров, в количестве 15 человек, сроком на 3 года. Попечительский совет избирает из

своего состава председателя и секретаря, определяет руководящие и контрольно-ревизионные органы совета. Права и обязанности участников Попечительского совета указываются в Положении о Попечительском совете. Решения попечительского совета принимаются открытым голосованием и являются правомочными при участии на его заседаниях более половины членов попечительского совета, и если за них проголосовало не менее двух третей присутствовавших. Решения попечительского совета оформляются протоколами.

Попечительский совет:

– участвует в совершенствовании образовательной деятельности в В ГБПОУ «Южноуральский энергетический техникум»;

– содействует привлечению дополнительных финансовых средств для обеспечения деятельности и развития ГБПОУ «Южноуральский энергетический техникум»;

– содействует социальной защите и поддержке обучающихся и сотрудников, улучшению условий труда работников ГБПОУ «Южноуральский энергетический техникум»;

– содействует совершенствованию материально -технической базы В ГБПОУ «Южноуральский энергетический техникум», благоустройству его помещений и территории;

– определяет порядок расходования денежных средств, полученных за счет добровольных пожертвований физических и (или) юридических лиц;

– осуществляет контроль за использованием указанных средств;

– поддерживает инновационную и научно-исследовательскую деятельность ГБПОУ «Южноуральский энергетический техникум»;

– содействует установлению связей с работодателями, службами занятости населения, органами государственной власти, органами местного самоуправления, средствами массовой информации, другими организациями, родителями (законными представителями) обучающихся, выпускниками ГБПОУ «Южноуральский энергетический техникум»;

– рассматривает другие вопросы, отнесенные к компетенции

попечительского совета в соответствии с положением о Попечительском совете.

Совет родителей является представительным органом родителей (законных представителей) несовершеннолетних обучающихся. В состав Совета родителей входят по одному представителю родителей от группы, которые избираются на родительских собраниях в группе на срок в соответствии с Положением о Совете родителей.

Совет родителей созывается по мере необходимости по решению председателя Совета родителей, по решению половины членов Совета родителей, по решению директора ГБПОУ «Южноуральский энергетический техникум». Решения Совета родителей принимаются открытым голосованием большинством голосов и являются правомочными, если за них проголосовало не менее двух третей присутствовавших.

Совет родителей:

– содействует объединению усилий родителей и администрации Учреждения в обучении и воспитании обучающихся;

– оказывает помощь ГБПОУ «Южноуральский энергетический техникум»в определении и защите социально не защищенных обучающихся, утверждает списки таких обучающихся;

– оказывает ГБПОУ «Южноуральский энергетический техникум» организационную и консультативную помощь;

– разрабатывает предложения по улучшению условий пребывания обучающихся в ГБПОУ «Южноуральский энергетический техникум» и другим вопросам деятельности ГБПОУ «Южноуральский энергетический техникум» и направляет предложения руководителю;

– содействует совершенствованию материально-технической базы в ГБПОУ «Южноуральский энергетический техникум», благоустройству его помещений и территории;

– контролирует расходование денежных средств, получаемых от добровольных пожертвований, целевых взносов физических и юридических лиц;

– участвует в управлении ГБПОУ «Южноуральский энергетический

техникум» и принятии локальных нормативных актов, по вопросам затрагивающим права и законные интересы обучающихся;

– рассматривает другие вопросы в соответствии с положением о Совете родителей.

Совет родителей действует на основании Положения о Совете родителей. В целях учета мнения обучающихся, родителей (законных представителей) несовершеннолетних обучающихся и педагогических работников по вопросам управления ГБПОУ «Южноуральский энергетический техникум» и при принятии локальных нормативных актов, затрагивающих их права и законные интересы, по инициативе обучающихся, родителей (законных представителей) несовершеннолетних обучающихся и педагогических работников в ГБПОУ «Южноуральский энергетический техникум» действуют профессиональные союзы обучающихся и (или) работников ГБПОУ «Южноуральский энергетический техникум», осуществляющие свою деятельность в соответствии с действующим законодательством.

Структуризация ГБПОУ «Южноуральский энергетический техникум» необходима для децентрализованного управления, к сожалению, в ГБПОУ «Южноуральский энергетический техникум» сложилась такая структура управления, которую можно назвать плоской, когда все субъекты управления, начиная с заместителей и заканчивая техперсоналом подчинены только одному человеку – директору. Традиционное учебное заведение является скорее централизованной организацией. Взаимосвязи осуществляются по принципу «команд и контроля». Управление в ГБПОУ «Южноуральский энергетический техникум» осуществляется в форме законной власти. Стиль управления скорее смешанный: демократичный, т.к. основывается на потребностях высокого уровня: творческая реализация, проявление интеллектуального потенциала, любовь к учащимся; автократичный, т.к. сама система образования предусматривает чёткие рамки программы и централизацию. Анализируя ГБПОУ «Южноуральский энергетический техникум», можно выявить, что децентрализация приведёт ко многим преимуществам. А именно, развитию навыков руководителей, полномочия и ответственность которых возрастёт; соревнование в организации

усилит стимул руководителей к созданию атмосферы конкуренции и большей самостоятельности; а это поможет раскрыть творческие способности руководителей, приведёт к росту и развитию ГБПОУ «Южноуральский энергетический техникум» в целом, коллектив станет командой единомышленников.

Профессиональная позиция педагогов не однозначная: с одной стороны они готовы обсуждать и решать проблемы с учащимися, с другой - эти проблемы ограничиваются рамками преподаваемого предмета. Для определённой части педагогов ГБПОУ «Южноуральский энергетический техникум» характерна повышенная конфликтность в общении с коллегами и учениками. По стилю педагогического общения коллектив неоднороден: демократизм и авторитарные тенденции представлены примерно с одинаковой степенью выраженности. Позиция студентов тоже двойственна: они признают, что могут участвовать в планировании и организации образовательного процесса, но чаще выражают готовность принимать уроки такими, какие они есть.

Таким образом, система управления, сложившаяся в техникуме, обеспечена необходимой нормативной и организационно-распорядительной документацией, соответствующей требованиям действующего законодательства и Устава техникума.

2.2. Анализ организации защиты персональных данных в ГБПОУ «Южноуральский энергетический техникум»

Исследование системы защиты персональных данных в ГБПОУ «Южноуральский энергетический техникум» требует предварительного проведения оргпроектных работ.

Организационное проектирование – это проектирование новых организаций, структурное преобразование или оптимизация деятельности уже существующих организаций, а также формирование их организационных структур. Организационное проектирование позволяет формировать системы с

заранее заданными характеристиками, содержащимися в проектной документации.

Целью организационного проектирования является формирование новых организационных структур или развитие уже существующих, а также придание процессу создания новых систем или развитию действующих целенаправленности, научной обоснованности.

Задачами организационного проектирования является:

– выявление условий, влияющих на деятельность организации и методов их изучения;

– определение качественного и количественного состава элементов структур управления, формирование их взаимосвязи;

– определение структуры управления организацией и определение условий, в которых каждая из них будет более эффективна;

– изучение принципов и методов проектирования структур управления и особенностей их применения;

– определение методики расчета необходимой численности персонала;

– разработка мероприятий по внедрения спроектированных мероприятий в организацию;

– разработка методов и форм контроля, а также специфики их использования.

Оргпроектирование включает несколько стадий.

Первая стадия называется предпроектным обследование. Предпроектное обследование организации – один из важнейших этапов успешного внедрения проекта. Этот этап служит фундаментом для всей последующей работы над проектом. Его цель – точное определение состава, объема, стоимости, сроков исполнения предстоящих проектно-исследовательских работ и соответствующее их документирование

Этот этап подразделяется, в свою очередь, на составные элементы:

– предпроектное ориентировочное исследование (экспресс-анализ) – диагностика;

– рабочее, детальное исследование;

– анализ, обобщение и выводы.

Следующий этап, проектирование – это наиболее творческая часть деятельности исследователей и проектантов. Она предполагает применение различных методических и организационно-технических приемов и средств, разработанных наукой и практикой на сегодняшний день в их сочетании.

Предметом организационного проектирования являются новые структуры, системы, управляемые процессы. Организационное проектирование настроено на создание новых объектов, модификацию существующих и коренную реконструкцию объектов и процессов.

План работ проведения оргпроектных работ в ГБПОУ «Южноуральский энергетический техникум» области представлен в таблице 1

Таблица 1 – План работ проведения оргпроектных работ в ГБПОУ «Южноуральский энергетический техникум»

№ п/п	Наименование этапа	Трудоемкость (дни)	Сроки проведения	Число исполнителей
1.	Обследование	30	01.04.2017г.-30.04.2017г.	1
2.	Проектирование	18	02.05.2017г-20.05.2017 г.	1

Организационная работа начинается с разработки программы исследования – это комплекс положений, определяющих цели и задачи исследования, предмет и условия его проведения, а также предполагаемы результат.

Рабочая программа является организационно-методическим документом, содержащим полный перечень вопросов, на которые требуется получить ответы в процессе исследования. Рабочая программа оформляется в виде таблицы 2.

В план работ рекомендуется вносить следующие показатели: номер этапа, наименование этапа, трудоемкость, сроки начала и окончания работ, число исполнителей.

Методы предпроектного исследования необходимы для получения и более полного представления о состоянии объекта исследования на сегодняшний день.

Изучение документов – это метод сбора первичных данных, при котором

документы используются в качестве главного источника информации; это также совокупность методических приёмов и процедур, применяемых для извлечения информации из документальных источников при изучении процессов и явлений в целях решения определённых задач[29, с. 139].

Таблица 2 – Рабочая программа исследования организации защиты персональных данных в ГБПОУ «Южноуральский энергетический техникум»

№ п/п	Наименование работ	Методы сбора данных	Источники информации	Форма сбора, обобщения, представления информации	Исполнители	Сроки
1	2	3	4	5	6	7
1	Изучение направлений деятельности, организационной структуры учреждения	изучение документов	локальные документы организации (историческая справка, приказ о создании, штатное расписание, регламент)	описание	Муратов Р.Р.	01.04.17-10.04.17
2	Изучение организационных документов, регламентирующих деятельность организации	изучение документов	организационно-правовые акты , приказы, положения	описание	Муратов Р.Р.	11.04.17-17.04.17
3	Изучение целей, задач, функций по защите персональных данных в организации	изучение документов, наблюдение	Положение, регламент, приказы, должностные инструкции	описание	Муратов Р.Р.	15.04.17-17.04.17
4	Изучение технологии защиты персональных данных в организации	изучение документов, обследование АРМ и подключение у Интернет	локальные документы организации (положения, штатное расписание, должностные инструкции,)	описание	Муратов Р.Р.	18.04.17-21.04.17
5	Изучение особенностей и выделение недостатков в функционировании системы защиты персональных данных в организации	изучение документов, обследование АРМ и подключение у Интернет	локальные документы организации (положения, штатное расписание, должностные инструкции,)	описание	Муратов Р.Р.	22.04.17-29.04.17

Непосредственное наблюдение – регистрация событий, явлений, фактов в соответствии с заранее установленными задачами и порядком их фиксации.

Статистический метод – методы анализа статистических данных, научные

методы описания и изучения массовых явлений, допускающих количественное (численное) выражение.

Графический метод – это метод условных изображений статистических данных при помощи геометрических фигур, линий, точек и разнообразных символических образов [34, с. 128].

Таким образом, в пред проектном обследовании используются следующие методы: изучение документов, непосредственное наблюдение, статистический, графический.

Основной целью создания защиты персональных данных в ГБПОУ «Южноуральский энергетический техникум» является минимизация ущерба от возможной реализации угроз безопасности персональных данных.

Для достижения основной цели система безопасности персональных данных информационная система персональных данных должна обеспечивать эффективное решение следующих задач:

1. защиту от вмешательства в процесс функционирования информационной системы персональных данных посторонних лиц (возможность использования информационной системой и доступ к ее ресурсам должны иметь только зарегистрированные установленным порядком пользователи);

2. разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам информационной системы персональных данных (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям информационной системы персональных данных для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа:

– к информации, циркулирующей в информационной системе персональных данных;

– средствам вычислительной техники информационной системы персональных данных;

– аппаратным, программным и криптографическим средствам защиты, используемым в информационной системе персональных данных;

3. регистрацию действий пользователей при использовании защищаемых ресурсов информационной системы персональных данных в системных журналах и периодический контроль корректности действий пользователей системы путем анализа содержимого этих журналов;

4. контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения;

5. защиту от несанкционированной модификации и контроль целостности используемых в информационной системе персональных данных программных средств, а также защиту системы от внедрения несанкционированных программ;

6. защиту персональных данных от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;

7. защиту персональных данных хранимой, обрабатываемой и передаваемой по каналам связи, от несанкционированного разглашения или искажения;

8. обеспечение живучести криптографических средств защиты информации при компрометации части ключевой системы;

9. своевременное выявление источников угроз безопасности персональных данных, причин и условий, способствующих нанесению ущерба субъектам персональных данных, создание механизма оперативного реагирования на угрозы безопасности персональных данных и негативные тенденции;

10. создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности персональных данных.

Защита персональных данных в ГБПОУ «Южноуральский энергетический техникум» не регламентирована, т.е. отсутствуют какие-либо документы регулирующие действия по защите персональных данных. В ходе исследования были исследованы все положения (62 положения) регулирующие деятельность техникума их перечень представлен в приложении 2.

Объектами защиты ГБПОУ «Южноуральский энергетический техникум»

являются – информация, обрабатываемая в информационной системе персональных данных, и технические средства ее обработки и защиты. Объекты защиты включают:

1. Обрабатываемая информация.

2. Технологическая информация.

3. Программно-технические средства обработки.

4. Средства защиты персональных данных.

5. Каналы информационного обмена и телекоммуникации.

6. Объекты и помещения, в которых размещены компоненты информационной системы персональных данных.

В таблице 3 приведен перечень должностей ГБПОУ «Южноуральский энергетический техникум», уполномоченных на обработку персональных данных и (или) имеющих доступ к персональным данным.

Таблица 3 – Перечень должностей сотрудников образовательного учреждения, уполномоченных на обработку персональных данных

№ п/п	Наименование должности	К каким персональным данным (сведениям, документам, носителям) допускаются
1.	Директор	в полном объеме
2.	Заместители директора	в объёме, необходимом для выполнения должностных обязанностей
3.	Специалист кадровой службы	к сведениям и документам, регулирующим взаимоотношения (трудовые, обучение) субъектов ПДн и образовательного учреждения (сторонних организаций)
4.	Специалисты бухгалтерии	к биографическим данным и данным, формируемым в процессе взаимоотношений (трудовые, обучение) с субъектами ПДн
5.	Специалисты ИТ (Администратор информационной системы обработки персональных данных, оператор информационной системы обработки персональных данных)	в объёме, необходимом для выполнения должностных обязанностей
6.	Преподаватели	в объёме, необходимом для выполнения должностных обязанностей

Пользователи информационной системы персональных данных ГБПОУ «Южноуральский энергетический техникум» делятся на три основные категории:

Администратор информационной системы обработки персональных данных. Сотрудники ГБПОУ «Южноуральский энергетический техникум», которые занимаются настройкой, внедрением и сопровождением системы. Администратор информационной системы персональных данных обладает следующим уровнем доступа:

– обладает полной информацией о системном и прикладном программном обеспечении информационной системы обработки персональных данных;

– обладает полной информацией о технических средствах и конфигурации информационной системы обработки персональных данных;

– имеет доступ ко всем техническим средствам обработки информации и данным информационной системы обработки персональных данных;

– обладает правами конфигурирования и административной настройки технических средств информационной системы обработки персональных данных.

Программист-разработчик информационной системы обработки персональных данных. Сотрудники ГБПОУ «Южноуральский энергетический техникум» или сторонних организаций, которые занимаются разработкой программного обеспечения. Разработчик информационной системы обработки персональных данных обладает следующим уровнем доступа:

– обладает информацией об алгоритмах и программах обработки информации на информационной системе обработки персональных данных;

– обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение информационной системы обработки персональных данных на стадии ее разработки, внедрения и сопровождения;

– может располагать любыми фрагментами информации о топологии информационной системы обработки персональных данных и технических

средствах обработки и защиты персональных данных, обрабатываемых в информационной системе обработки персональных данных.

Оператор информационной системы обработки персональных данных – сотрудники подразделений ГБПОУ «Южноуральский энергетический техникум», участвующие в процессе эксплуатации информационной системы обработки персональных данных. Оператор информационной системы обработки персональных данных – сотрудник обладает следующим уровнем доступа:

– обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству персональных данных;

– располагает конфиденциальными данными, к которым имеет доступ.

Подсистемы – носители персональных данных в информационной системе ГБПОУ «Южноуральский энергетический техникум» взаимодействующие так кадровый и бухгалтерский учет персонала. Подсистема обеспечения учебного процесса функционирует отдельно.

В ходе исследования было выявлено, что в информационной и системе автоматизированные рабочие места имеющие доступ и обрабатывающие персональные данные не подключены к сети интернет.

При обработке персональных данных в пределах ГБПОУ «Южноуральский энергетический техникум» система соответствует нераспределенным информационным системам персональных данных класса К3. При этом лицензий ФСТЭК России от оператора персональных данных не требуется, а защита данных осуществляется типовыми широко распространенными средствами.

Загрузку обновленных антивирусных баз данных, а также программ и форм персонифицированного учета и отчетности осуществляют на других компьютерах, подключенных к сети Интернет. Осуществляется безопасный перенос загруженных файлов в изолированные от Интернета локальные информационные системы персональных данных с использованием маркированных съемных носителей, в обязательном порядке проверяемых антивирусными средствами перед загрузкой в информационную систему

персональных данных.

Официально распространяемые территориальными органами ФНС России и Пенсионного фонда России программы используются при подготовке данных персонифицированного учета. При этом сформированные данные персонализированного учета выгружаются из информационной системы персональных данных на съемные маркированные носители.

Информационная система в ГБПОУ «Южноуральский энергетический техникум» защищена антивирусной лицензионной программой «Kaspersky».

В ней реализованы следующие функции безопасности:

- разграничение доступа к управлению антивирусной защитой;
- управление работой антивирусной защитой;
- управление параметрами антивирусной защитой;
- управление установкой обновлений (актуализации) базы данных
- признаков вредоносных компьютерных программ (вирусов) антивирусной защиты;
- аудит безопасности антивирусной защиты;
- сигнализация антивирусной защиты.

В среде, в которой антивирусной защита функционирует, реализованы

- следующие функции безопасности среды:
- обеспечение доверенной связи (маршрута) между антивирусной защиты и
- пользователями;
- обеспечение доверенного канала получения обновлений антивирусной защиты;
- обеспечение условий безопасного функционирования;
- управление атрибутами безопасности.

Перечень персональных данных обрабатываемых в ГБПОУ «Южноуральский энергетический техникум» в приложении 3.

Категории субъектов персональных данных в ГБПОУ «Южноуральский энергетический техникум»:

а) Субъекты, учащиеся в ГБПОУ «Южноуральский энергетический техникум».

б) Другие категории:

– сотрудники ГБПОУ «Южноуральский энергетический техникум»;

– лица, обратившиеся в ГБПОУ «Южноуральский энергетический техникум» с целью трудоустройства;

– лица, уволенные из ГБПОУ «Южноуральский энергетический техникум».

В таблице 4 приведены статистические данные по учащимся в ГБПОУ «Южноуральский энергетический техникум».

Таблица 4 – Статистические данные по субъектам, учащихся в ГБПОУ «Южноуральский энергетический техникум»

Субъекты	2017	2015	Изменение 2015- 2014	2016	Изменение 2016-2015
Обучающиеся	994	987	-7	1003	16
Отчисленные	17	11	-3	15	4

Структура категорий субъектов персональных данных учащихся в ГБПОУ «Южноуральский энергетический техникум» в 2016 году представлена на рисунке 1.

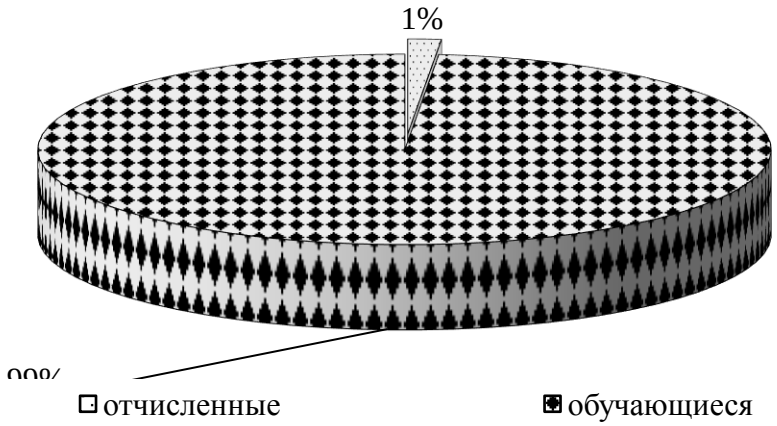

Рисунок 1 – Структура категорий субъектов персональных данных учащихся в ГБПОУ «Южноуральский энергетический техникум»

Таким образом, основным источником носителей персональных данных

являются студенты проходящие обучение в образовательном учреждении. Наблюдается тенденция роста объема персональных данных в ГБПОУ «Южноуральский энергетический техникум», что обуславливает актуальность защиты персональных данных в организации.

Так же, в архивах и в кадровой службе организации находиться более двухсот дел сотрудников уволенных и работающих на данный момент. В таблице 5 приведены статистические данные движение кадров в ГБПОУ «Южноуральский энергетический техникум».

Таблица 5 – Персональные данные сотрудников ГБПОУ «Южноуральский энергетический техникум»

Субъекты	2017	2015	Изменение 2015- 2014	2016	Изменение 2016-2015
сотрудники	184	188	-1	187	-3
лица, обратившиеся с целью трудоустройства	13	11	-2	18	+7
лица, уволенные	2	1	-1	2	+1

ГБПОУ «Южноуральский энергетический техникум» в целях реализации обучения и других возложенных функций использует следующие виды информационных ресурсов персональных данных:

– автоматизированные информационные ресурсы персональных данных, а именно информационные ресурсы, объединенные системами управления (обновляемые, справочные);

– автоматизированные информационные ресурсы, координатором которых является ГБПОУ «Южноуральский энергетический техникум», используемые совместно с иными органами государственной власти (Министерство образования и пр);

– автоматизированные информационные ресурсы персональных данных, оператором которых ГБПОУ «Южноуральский энергетический техникум» не является, но в соответствии с законодательством РФ имеет доступ к хранящимся в них данным;

– локальные информационные ресурсы, используемые для обработки персональных данных сотрудников ГБПОУ «Южноуральский энергетический техникум».

ГБПОУ «Южноуральский энергетический техникум» осуществляет обработку персональных данных с использованием средств автоматизации, используя следующие информационные системы:

- «1С-Бюджет»;
- «1С-Зарплата-Кадры»;
- Автоматизированная информационная библиотечная система;
- информационная система «Налогоплательщик»

Места обработки персональных данных:

- бухгалтерия;
- библиотека;
- учительская;
- отдел кадров;
- медпункт.

Исследование организации защиты персональных данных в ГБПОУ «Южноуральский энергетический техникум» выявило рад недостатков в функционировании системы защиты персональных данных: нет документов регламентирующих функционирование системы защиты персональных данных, так же, обращает на себя внимание отсутствие мероприятий обеспечивающих создание единой, целостной и скоординированной информационной системы безопасности персональных данных и создание условий для ее дальнейшего совершенствования.

Глава 3. Разработка мероприятий по повышению эффективности защиты персональных данных

3.1. Пути повышения эффективности системы защиты персональных данных

Ситуация с выполнением в ГБПОУ «Южноуральский энергетический техникум» требований ФЗ-152 существенно усложняется особенностями его функционирования. К таковым можно отнести следующие:

- отсутствие финансовых средств на реализацию мер по организационной и технической защите персональных данных;
- отсутствие штатных квалифицированных специалистов по информационной безопасности;
- сложность детерминации отношений между образовательным учреждением, обучаемыми, их представителями и иными лицами (родителями, опекунами, работодателями, организациями, выделяющими гранты, и т. п.).

В ГБПОУ «Южноуральский энергетический техникум» необходимо осуществить планирование организации защиты персональных данных, а так же разработать документы. регламентирующие ее функционирование.

Отсутствие элементарного положения о защите персональных данных является нарушением закона № 152-ФЗ «О персональных данных». На первый взгляд, штрафы за нарушение правил работы с персональными данными не так уж и высоки. Согласно статье 13.11 КоАП РФ штрафы составляют 5-10 тысяч рублей для организации и 500-1000 рублей для ее должностного лица.

Однако надо учитывать, что этот штраф может налагаться за каждое допущенное нарушение. А правил для тех, кто работает с персональными данными, законодатели установили очень много. Так что 10 тысяч рублей штрафа легко могут превратиться в 50 или 100 тысяч рублей даже в рамках одной проверки. А за год эти суммы могут оказаться еще внушительнее.

Главным документом, который должен иметь любой работодатель, является положение о персональных данных. Принять этот локальный акт, регулирующий

порядок хранения и использования персональных данных работодателя обязывает статья 87 Трудового кодекса. В положении обычно прописывают все требования к получению, хранению, комбинированию, передаче и любому другому использованию персональных данных, а также гарантии по их защите.

Предлагается разработать основной документ регламентирующий безопасность персональных данных. – это положение о защите персональных данных.

Необходимость разработки положения обусловлена стремительным расширением сферы применения новейших информационных технологий и процессов в ГБПОУ «Южноуральский энергетический техникум», при обработке информации вообще, и персональных данных в частности.

Положение будет определять основные цели и задачи, а также общую стратегию построения системы защиты персональных данных. Политика определяет основные требования и базовые подходы к их реализации, для достижения требуемого уровня безопасности информации.

Положение должно быть разработано в соответствии с системным подходом к обеспечению информационной безопасности. Системный подход предполагает проведение комплекса мероприятий, включающих исследование угроз информационной безопасности и разработку системы защиты персональных данных, с позиции комплексного применения технических и организационных мер и средств защиты.

Задачи информационной безопасности сводятся к минимизации ущерба от возможной реализации угроз безопасности персональных данных, а также к прогнозированию и предотвращению таких воздействий.

Положение будет служить основой для разработки комплекса организационных и технических мер по обеспечению информационной безопасности ГБПОУ «Южноуральский энергетический техникум», а также нормативных и методических документов, обеспечивающих ее реализацию, положение не предполагает подмены функций государственных органов власти Российской Федерации, отвечающих за обеспечение безопасности информационных технологий и защиту информации.

При планировании в ГБПОУ «Южноуральский энергетический техникум» мероприятий, связанных с защитой персональных данных, рекомендуется привлекать юристов, специалистов отдела кадров и по информационной работе (компьютерным технологиям).

Правовая составляющая должна стать обязательным элементом всей деятельности учреждения в этом направлении, поскольку необходимо: разработать локальные акты (нормативные и правовые), связанные не только с организационной и правовой, но и с технической защитой персональных данных; сформировать механизмы взаимоотношений с органами, осуществляющими управление в сфере образования, профсоюзными организациями, органами контроля и надзора и т. д.

Главным условием защиты персональных данных является четкая регламентация функций работников, а также принадлежности работникам документов, дел, картотек, журналов персонального учета и баз данных. Далее ключевым вопросом становится оценка наличия предусмотренных законодательством оснований для обработки персональных данных, а в случаях, когда они отсутствуют, получение согласия субъекта персональных данных на их обработку.

При этом согласно Закону № 152-ФЗ «О персональных данных» обязанность доказательства согласия субъекта персональных данных на их обработку возлагается на оператора, т. е. на работодателя. Несмотря на то, что в данном комментарии речь идет исключительно о защите персональных данных работников, хотелось бы в контексте обратить внимание на то, что обрабатываются персональные данные в образовательном учреждении обучающихся и их родителей, поэтому ГБПОУ «Южноуральский энергетический техникум» предварительно должно получить согласие родителей на обработку персональных данных их самих и их детей. Следует уделить особое внимание процедуре передачи персональных данных третьим лицам. Для этого необходимо наличие: основания для такой передачи, предусмотренного федеральными законами, или согласия на обработку персональных данных в школе субъекта персональных данных, закрепленного, например, в договоре на оказание услуг;

договора с этим третьим лицом, существенным условием которого должна быть обязанность обеспечения указанным лицом конфиденциальности и безопасности при обработке персональных данных в образовательном учреждении. Необходимо очень внимательно подойти к вопросу размещения информации, содержащей персональные данные, на интернет-сайте ГБПОУ «Южноуральский энергетический техникум».

С учетом выше изложенного можно выделить следующие обязательные этапы работы по защите персональных данных работников:

– определение всех ситуаций, когда требуется проводить обработку персональных данных;

– выделение процессов, в которых обрабатываются персональные данные;

– выбор ограниченного числа процессов для проведения аналитики (на этом этапе формируется перечень подразделений и работников, участвующих в обработке персональных данных в рамках своей служебной деятельности);

– определение круга информационных систем и совокупности обрабатываемых персональных данных;

– проведение категорирования персональных данных и предварительной классификации информационных систем;

– разработка пакета организационно-распорядительных документов для обеспечения защиты персональных данных (положения, приказы, акты, инструкции и т. п.);

– внедрение системы обеспечения безопасности информации.

Следовательно, защита персональных данных в образовательных учреждениях, по сути, сводится к созданию режима обработки персональных данных, включающего:

– создание внутренней документации по работе с персональными данными;

– организацию системы защиты персональных данных;

– внедрение технических мер защиты персональных данных.

Предлагается следующий пакет документов для ГБПОУ «Южноуральский энергетический техникум»:

– Положение о защите персональных данных.

– Согласие работника образовательного учреждения на обработку своих персональных данных.

– Согласие обучающегося (18 лет и старше) в образовательном учреждении на обработку своих персональных данных.

– Согласие законного представителя обучающегося (до 18 лет) в образовательном учреждении на обработку персональных данных обучающегося.

– Положение об ответственном лице информационной безопасности образовательного учреждения.

– Инструкция по проведению мониторинга информационной безопасности и антивирусного контроля при обработке персональных данных.

– Журнал учета персональных данных.

– Обязательство работника о неразглашении персональных данных.

– Приказ «О ведении Электронного журнала обращений пользователей персональных данных в ГБПОУ «Южноуральский энергетический техникум».

Так же более эффективно осуществлять сегментирование до отдельных рабочих мест в сочетании с обезличиванием действующей информационной системы персональных данных. При этом затраты на эксплуатацию единой обезличенной действующей информационной системы персональных данных не увеличиваются, а хранить кодификаторы ФИО (или их части) можно непосредственно на тех рабочих станциях, на которых персональные данные визуализируются. Если действующей информационная система персональных данных не является распределенной и не подключена к Интернету, то мероприятия по защите отдельных рабочих мест не потребуют больших затрат.

3.2. Разработка рекомендаций по повышению эффективности защиты персональных данных в ГБПОУ «Южноуральский энергетический техникум»

Представим проект организации системы защиты персональных данных в ГБПОУ «Южноуральский энергетический техникум» в виде таблицы 6.

Таблица 6 – Проект организации системы защиты персональных данных в ГБПОУ «Южноуральский энергетический техникум»

Мероприятия	Ответственное	Сроки
Издание приказа о назначении ответственных лиц за обработку персональных данных и приказа о создание положения о персональных данных	Директор	24.12. 2017
определение всех ситуаций, когда требуется проводить обработку персональных данных	Ответственное лицо, администратор автоматизированных информационных систем, специалист отдела кадров, секретариат	24.12. 2017-11.01 2018г.
выделение процессов, в которых обрабатываются персональные данные	администратор автоматизированных информационных систем, администратор автоматизированных информационных систем,	12.01.2018-17.01.2018
формирование перечня подразделений и работников, участвующих в обработке персональных данных в рамках своей служебной деятельности	Ответственное лицо, специалист отдела кадров, администратор автоматизированных информационных систем	12.01.2018-17.01.2018
определение круга информационных систем и совокупности обрабатываемых персональных данных	Ответственное лицо за обработку персональных данных, администратор автоматизированных информационных систем	17.01.2018-18.01.2018
проведение категорирования персональных данных и предварительной классификации информационных систем	Ответственное лицо за обработку персональных данных, администратор автоматизированных информационных систем	19.01.2018-22.01.2018
разработка пакета организационно-распорядительных документов для обеспечения защиты персональных данных (положение, согласия, журнал и пр.)	Ответственное лицо за обработку персональных данных, секретариат, специалист отдела кадров.	24.12. 2017-19.01 2018г.
Ознакомление под роспись всех лиц, имеющих доступ к персональным данным с положением о защите персональных данных	Специалист отдела кадров, ответственное лицо	19.01 – 20.01 2018
разработку технических решений по построению системы защиты персональных данных информационных систем персональных данных, осуществить выбор средств защиты информации для использования в составе системе защиты персональных данных.	администратор автоматизированных информационных систем	24.12. 2017-22.01 2018г.

На первом этапе издается приказ о назначении ответственного лица за безопасность персональных данных, проект приказа представлен в приложении 4.

Основные задачи ответственного лица за безопасность персональных данных заключаются в следующем.

– Разработка и реализация комплекса организационных и технических мер, направленных на выполнение установленных требований к обеспечению безопасности и защите информации, в том числе персональных данных.

– Обеспечение постоянного контроля в подразделениях за выполнением установленных требований к обеспечению безопасности и защите информации, в том числе персональных данных.

– Разработка и внесение предложений по совершенствованию и развитию корпоративной системы обеспечения безопасности и защиты информации, в том числе персональных данных.

Проект положения об ответственном лице за информационную безопасность ГБПОУ «Южноуральский энергетический техникум» представлен в приложении 5.

Рекомендуемая структура положения:

– Общие положения.

– Задачи.

– Функции.

– Взаимодействие.

– Ответственность.

Предлагается к работе проект положения о персональных данных обучающихся в ГБПОУ «Южноуральский энергетический техникум», который представлен в приложении 6.

Начать положение рекомендуется с раздела с основных понятия и обозначений. Далее выделить понятия и состав персональных данных . Третьим пунктом рекомендуется включить «Создание и обработка персональных данных». В нем обязательно нужно зафиксировать, что персональные данные в организации можно получить и обрабатывать исключительно на основании письменного согласия работника. А значит, сразу разрабатывается и утверждается

форма такого заявления (приложение 7). На подпись такое заявление работнику надо давать сразу при приеме на работу. А по действующим сотрудникам такую работу придется провести сразу же после утверждения Положения.

В обязательном порядке необходимо взять письменное заявление на обработку персональных данных у обучающихся и родителей, проект заявления представлен в приложении 8.

Далее может следовать раздел «Доступ к персональным данным». В нем последовательно описывается порядок доступа к таким данным работников организации и третьих лиц (отдельно родственников, государственных органов, представителей других организаций). При необходимости тут можно ввести уровни доступа в зависимости от должности сотрудника. Например, директор и аппарат дирекции имеют доступ ко всем персональным данным; сотрудники бухгалтерии - только к тем сведениям, которые необходимым для расчета заработной платы и налогов; представители кадровой службы – к сведениям, необходимым для оформления кадровой документации и т.п.

Продолжит Положение раздел «Порядок обработки и передачи данных». Здесь надо зафиксировать правила для передачи данных о сотрудниках определенным органам или лицам. В случаях, когда передача данных регулируется законодательно (налоговые органы, органы статистики, Пенсионный фонд и т.п.) достаточно сделать ссылки на порядок передачи сведений, установленный законодательством. Но, при этом следует обязательно зафиксировать, кто и в каком порядке вправе готовить данные сведения для передачи в госорганы. В положение обязательно включить раздел ответственность.

Предлагается следующая структура положения о персональных данных работников и обучающихся в ГБПОУ «Южноуральский энергетический техникум»:

– Общие положения.

– Основные понятия, обозначения.

– Цели и задачи .

– Понятие и состав персональных данных.

– Создание и обработка персональных данных.

– Доступ к персональным данным.

– Порядок хранения, использования и передачи персональных данных.

– Обязанности работодателя по хранению и защите персональных данных работника.

– Обязанности работника администрации, имеющих доступ к персональным данным обучающегося.

– Ответственность работодателя и лиц, осуществляющих работу с персональными данными

Ограничение доступа работников организации к персональным данным – неотъемлемая часть мероприятий по обеспечению безопасности персональных данных при их обработке в информационных системах. Допуск к обработке персональных данных должен быть только у тех сотрудников, которым это необходимо для выполнения служебных (трудовых) обязанностей.

Со всех лиц, имеющих доступ к персональным данным рекомендуется под роспись взять обязательство о конфиденциальности и неразглашении персональных данных, проект обязательства представлен в приложении 9.

В ГБПОУ «Южноуральский энергетический техникум» рекомендуется разработать инструкцию по проведению мониторинга информационной безопасности и антивирусного контроля при обработке персональных данных, проект которой представлен в приложении 10.

В Инструкции рекомендуется отразить следующее:

– Общие положения.

– Виды мониторинга информационной безопасности.

– Порядок проведения системного аудита.

– Порядок антивирусного контроля.

– Порядок анализа инцидентов.

Проект журнала обращений по ознакомлению с персональными данными представлен в приложении 11.

Журнал рекомендуется вести в каждом структурном подразделении в произвольной форме. В журнале необходимо фиксировать все обращения субъектов персональных данных (дата, ФИО, адрес) по ознакомлению с их персональными данными, дату направления запрашиваемых данных почтовой связью или предоставления лично заявителю. В случае отзыва данных субъектом персональных данных или выявления их несоответствия, в журнале должны быть сделаны соответствующие записи. По каждому обращению необходимо указывать, когда и каким образом на него было отреагировало.

Хранение журналов должно исключать несанкционированный доступ к ним.

Так же необходимо вести электронный журнал обращений пользователей к персональным данным. Для этого необходимо издать приказ проект, которого представлен в приложении 12.

Ограничение доступа работников организации к персональным данным – неотъемлемая часть мероприятий по обеспечению безопасности персональных данных при их обработке в информационных системах. Допуск к обработке персональных данных должен быть только у тех сотрудников, которым это необходимо для выполнения служебных (трудовых) обязанностей.

Так же, в нашем случае целесообразно сегментировать слабо взаимодействующие подсистемы информационной системы персональных данных, так необходимо разделить кадровый и бухгалтерский учета персонала и организовать обмен данными между ними с помощью съемных носителей.

Учитывая, что с июля 2017 года ужесточилось законодательство по работе с персональными данными ГБПОУ «Южноуральский энергетический техникум» необходимо ввести в практику разработанные нами рекомендации. В таблице 7 приведена эффективность разработанных мероприятий.

Таблица 7 – Эффективность мероприятий для ГБПОУ «Южноуральский энергетический техникум» в целях организации защиты персональных данных

Затраты	Эффективность
На расходные материалы: бумага (А4) 4000 листов - 1600руб картридж в принтер (1) – 2100руб. Затраты на персонал равны 0, так как работа по совершенствованию деятельности образовательной организации входит в функциональные обязанности управленческого персонала	Избежание штрафов: – за обработку данных без согласия – штраф до 75 тыс. руб.; – оператор персональных данных (например, работодатель или интернет-сайт) обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных – штраф до 30 тыс. руб.

Предложенные нами мероприятия помогут существенно снизить угрозу разглашением персональных данных и избежать неблагоприятных последствий. Организовать систему защиты персональных данных техникума, соответствующую современным требованиям и законодательству РФ.

Заключение

Проведенное исследование в рамках поставленной цели и выдвинутых задач позволило делать следующие выводы.

Защита персональных данных представляет собой регламентированный технологический процесс, предупреждающий нарушение установленного порядка доступности, целостности, достоверности и конфиденциальности персональных данных и обеспечивающий безопасность информации в процессе управленческой и производственной деятельности компании.

Нормативной основой защиты персональных данных являются нормы Конституции РФ, Федерального закона «О персональных данных», Указ Президента РФ «О перечне сведений конфиденциального характера» и другие акты.

Образовательные организации являются операторами персональных данных, поскольку занимаются обработкой персональных данных учащихся и педагогов. Следовательно, ответственными сотрудниками этих организаций должно обеспечиваться соблюдение законодательства.

В Российской Федерации защита персональных данных сводится к созданию режима обработки персональных данных, которые включают ряд последовательных этапов.

В системе защиты персональных данных информационная система обработки персональных данных выбирается в зависимости от класса информационной системы и исходя из угроз безопасности персональным данным, структуры информационной системы, наличия межсетевого взаимодействия и режимов обработки персональных данных с использованием соответствующих методов и способов защиты информации от несанкционированного доступа реализуются функции управления доступом, регистрации и учета, обеспечения целостности, анализа защищенности, обеспечения безопасного межсетевого взаимодействия и обнаружения вторжений.

Исследование проводилось на базе ГБПОУ «Южноуральский

энергетический техникум». Деятельность ГБПОУ «Южноуральский энергетический техникум» целиком направлена на четкое исполнение образовательных функций.

Для исследования организации защиты персональных данных в ГБПОУ «Южноуральский энергетический техникум» были проведены оргпроектные работы. План работы включал этап обследования и этап проектирования.

Организационно-методический документ – рабочая программа предпроектного обследования предполагала применения методов исследования: изучение документов, непосредственное наблюдение, статистический, графический.

Основной целью создания защиты персональных данных в ГБПОУ «Южноуральский энергетический техникум» области является минимизация ущерба от возможной реализации угроз безопасности персональных данных.

В ГБПОУ «Южноуральский энергетический техникум» в целях реализации государственных услуг и других возложенных функций использует следующие виды информационных ресурсов персональных данных:

- «1С-Бюджет»;
- «1С-Зарплата-Кадры»;
- Автоматизированная информационная библиотечная система;
- информационная система «Налогоплательщик»

При обработке персональных данных в пределах ГБПОУ «Южноуральский энергетический техникум» система соответствует нераспределенным информационным системам персональных данных класса К3. При этом лицензий ФСТЭК России от оператора персональных данных не требуется, а защита данных осуществляется типовыми широко распространенными средствами.

Исследование организации защиты персональных данных в ГБПОУ «Южноуральский энергетический техникум» выявило рад недостатков в функционировании системы защиты персональных данных: нет документов регламентирующих функционирование системы защиты персональных данных, так же, обращает на себя внимание отсутствие мероприятий обеспечивающих создание единой, целостной и скоординированной информационной системы

безопасности персональных данных и создание условий для ее дальнейшего совершенствования.

В целях создания единой, целостной и скоординированной системы информационной безопасности персональных данных и создание условий для ее дальнейшего совершенствования, предлагается комплексный подход для которго необходимо разработать следующий пакет документов для ГБПОУ «Южноуральский энергетический техникум»:

– Положение о защите персональных данных.

– Согласие работника образовательного учреждения на обработку своих персональных данных.

– Согласие обучающегося (18 лет и старше) в образовательном учреждении на обработку своих персональных данных.

– Согласие законного представителя обучающегося (до 18 лет) в образовательном учреждении на обработку персональных данных обучающегося.

– Положение об ответственном лице информационной безопасности образовательного учреждения.

– Инструкция по проведению мониторинга информационной безопасности и антивирусного контроля при обработке персональных данных.

– Журнал учета персональных данных.

– Обязательство работника о неразглашении персональных данных.

– Приказ «О ведении Электронного журнала обращений пользователей персональных данных в ГБПОУ «Южноуральский энергетический техникум».

Целесообразно сегментировать слабо взаимодействующие подсистемы информационной системы персональных данных, так необходимо разделить кадровый и бухгалтерский учета персонала и организовать обмен данными между ними с помощью съемных носителей.

Необходимость разработки предложенных выше положений и документов обусловлена стремительным расширением сферы применения информационных технологий и процессов на ГБПОУ «Южноуральский энергетический техникум», при обработке информации вообще, и персональных данных в частности.

Реализация предложенных мероприятий регламентированных разработанными документами в информационных системах персональных данных позволит:

– оценить состояние безопасности информации в информационных системах персональных данных, выявить источники внутренних и внешних угроз информационной безопасности, определить приоритетные направления предотвращения, отражения и нейтрализации этих угроз;

– разработать распорядительные и нормативно-методические документы применительно к информационным системам персональных данных;

– провести классификацию, аттестацию информационных систем персональных данных;

– провести организационно-режимные и технические мероприятия по обеспечению безопасности персональных данных в информационных системах персональных данных;

– обеспечить необходимый уровень безопасности объектов защиты.

Осуществление этих мероприятий обеспечит создание единой, целостной и скоординированной системы информационной безопасности информационных систем персональных данных и создаст условия для ее дальнейшего совершенствования.

Кроме того, подложенные нами мероприятия помогут существенно снизить угрозу разглашением персональных данных и избежать неблагоприятных последствий. Организовать систему защиты персональных данных техникума, соответствующую современным требованиям и законодательству РФ.

Список использованных источников

1. «Конституция Российской Федерации» (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ, от 21.07.2014 N 11-ФКЗ) [Электронный ресурс]// Консультант Плюс : справ. правовая система. Режим доступа – http://www.consultant.ru/document/cons_doc_LAW_28399/

2. «Трудовой кодекс Российской Федерации» от 30.12.2001 N 197-ФЗ (ред. от 29.07.2017) (с изм. и доп., вступ. в силу с 01.10.2017)// Консультант Плюс : справ. правовая система. Режим доступа – http://www.consultant.ru/document/cons_doc_LAW_34683/

3. Федеральный закон от 29.12.2012 N 273-ФЗ (ред. от 29.07.2017) «Об образовании в Российской Федерации» [Электронный ресурс]// Консультант Плюс : справ. правовая система. Режим доступа - ttp://www.consultant.ru/document/cons_doc_LAW_140174/27f9ddea0cccf9a6b90bb2cb8b545d436f18157b/

4. Федеральный закон от 27.07.2010 N 210-ФЗ (ред. от 28.12.2016) «Об организации предоставления государственных и муниципальных услуг» [Электронный ресурс]// Консультант Плюс : справ. правовая система. Режим доступа - http://www.consultant.ru/document/cons_doc_LAW_103023/

5. Федеральный закон от 27.07.2006 N 179-ФЗ (ред. от 29.07.2017) "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 01.10.2017) [Электронный ресурс]// Консультант Плюс : справ. правовая система. Режим доступа – http://www.consultant.ru/document/cons_doc_LAW_61798/

6. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 29.07.2017) «О персональных данных» [Электронный ресурс]// Консультант Плюс : справ.

правовая система. Режим доступа – http://www.consultant.ru/document/cons_doc_LAW _ 61801/

7. Приказ ФСБ России от 10.07.2017 N 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» (Зарегистрировано в Минюсте России 18.08.2017 N 33620) [Электронный ресурс]// Консультант Плюс : справ. правовая система. Режим доступа - http://www.consultant.ru/document/cons_doc_LAW_146520/

8. Аверченков, В.И. Защита персональных данных в организации : монография / В.И. Аверченков, М.Ю. Рытов, Т.Р. Гайнулин. - 3-е изд., стер. - М. : Флинта, 2016. - 124 с.

9. Амелин, Р.В. Информационное право в схемах : учебное пособие / Р.В. Амелин, С.А. Куликова, С.Е. Чаннов ; отв. ред. С.Е. Чаннов. - М. : Проспект, 2016. - 125 с

10. Алавердов, А. Р. Организация и управление безопасностью в организациях [Текст]: Учебное пособие/ А. Р. Аведов. – М.: Московский государственный университет статистики и информатики, 2014. – 411с.

11. Абаев, Ф.А. Историко-правовые предпосылки формирования и современные тенденции развития института персональных данных в трудовом праве [Текст]/ Ф.А. Абаев // Пробелы в российском законодательстве. 2013. – № 5. – С. 136-139.

12. Абаев, Ф.А. Понятие, правовая природа персональных данных [Текст]/ Ф.А. Абаев // Право и государство: теория и практика. 2014. –№ 3 (111). – С. 126-131.

13. Аленевская, В.В. Ограничение права на информацию в трудовых отношениях [Текст]/ В.В. Аленевская // Вестник Прикамского социального института. Гуманитарное обозрение. 2014. – № 1 (8). – С. 42-49.

14. Ануфриева, Н.С. Правовые проблемы обработки персональных данных в трудовых отношениях [Текст]/ Н.С. Ануфриева // Актуальные проблемы современной юридической науки: Сборник научных трудов. Сургут: ИЦ СурГУ, 2012. – С. 114-119.

15. Астахова, Л.В., Рублёв Е.Л. Проблемы защиты персональных данных в период смены нормативной базы и пути их решения [Текст]/ Л.В. Астахова, Е.Л. Рублёв // Вестник УрФО. Безопасность в информационной сфере. 2013. – № 1 (7). – С. 32-41.

16. Барышников, А.Б. Безопасность корпоративных центров обработки персональных данных [Текст]/ Барышников А.Б. // Защита информации. Инсайд. 2013. - № 6 (54). С. 40-41.

17. Бегларян, М.Е. Безопасность персональных данных в современной России [Текст]/ М.Е. Бегларян, Е.А. Пичкуренко // Уголовная политика в сфере обеспечения здоровья населения, общественной нравственности и иных социально-значимых интересов материалы 4-ой Международной научно-практической конференции. 2015. С. 24-28.

18. Беденкова, А.А. Правовой статус персональных данных работников [Текст]/ А.А.Беденкова, И.С. Хоменко // Вестник науки Сибири. 2014. - № 4 (14). С. 148-151.

19. Бобров, И.В. Проблема защиты персональных данных работника [Текст]/ И.Вю Бобров, Ю.В. Комарецев // Проблемы российского законодательства и международного права Сборник статей Международной научно-практической конференции. Ответственный редактор: Сукиасян Асатур Альбертович . 2015. - С. 26-28.

20. Бойкова, О.Ф. Обрабатываем персональные данные работников [Текст]/ О.Ф. Бойкова // Независимый библиотечный адвокат. 2012. - № 2. С. 21-32.

21. Болотин, В.С. Механизм защиты права на неприкосновенность частной жизни при обработке персональных данных в информационных системах [Текст]/ В.С.Болотин, М.А. Маслёха // Вестник государственного и муниципального управления. 2012. - № 3. С. 99-103.

22. Бондарь, А.О. Организация работы по обеспечению защиты государственных информационных систем персональных данных [Текст]/ А.О. Бондарь, В.П. Железняк, В.А. Мещеряков // Техника и безопасность объектов уголовно-исполнительной системы: сборник материалов Международной научно-практической конференции. Воронеж: ИПЦ «Научная книга», 2013.- С. 174-175.

23. Балашкина, И. В. Особенности конституционного регулирования права на неприкосновенность частной жизни в Российской Федерации [Текст]/ И. В. Балашкина. // Право и политика. 2017. – №7. – С. 92-105.

24. Блоцкий, В.Н. Конституционное обеспечение права человека на неприкосновенность частной жизни в Российской Федерации [Текст]/ В.Н. Блоцкий. // Автореф. дис. канд. юрид. Наук – М. 2017. – с. 31.

25. Борисова, С. А. Общие требования при обработке персональных данных работника и гарантии их защиты [Текст]/ С. С. Борисова // Трудовое право. 2013. – N 11. – С. 30-36.

26. Бобылева, М.П. Вопросы использования элементов электронного документооборота внутри организации [Текст]/ М.П. Бобылева// Делопроизводство. 2013. – №2. – С. 15.

27. Герасимов А. А. Задача моделирования процессов защиты информации в информационных системах персональных данных / А.А. Герасимов// Интеллектуальные системы – М. : МГТУ им. Н. Э. Баумана. 2012. – С. 588-589.

28. Грушо, А. А. Теоретические основы компьютерной безопасности: учеб. пособие / А.А. Грушо. : Академия Москва. 2013. 272 с.

29. Гугуева, Т. А. Конфиденциальное делопроизводство [Текст] : учеб. пособие / Т.А. Гугуева. – М. : Альфа-М ; ИНФРА-М. 2016. – 192 с.

30. Гугуева, Т. А. Конфиденциальное делопроизводство [Текст] : учеб. пособие / Т.А. Гугуева. – М. : Альфа-М ; ИНФРА-М, 2016. – 192 с.

31. Дворянкин, С. В. Обеспечение информационной безопасности в распределенных системах обработки данных / С.В. Дворянкин. // Безопасность информационных технологий. 2012. №1. С. 92-93.

32. Ищейнов, В. Я. Персональные данные в законодательных и

нормативных документах Российской Федерации и информационных системах[Текст] / В. Я. Ищейнов // Делопроизводство. 2015. – N 3. – С. 87-90.

33. Кузнецова, Т. В. Организация работы с персональными данными [Текст] / Т. В. Кузнецова // Делопроизводство. 2014. – № 2. – С. 3–8.

34. Лушников, А. М. Защита персональных данных работника: сравнительно-правовой комментарий гл.14 Трудового кодекса РФ [Текст]/ А.М. Лушников // Трудовое право. 2016 – № 9. – С. 93-101.

35. Маркевич, А. С. Организационно-правовая защита персональных данных в служебных и трудовых отношениях [Текст]: Автореф. дис. на соиск. уч. ст. канд. юрид. наук./ А. С. Маркевич. – Воронеж, 2015. – 28 с.

36. Макаров, А.М. Организация защиты персональных данных : лабораторный практикум / Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет», Министерство образования и науки Российской Федерации ; авт.-сост. А.М. Макаров, И.В. Калиберда и др. - Ставрополь : СКФУ. 2015. - 92 с.

37. Маслеха, М.А. Теоретические основы защиты персональных данных // Законность и правопорядок в современном обществе. 2012. - № 8. – С. 94-103.

38. Международные трудовые стандарты и российское трудовое право: перспективы координации: монография / Э.Н. Бондаренко, Е.С. Герасимова, С.Ю. Головина и др.; под ред. С.Ю. Головиной, Н.Л. Лютова. М.: НОРМА, ИНФРА-М, 2016.

39. Меликов, У.А. Гражданско-правовая защита персональных данных // Вестник УрФО. Безопасность в информационной сфере. 2015. – № 4 (18). – С. 49-53.

40. Меньшикова, А.В. Некоторые проблемы защиты персональных данных работника, перспективы и пути их решения // Экономика и менеджмент инновационных технологий. 2014. – № 11 (38). – С. 156-159.

41. Минаев, В. А. Информационные операции и проблема формирования Современной культуры информационной безопасности / В. А. Минаев // Системы

высокой доступности. 2017. №3. – С. 38-46.

42. Минбалеев, А.В. Проблемные вопросы понятия и сущности персональных данных // Вестник УрФО. Безопасность в информационной сфере. 2012. – № 2 (4). – С. 4-9.

43. Мищенко, Е.Ю., Соколов А.Н. Количественные критерии идентификации физического лица при обезличивании персональных данных // Вестник УрФО. Безопасность в информационной сфере. 2014. - № 1 (11). -С. 27-33.

44. Новичкова, Ю. В. Персональные данные - без права передачи, или Особенности расторжения трудового договора за разглашение персональных данных[Текст]/ Ю. в. Новикова // Справочник кадровика. – 2016. – N 1. – С. 14-23.

45. Пелешенко, В.С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления : учебное пособие / В.С. Пелешенко, С.В. Говорова, М.А. Лапина ; Федеральное государственное автономное образовательное учреждение высшего образования «Северо-Кавказский федеральный университет», Министерство образования и науки РФ. - Ставрополь : СКФУ, 2017. - 86 с.

46. Петренко, В.И. Защита персональных данных в информационных системах : учебное пособие / В.И. Петренко ; Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет», Министерство образования и науки Российской Федерации. - Ставрополь : СКФУ, 2016. - 201 с.

47. Савинцева, М. Н. Правовая защита персональной информации граждан в России [Текст]/ М. Н. Савинцева // Законодательство и практика масс-медиа. - 2013. - № 9. – С. 23

48. Соколова, О. С. Проблемы реализации Федерального закона «О персональных данных» [Текст]/ О. С. Соколова// Современное право. - 2011. - N 9. - С. 37-41.

49. Силакова О. В. Комплексная безопасность образовательного учреждения как важнейшее условие обеспечения безопасных условий проведения учебно-воспитательного процесса // Молодой ученый. — 2014. — №18.1. — С. 84-88.

50. Скрыль, С. В. Показатели эффективности информационных процессов и их защищенности в системах реального времени / С. В. Скрыль // Безопасность информационных технологий. – М. : МИФИ, 2012. - № 3. –С. 104-106.

51. Сычев М. П. Моделирование угроз информационной безопасности с использованием принципов системной динамики / М. П. Сычев // Вопросы радиоэлектроники. 2017. - № 6. – С. 75-82.

52. Федосова, М. А. Защита персональных данных работника [Текст]/ М.А. Федосова // Финансовые и бухгалтерские консультации. - 2017. - N 11. - С. 71-74.

53. Федосеева, Н.Н. Сущность и проблемы электронного документооборота [Текст] / Н.Н. Федосеева // Юрист. - 2016. - №6. - с.61 – 64

54. Хачатурян, Ю. А. Право работника на защиту персональных данных[Текст]/ Ю. А. Хачатурян // Современное право. - 2016. - N 1. - С. 43-51.

55. Чаннов, С. Е. Правовой режим персональных данных на государственной и муниципальной службе [Текст]/ С. Е. Чаннов // Российская юстиция. - 2017. - N 1. - С. 21-23.