МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
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 и управление службой информационной безопасности в образовательной организации СПО

Магистерская диссертация
по направлению 44.04.04 Профессиональное обучение
Направленность программы магистратуры
«Управление информационной безопасностью в профессиональном образовании»

Выполнил:
студент группы ЗФ-309/210-2-1,
Колганова Лариса Леонидовна
Научный руководитель:
к.п.н., старший преподаватель
кафедры АТ, ИТ и МОТД
Гафарова Елена Аркадьевна

Проверка на объём заимствований:
77,95 авторского текста
Работа рекомендована к защите
«01» февраля 2019 г.
Зав. кафедрой АТ, ИТ и МОТД
_____В.В. Руднев

Челябинск, 2019

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
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 (по отраслям)
Направленность (профиль): Управление информационной безопасностью в профессиональном образовании

ЗАДАНИЕ
на магистерскую диссертацию

Магистранту группы ЗФ-309/210-2-1 заочного отделения Колгановой Ларисе Леонидовне, обучающейся по программе магистратуры «Управление информационной безопасностью в профессиональном образовании».

Научный руководитель выпускной квалификационной работы: Гафарова Е.А., к.п.н., старший преподаватель кафедры АТ, ИТ и МОТД.

1.Тема квалификационной работы: «Организация и управление службой информационной безопасности в образовательной организации СПО», утверждена приказом Южно-уральского государственного гуманитарно-педагогического университета № 580-сз от «26» апреля 2017 г.

2. Материалы для выполнения магистерской диссертации:

2.1. Учебная, научно-техническая, педагогическая, методическая литература по теме магистерской диссертации: отчет по преддипломной практике в Верхнеуфалейском филиале ГБПОУ «Каслинский промышленно-гуманитарный техникум», нормативная и законодательная документация, специальная литература, периодические издания, Интернет.

3. Основные части магистерской диссертации (перечень подлежащих разработке вопросов) и сроки их выполнения представлены в нижеприведенной таблице:

Календарный план работы

	Перечень вопросов, подлежащих разработке в диссертации	Сроки
1	ВВЕДЕНИЕ Оговаривается значение и актуальность темы работы, объект и предмет исследования,	15.05.2017

	проблема, цель и задачи работы, пути их решения. Указываются методы исследования.	
2	Глава 1. Понятие и сущность информационной безопасности в образовательных организациях Выводы по главе 1	16.10.2017
3	Глава 2. Информационная безопасность, как ключевой фактор реализации программы АИС «Сетевой город. Образование» Выводы по главе 2	23.04.2018
4	Глава 3. Направления совершенствования информационной безопасности в организациях СПО в рамках реализации программы АИС «Сетевой город. Образование» Выводы по главе 3	29.12.2018
5	ЗАКЛЮЧЕНИЕ (объем в пределах 3 стр.) Содержит кратко и четко сформулированные выводы, и рекомендации.	29.12.2018
6	СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ Законы и нормативные акты, справочно-статистические материалы, монографии, учебники, сборники брошюры, статьи из периодической печати, иностранная литература.	29.12.2018
7	ПРЕЗЕНТАЦИЯ (НАГЛЯДНЫЕ МАТЕРИАЛЫ) предоставляется в виде слайдов рекомендаций Microsoft PowerPoint, 10-12 слайдов, раскрывающих содержание магистерской диссертации	28.01.2019
	ПРЕДВАРИТЕЛЬНАЯ ЗАЩИТА	28.01.2019
	СДАЧА МАГИСТЕРСКОЙ ДИССЕРТАЦИИНА КАФЕДРУ	18.02.2019

Дата выдачи задания «01» ноября 2017 года

Заведующий кафедрой АТ, ИТ и МОТД
Наименование кафедры

_____

Ф.И.О., ученое звание и степень Подпись заведующего кафедрой

Задание выдал: _____
Ф.И.О., ученое звание и степень Подпись научного руководителя

Задание принял_____
Ф.И.О магистранта Подпись магистранта

Аннотация
на магистерскую диссертацию
Колгановой Ларисы Леонидовны

Тема магистерской диссертации «Организация и управление службой информационной безопасности в образовательной организации СПО».

Магистерская диссертация содержит 89 страниц, 5 таблиц, 4 рисунка, 57 источник литературы, приложение - 1.

Ключевые слова: угроза, защита информации, информационная безопасность, персональные данные, Сетевой город. Образование.

Объектом исследования является функционирование службы информационной безопасности в образовательной организации СПО.

Цель магистерской диссертации – разработка и обоснование программы организации службы информационной безопасности в образовательной организации СПО.

В процессе исследования изучены теоретические аспекты: изучены понятие и сущность информационной безопасности в образовательных организациях; нормативно-правовое обеспечение АИС «Сетевой город. Образование», проведена оценка исходной защищенности ИСПДн в Верхнеуфалейском филиале ГБПОУ «Каслинский промышленно-гуманитарный техникум» техникуме.

В результате проведенного исследования разработана программа совершенствования информационной безопасности в Верхнеуфалейском филиале ГБПОУ «Каслинский промышленно-гуманитарный техникум», определены задачи службы информационной безопасности, разработано электронное учебно-методическое обеспечение для обучения персонала техникума «Персональные данные и их защита».

Магистрант Колганова Лариса Леонидовна _____
(Ф.И.О.) Подпись

Оглавление

Введение

Актуальность. Отличительной особенностью современности является переход от индустриального общества к информационному, в котором главным ресурсом становится информация. В этой связи информационная сфера представляет собой специфическую составляющую деятельности образовательной организации, связанную с созданием, хранением, распространением, передачей, обработкой и использованием информации.

С учетом усиления роли информации на современном этапе, правовое регулирование общественных отношений, возникающих в информационной сфере, является приоритетным направлением в Российской Федерации, целью которого является обеспечение информационной безопасности.

Обеспечение, создание и управление службы безопасности образования является одним из основных направлений информатизации, поскольку информационная безопасность является обязательным условием и одним из критериев эффективности образовательной организации и безопасности образовательного процесса в целом.

Становление научного направления «информационная безопасность и защита информации» в РФ связано с именами таких отечественных ученых, как А.А. Грушко, В.Ю. Гайкович, В.А. Герасименко, В.И. Герасимов, Н.Н. Дмитриевский, Г.В. Емельянов, В.А. Минаев, П.Д. Зегжда, В.В. Кульба, А.Г. Мамиконов, А.П. Першин, С.П. Расторгуев, А.А. Стрельцов, Е.Е. Тимонина, Л.М. Ухлинов, Д.С. Черешкин, В.В. Шураков, А.Б. Шелков и др.

Общие вопросы информационной безопасности посвящены в работах таких ученых, как В.В.Домарев, В.А. Галатенко, С.М. Доценко, В.Ф. Шпак, В.И. Ярочкин, А. Володин, Б. Байбурин, А.В. Петраков, А.Ю. Щербаков, Е.Б. Белов, А.А. Малюк и др.

Правовые аспекты информационной безопасности нашли отражение в трудах Ю.М. Батурина, И.Л. Бачило, В.А. Копылова, В.Н. Лопатина, Ю.А. Тихомирова, М.А. Федотова и др.

Технические стороны информационной безопасности отражены в работах А.П. Тимофеев, А.В. Соколов, Г. Н. Устинова, В.Г. Проскурин, С.А. Маркова, О.Ю. Макаров и другие.

Законодательство в области обеспечения информационной безопасности представлено различными нормативно-правовыми актами, включая Федеральные Законы, Постановления Правительства, Указы Президента, ведомственные приказы Федеральной службы по техническому и экспортному контролю (ФСТЭК России), Федеральной службы безопасности Российской Федерации (ФСБ России), Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) и Федерального агентства правительственной связи и информации при Президенте Российской Федерации (ФАПСИ).

Федеральный закон (ФЗ) «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ регулирует отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации; применении информационных технологий; обеспечении защиты информации. В силу того, что образовательные организации в своей деятельности неизбежно сталкиваются с информацией в различных формах её представления, действие данного ФЗ распространяется и на них.

В статье 5 ФЗ «Об информации, информационных технологиях и о защите информации» говорится о том, что информация, в зависимости от категории доступа к ней, подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами. К информации ограниченного доступа относятся персональные данные. Отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами, органами местного самоуправления, иными муниципальными органами, юридическими лицами и физическими лицами с использованием

средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, регламентируются Федеральным законом «О персональных данных» от 27.07.2006 N 152-ФЗ. Целью настоящего Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Все образовательные организации являются операторами персональных данных, так как при организации образовательного процесса сталкиваются с обработкой информации, в том числе и в первую очередь с обработкой персональных данных. Согласно нормативно-правовым актам в области обеспечения защиты персональных данных в обязанности оператора персональных данных входит обеспечение безопасности персональных данных, которое достигается путем определения актуальных угроз информационной безопасности, классификация ИСПДн, применение правовых, организационных и технических мер по защите информации.

Персональные данные являются наиболее значимым и наиболее уязвимым компонентом информационных ресурсов образовательной организации.

Лицам, нарушившим требования закона о персональных данных, в зависимости от конкретных обстоятельств и серьезности деяния может грозить не только административная и уголовная ответственность, но также гражданско-правовая и даже дисциплинарная. При этом административная ответственность с 1 июля 2017 года ужесточилась – вместо одного состава правонарушения ст. 13.11 КоАП РФ теперь предусматривает семь, а максимальный штраф составляет 75 тыс. руб. Ответственность за нарушение ФЗ «О персональных данных» не ограничивается административными штрафами, отдельные нормы Трудового, Гражданского и Уголовного кодексов РФ также предусматривают санкции для операторов-правонарушителей.

Необходимость обеспечения нормативных требований и учета специфики организационно-правовых и программно-аппаратных мер защиты информационных ресурсов, и в частности, персональных данных в конкретной образовательной организации определяют **актуальность** темы диссертации.

Для большинства служб информационной безопасности образовательных организаций обеспечение достаточного уровня защиты информационных ресурсов согласованным набором различных мер является **проблемой.**

Целью исследования является разработка и обоснование программы организации службы информационной безопасности в образовательной организации СПО.

Объект исследования: функционирование службы информационной безопасности в образовательной организации СПО.

Предмет исследования: реализация мер по обеспечению безопасности персональных данных в образовательной организации СПО службой информационной безопасности.

Гипотеза исследования состоит в предположении о достаточном уровне защищенности персональных данных при условии реализации программы, содержащей меры по обеспечению нормативных рекомендаций, разработанной на основе анализа частной модели угроз в образовательной организации для службы информационной безопасности.

В соответствии с объектом, предметом и целью исследования были поставлены следующие **задачи:**

- рассмотреть основные составляющие и специфику информационной безопасности образовательной организации СПО;
- описать нормативно-правовое обеспечение АИС «Сетевой город. Образование»;

– раскрыть реализацию программы АИС «Сетевой город. Образование» на примере муниципалитета (Верхнеуфалейский городской округ);

– оценить исходную защищенность ИСПДн в Верхнеуфалейском филиале государственного бюджетного профессионального образовательного учреждения «Каслинский промышленно-гуманитарный техникум»;

– разработать программу совершенствования службы информационной безопасности в Верхнеуфалейском филиале государственного бюджетного профессионального образовательного учреждения «Каслинский промышленно-гуманитарный техникум».

Методологическую основу исследования составили процессный и системный подходы, законодательные и нормативно-правовые документы РФ, разработки в области обеспечения информационной безопасности, методы и способы построения процессов управления информационной безопасностью в целях повышения ИБ в организациях.

Теоретическую и информационную базу исследования составляют основные положения по информационной безопасности, системный подход к исследуемому объекту и предмету, в качестве информационных источников использованы аналитические и статистические материалы по информационной безопасности, материалы научных конференций, средств массовой информации, отражающие аспекты информационной безопасности. нормативные акты и документы Управления образования Верхнеуфалейского городского округа.

Научная новизна исследования состоит в том, что показана возможность развертывания единой образовательной и информационной сетевой федеральной системы с включением в нее образовательных организаций СПО при сохранении достаточного уровня защиты персональных данных.

Практическая значимость работы заключается в разработке программы совершенствования службы информационной безопасности ГБПОУ «КПГТ» (Верхнеуфалейский филиал), разработанной на основе анализа частной модели угроз названной организации; разработке электронного учебно-методического обеспечения для обучения сотрудников техникума по организации работы с персональными данными, которое может быть применено в других образовательных организациях СПО.

База исследования: Верхнеуфалейский филиал государственного бюджетного профессионального образовательного учреждения «Каслинский промышленно-гуманитарный техникум».

Апробация исследования: Колганова Л.Л. Опыт организации защиты персональных данных в образовательных организациях / Л.Л. Колганова // Инновации в информационных технологиях, машиностроении и автотранспорте: сборник материалов II Международной научно-практической конференции (03 - 04 октября 2018 года), Кемерово / ФГБОУ ВО «Кузбас. гос. техн. ун-т им. Т. Ф. Горбачева»; редкол.: Д.М. Дубинкин (отв. ред.) [и др.]. – Кемерово, 2018. С. 51-53; Колганова Л.Л. Реализация программы АИС «Сетевой город. Образование» на примере муниципалитета Верхнеуфалейский городской округ / Л.Л. Колганова // Международная научно-практическая конференция «Приоритеты мировой науки: эксперимент и научная дискуссия». 2019. С. 37-39; Колганова Л.Л. Организация защиты персональных данных при их обработке в автоматизированных информационных системах / Л.Л. Колганова // Международная научно-практическая конференция «Научно-технический прогресс как фактор развития современного общества», 2019. С. 88-90.

Структура магистерской диссертации состоит из введения, трех глав, заключения, библиографического списка, состоящего из 57 наименований, приложение. Работа содержит 4 рисунка. Общий объем работы составляет 89 страниц.

Глава 1. Понятие и сущность информационной безопасности в образовательных организациях

1.1. Основные составляющие информационной безопасности

Система обеспечения информационной безопасности организации – эффективный инструмент защиты интересов собственников и пользователей информации. Следует отметить, что ущерб может быть нанесен не только несанкционированным доступом к информации. Он может быть получен в результате поломки коммуникационного или информационного оборудования. Особенно актуальна эффективная организация обеспечения безопасности информационных банковских систем и организаций открытого типа (учебные, социальные и др.).

Вопросы информационной безопасности занимают особое место и в связи с возрастающей ролью в жизни общества требуют к себе все большего внимания. Успех практически любой деятельности в немалой степени зависит от умения распоряжаться такой ценностью, как информация. В законе РФ «Об информации, информатизации и защите информации» подчеркивается, что «информационные ресурсы являются объектами собственности граждан, организаций, общественных объединений, государства».

Информационная безопасность - достаточно сложная и многогранная проблема, решение которой под силу хорошо организованным структурам и успех может принести только систематический, комплексный подход. Для решения данной проблемы рассматриваются меры законодательного, административного, процедурного и программно-технического уровня.

Возникновение проблемы информационной безопасности во многом связано с созданием и повсеместным использованием ЭВМ и, на их основе, разнообразных организационно-технических («человек-машина») систем. Важнейшим классом таких систем являются автоматизированные системы управления (АСУ), в которых сбор, хранение и обработка данных при

реализации функций управления осуществляется средствами автоматизации и ВТ.

Предметом защиты является информация, хранящаяся, обрабатываемая и передаваемая в компьютерных (информационных) системах.

Объектом защиты информации является компьютерная (информационная) система или автоматизированная система обработки информации (АСОИ).

Под автоматизированной системой обработки информации (АСОИ) понимают организационно-техническую систему, представляющую собой совокупность следующих взаимосвязанных компонентов:

– технических средств обработки и передачи данных (СВТ и связи);

– методов и алгоритмов обработки в виде программного обеспечения;

– информации (массивов, наборов, баз данных) на различных носителях;

– персонала и пользователей системы, объединенных по организационно-структурному, тематическому, технологическому или другим признакам для выполнения автоматизированной обработки информации (данных) с целью удовлетворения информационных потребностей субъектов информационных отношений.

Для того чтобы наладить должное обеспечение защиты информации следует иметь четкое представление об основных понятиях, целях и роли информационной безопасности.

Словосочетание *«информационная безопасность»* в разных контекстах может иметь различный смысл. В Доктрине информационной безопасности Российской Федерации термин «информационная безопасность» используется в широком смысле. Имеется в виду состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.

Информационная безопасность АС - состояние рассматриваемой автоматизированной системы, при котором она, с одной стороны, способна противостоять дестабилизирующему воздействию внешних и внутренних информационных угроз, а с другой ее наличие и функционирование не создает информационных угроз для элементов самой системы и внешней среды.

В Законе РФ «Об участии в международном информационном обмене» информационная безопасность определяется аналогичным образом - как состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

Под *информационной безопасностью* понимают защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

Защита информации - это комплекс мероприятий, направленных на обеспечение информационной безопасности, ее целостности и конфиденциальности информации при условии ее доступности для пользователей, имеющих соответствующие права.

Таким образом, правильный с методологической точки зрения подход к проблемам информационной безопасности начинается с выявления *субъектов информационные отношений* и интересов этих субъектов, связанных с использованием информационных систем (ИС). Угрозы информационной безопасности - это оборотная сторона использования информационных технологий.

Из этого положения можно вывести два важных следствия:

1. Трактовка проблем, связанных с информационной безопасностью, для разных категорий субъектов может существенно различаться.

2. Информационная безопасность не сводится исключительно к защите от несанкционированного доступа к информации, это принципиально более широкое понятие. Субъект информационных отношений может пострадать (понести убытки и/или получить моральный ущерб) не только от несанкционированного доступа, но и от поломки системы, вызвавшей перерыв в работе. Более того, для многих открытых организаций (например, образовательных организаций) собственно защита от несанкционированного доступа к информации стоит по важности отнюдь не на первом месте.

Информационная безопасность - многогранная, можно даже сказать, многомерная область деятельности, в которой успех может принести только систематический, комплексный подход.

Спектр интересов субъектов, связанных с использованием информационных систем, можно разделить на следующие категории: обеспечение *доступности, целостности* и *конфиденциальности* информационных ресурсов и поддерживающей инфраструктуры.

Поясним понятия доступности, целостности и конфиденциальности.

Доступность - это возможность за приемлемое время получить требуемую информационную услугу.

Под *целостностью* подразумевается актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.

Конфиденциальность - это защита от несанкционированного доступа к информации.

Источниками конфиденциальной информации в информационных системах являются люди, документы, публикации, технические носители, технические средства обработки информации, продукция, промышленные и производственные отходы.

В большинстве случаев активные действия противоборствующих сторон по сбору информации осознаны и целенаправленны. К ним относятся:

- разглашение конфиденциальной информации ее обладателем;

- утечка информации по различным (в основном-техническим) каналам;
- несанкционированный доступ к конфиденциальной информации различными способами.

Конфиденциальность - самый проработанный у нас в стране аспект информационной безопасности. К сожалению, практическая реализация мер по обеспечению конфиденциальности современных информационных систем наталкивается в России на серьезные трудности. Во-первых, сведения о технических каналах утечки информации являются закрытыми, так что большинство пользователей лишено возможности составить представление о потенциальных рисках. Во-вторых, на пути пользовательской криптографии как основного средства обеспечения конфиденциальности стоят многочисленные законодательные препятствия и технические проблемы. Наконец, конфиденциальные моменты есть также у многих организаций (даже в образовательных организациях стараются не разглашать сведения о зарплате сотрудников) и отдельных пользователей (например, пароли).

Цель защиты информации – минимизация ущерба вследствие нарушения требований целостности, конфиденциальности и доступности.

Основополагающим элементом формирования представлений о безопасности является выделение понятия «угроза» как причины нарушения состояния безопасности. Угрозы могут быть как реальными, т.е. уже проявившимися в своем негативном, разрушительном воздействии на объект безопасности, так и потенциальными, т.е. их негативное воздействие может проявить себя в ближайшем или отдаленном будущем [12].

Под угрозой (в общем смысле) обычно понимают потенциально возможное событие (воздействие, процесс или явление), которое может привести к нанесению ущерба чьим-либо интересам, в частности под угрозой безопасности автоматизированных систем (АС) обработки информации понимается возможность воздействия на АС, которое прямо или косвенно может нанести ущерб ее безопасности. АС является наиболее уязвимой частью информационной системы персональных данных (ИСПДн),

поскольку предоставляет злоумышленнику самый быстрый доступ к информации, во отличии от базы данных (БД), хранящихся на бумажных носителях.

Угроза информации - возможность возникновения (на каком-либо этапе жизнедеятельности системы) явления или события, следствием которого могут быть нежелательные воздействия на информацию [11].

Для формирования политики информационной безопасности (ИБ) в образовательной организации (ОО) необходимо, прежде всего, определить субъектов и категории участников информационного обмена. Определить характер и уровень информационных угроз, который может исходить от них [14].

Анализ специальной литературы по рассматриваемой проблематике позволяет констатировать, что проблема комплексного обеспечения информационной безопасности субъектов образовательного процесса на всех уровнях образования является малоизученной и нуждается в отдельной проработке. Это тем более актуально, что организация обеспечения безопасности информации должна носить комплексный характер и основываться на глубоком анализе возможных негативных последствий.

При этом важно не упустить какие-либо существенные аспекты. Анализ негативных последствий предполагает обязательную идентификацию возможных источников угроз, факторов, способствующих их проявлению и, как следствие, определение актуальных угроз безопасности информации.

Выделяются различные классификации угроз информационной безопасности. Обзор различных точек зрения на исследуемый предмет позволил сделать вывод, что в настоящее время нет достаточно обоснованной и подробной общей классификации угроз информационной безопасности и их источников.

Общая схема классификации угроз ИБ представлена на рисунке 1.

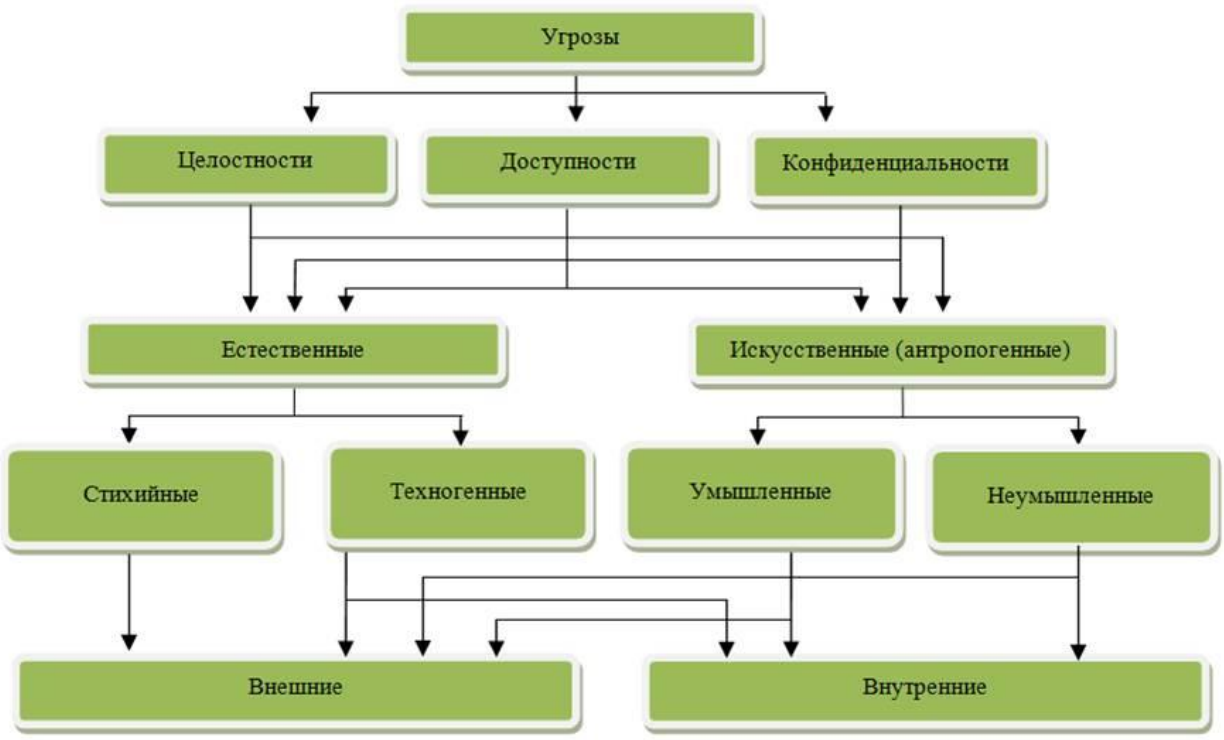

Рис.1. – Классификация угроз информационной безопасности [2]

Таким образом, классификацию угроз, характерных для той или иной системы можно продолжать, основываясь при этом либо на методологиях, описанных в отечественных и зарубежных стандартах, либо используя практический опыт, но в любом случае их перечисление является важным этапом определения уязвимостей и создает фундамент для будущего проведения анализа рисков.

Анализ классифицированных угроз создает предпосылки для формирования в образовательной организации специальной службы информационной безопасности. При этом в зависимости от актуальных угроз информационной безопасности необходимо разработать условия безопасного использования соответствующих образовательных информационных сервисов.

Обеспечение информационной безопасности субъектов и объектов образовательного процесса представляет собой многоаспектную междисциплинарную проблему, решение которой во многом сказывается на состоянии национальной безопасности общества в целом.

1.2. Специфика информационной безопасности в образовательных организациях

Информационная безопасность является одним из важнейших аспектов интегральной безопасности, на каком бы уровне мы ни рассматривали последнюю - национальном, отраслевом, корпоративном или персональном.

Разнообразные информационные системы достаточно давно и эффективно используются в образовательном процессе колледжа, активизируя познавательную активность обучающихся, влияя на их творческие способности, на вовлеченность в образовательный процесс. Однако это только одна из граней внедрения и введения информационных систем в образовательную организацию. Другой особенностью является использование систем не только в качестве обучающих средств, но и в поддержке организации данного процесса, и в управлении образовательной организации.

Таким образом, вопрос организации защиты информации в образовательной организации является в достаточной степени актуальным и диктует свои требования к защите ресурсов образовательных организаций и ставит задачу построения собственной интегрированной системы безопасности. Ее решение предполагает наличие нормативно-правовой базы, формирование концепции безопасности, разработку мероприятий, планов и процедур по безопасной работе, проектирование, реализацию и сопровождение технических средств защиты информации в рамках образовательной организации.

Информационная безопасность образовательных организаций отличается от информационной безопасности других предприятий и организаций. Это обусловлено, прежде всего, специфическим характером угроз, а также публичной деятельностью образовательных организаций, которые вынуждены делать доступ к информационным ресурсам легким с целью удобства для граждан.

Информационная безопасность в организациях профессионального образования должна учитывать следующие специфические факторы:

- конфиденциальность информации (несанкционированное получение информации, в т.ч. персональных данных педагогов и студентов, служебной информации о самой образовательной организации);

- технические сбои и неполадки вычислительной техники и аппаратуры передачи данных, нарушения энергообеспеченности техники, физическое уничтожение или порча техники и др.;

- вредоносное и нежелательное программное обеспечение, хакерские атаки и спам;

- несанкционированное использование нелицензионного программного обеспечения сотрудниками образовательной организации;

- недисциплинированность и бесконтрольность педагогов, учебно-вспомогательного персонала и студентов в вопросах защиты информации;

- непонимание и незнание проблем информационной безопасности;

- нарушение авторских прав и прав интеллектуальной собственности.

С учетом зарубежного и отечественного опыта обеспечение информационной безопасности осуществляется по следующим направлениям:

– правовая защита – это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;

– организационная защита – это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба;

– инженерно-техническая защита – это использование различных технических средств, препятствующих нанесению ущерба [4].

Следует помнить, что информация существует в различных формах. Ее можно хранить на компьютерах, передавать по локальным сетям и через Интернет, распечатывать на бумажных носителях, копировать, сканировать,

а также озвучивать в разговорах. В целях безопасности все виды носителей информации (документы, пленки, магнитные ленты, дискеты, диски и др.), используемые для ее хранения, должны быть надлежащим образом защищены.

В образовательной организации для обеспечения информационной безопасности необходимо:

- во-первых, целесообразно обеспечить защиту компьютеров от внешних несанкционированных воздействий (компьютерные вирусы, логические бомбы, атаки хакеров и т.д.). Решение данной проблемы возможно только при условии, исключающем вывод локальных сетей образовательной организации на Интернет, либо размещение своего сайта у удаленного провайдера;

- во-вторых, необходимо иметь как минимум два сервера. Наличие хороших серверов позволит протоколировать любые действия работников образовательной организации в вашей локальной сети;

- в-третьих, необходимо установить строгий контроль за электронной почтой, обеспечив постоянный контроль за входящей и исходящей корреспонденцией;

- в-четвертых, установка соответствующих паролей на персональные ЭВМ, а также определение работы с информацией на съемных носителях ЭВМ (флэшки, диски). И самое главное, класс информатики не должен быть подключен к локальным сетям образовательной организации.

В свою очередь, ст. 16 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях по защите информации» определяет порядок защиты информации. В соответствии с данной статьей защита информации представляет собой принятие правовых, организационных и технических мер. Меры должны быть направлены на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления,

распространения, а также от иных неправомерных действий в отношении такой информации [8].

Кроме того, определяется и ответственность граждан за защиту информации. Так, п. 5 ст. 9 Закона № 149-ФЗ гласит: «Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению такой информации» [8].

Такая обязанность возлагается Трудовым кодексом РФ (далее – ТК РФ), гл. 14 которого определяет защиту персональных данных работника. В соответствии со ст. 90 ТК РФ: «Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами».

Для развития данных положений в РФ 27.07.2006 принят Федеральный закон № 152-ФЗ «О персональных данных», который вступил в силу с 1 января 2008 г. Его основной целью является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в т.ч. защиты прав на неприкосновенность частной жизни, личную и семейную тайны [7].

Статья 3 данного закона определяет: «Персональные данные – любая информация, относящаяся к определенному или неопределенному на основании такой информации лицу (субъекту персональных данных), в т.ч. его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация» [7].

Вопрос обеспечения правового поля защиты персональных данных в общеобразовательной организации в настоящее время особенно актуален, так

как, во-первых, такие данные должны храниться в электронном виде, а во-вторых, оператор, обрабатывающий такие данные, в соответствии с ч. 1 ст. 19 закона № 152-ФЗ должен предпринимать все необходимые организационно-технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, от иных неправомерных действий. Постановлением Правительства РФ от 1 ноября 2012 г. N 1119 утверждено Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных [7].

На основании положений ст. 1 Федерального закона Российской Федерации от 27 июля 2006 г. N 152-ФЗ «О персональных данных», законом регулируются отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами, органами местного самоуправления, не входящими в систему органов местного самоуправления муниципальными органами, юридическими лицами, физическими лицами с использованием средств автоматизации или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации.

Основные нормативные правовые акты в сфере персональных данных:

1. Федеральный закон от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Федеральный закон от 27.07.2006 г. №152-ФЗ «О персональных данных».

3. Федеральный закон от 21.07.2014 г. №242 «..«о запрете хранения ПДн россиян заграницей» (вступилвсилу01.09.2015г).

4. Постановление Правительства РФ от 01.11.2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

5. Постановление Правительства РФ от 15.09.2008 г. №687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

6. Постановление Правительства РФ от 21.03.2012 г №211. «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

7. Административный регламент проведения проверок Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций при осуществлении федерального государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных (Приказ Роскомнадзора от 11.11.2011 №312).

8. Приказ Роскомнадзора от 19.08.2011г. №706 «Об утверждении Рекомендаций по заполнению образца формы уведомления об обработке (о намерении осуществлять обработку) персональных данных».

9. Приказ Минкомсвязи от 28.08.2015 №315 «О внесении изменений в Административный регламент Роскомнадзора…» «…О месте нахождения базы данных информации, содержащей персональные данные».

10. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Приказ ФСТЭК РФ от 15.02.2008).

11. Методика определения актуальных угроз безопасности персональных данных при их обработке, в информационных системах персональных данных (Приказ ФСТЭК РФ от 14.02.2008 г.).

12. Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

13. Приказ Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. №17 «Требования о защите информации, не содержащей государственную тайну, содержащейся в государственных информационных системах».

14. Методический документ**.** Меры защиты информации в государственных информационных системах. (Утверждено ФСТЭК России 11.02.2014г.).

15. Банк данных угроз безопасности информации. (Утверждено ФСТЭК России 06.03.2015 №240/22/879).

16. Приказ 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 (Приказ ФСБ РФ от 10.07.2014 г. №378).

На рисунке 2 представлена структура законодательства РФ по персональным данным.

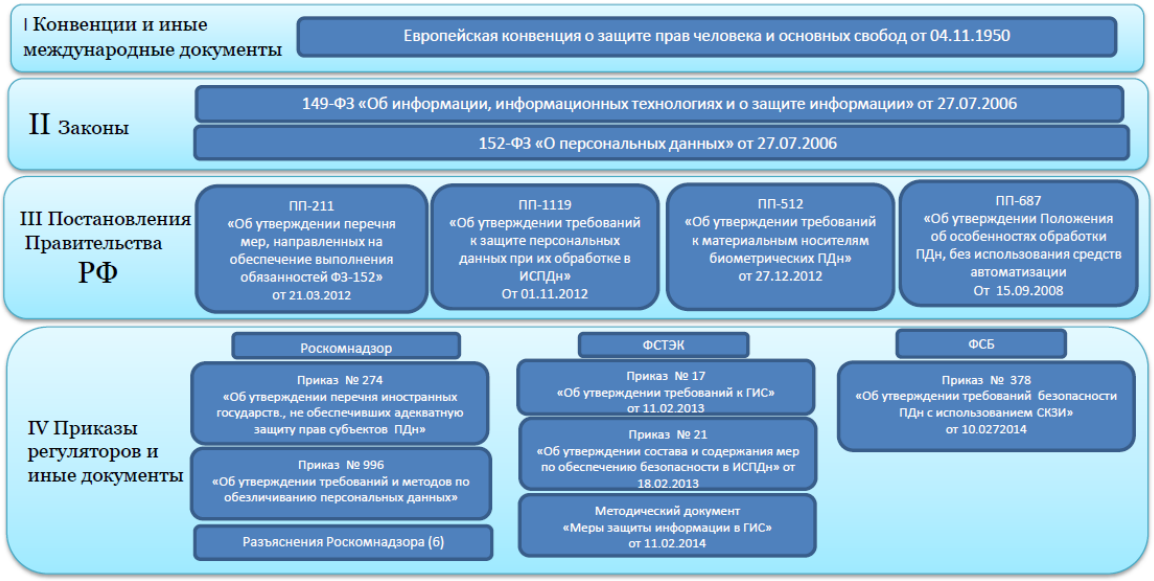

Рис.2. – Структура законодательства РФ по персональным данным

Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Нормативные правовые акты, регламентирующие размещение персональных данных на сайте образовательной организации:

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

- ПП от 10.07.2013 №582 «Об утверждении Правил размещения на официальном сайте образовательной организации в сети «Интернет» и обновления информации об образовательной организации»;

- Приказ Минобрнауки от 29.05.2014 №785 «Об утверждении требований к структуре официального сайта образовательной организации в сети «Интернет» и формату представления на нем информации»;

- Письмо Рособрнадзора от 25.03.2015 №07-675 с «Методическими рекомендациями представления информации об образовательной организации в открытых источниках с учетом соблюдения требований законодательства в сфере образования»;

- Приказ Роскомнадзора от 05.09.2013 №996 «Об утверждении требований и методов по обезличиванию персональных данных»;

- Методические рекомендации Роскомнадзора от 14.12.2012 «Разъяснение вопросов, касающиеся обработки персональных данных работников, соискателей и лиц, находящихся в кадровом резерве».

Документы, определяющие политику в отношении обработки персональных данных, подлежат опубликованию на официальном сайте государственного или муниципального органа в течение 10 дней после их утверждения.

Оценивая законодательную базу, следует обратить внимание, что к объектам информационной безопасности в Минобрнауки России, региональных министерствах (департаментах) образования, муниципальных органах управления образованием и в образовательных организациях относят:

– сведения, составляющие государственную тайну, в соответствии с выписками из перечня сведений, подлежащих засекречиванию в министерствах, ведомствах и организациях;

– информационные ресурсы, содержащие документированную информацию, в соответствии с перечнем сведений конфиденциального характера;

– информацию, защита которой предусмотрена законодательными актами РФ, в т.ч. и персональные данные;

– средства и системы информатизации, программные средства, автоматизированные системы управления, системы связи и передачи данных, осуществляющие прием, обработку, хранение и передачу информации с ограниченным доступом.

Персональные данные (ПДн) - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

К ПДн могут относиться:

1. ПДн работников организации:

- фамилия, имя, отчество;
- сведения об идентификационном номере налогоплательщика;
- сведения о пенсионном страховом свидетельстве;
- дата рождения, место рождения, гражданство;
- данные об образовании;
- данные документа, удостоверяющего личность (вид, серия, номер, дата выдачи, наименование органа, выдавшего документ);
- адрес и дата регистрации по месту жительства, адрес проживания;
- телефонный номер, адрес электронной почты;
- занимаемая должность (специальность, профессия), разряд, класс (категория) квалификации, стаж работы;
- сведения о наградах, поощрениях, почетных званиях (наименование, номер, дата награды) и др.

2. ПДн граждан (обучающиеся, родители.):

- фамилия, имя, отчество;
- дата рождения, пол;
- адрес и дата регистрации по месту жительства, адрес проживания;
- данные документа, удостоверяющего личность;
- контактный телефон;
- срок начала и окончания обучения;
- сведения об успеваемости, сведения о научной деятельности;
- фотография;
- банковские реквизиты для перевода денежных сумм;
- сведения о совершенном правонарушении и др.

Состав и содержание сведений, относящихся к ПДн, зависит от особенностей деятельности организации и влияет на категорию ПДн и их уровень защищенности в информационной системе.

Информационная система персональных данных (далее –ИСПДн) - совокупность содержащихся в базах данных персональных данных и

обеспечивающих их обработку информационных технологий и технических средств.

Информационные системы персональных данных в образовательной организации:

- ИСПДн «Бухгалтерия и Кадры» - цель: трудовые отношения, кадровое делопроизводство, бухгалтерский учет;

- ИСПДн «Граждане» - цель: предоставление социальных услуг.

Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы.

Система защиты персональных данных включает в себя:

- организационные;

- и (или) технические меры, определенные с учетом актуальных угроз безопасности ПДн.

Безопасность ПДн обеспечивает Оператор или лицо (уполномоченное лицо), осуществляющее обработку ПДн по поручению оператора на основании заключаемого договора. Договор должен предусматривать обязанность уполномоченного лица обеспечить безопасность ПДн.

Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к ПДн при их обработке в ИСПДн, результатом которого могут стать: уничтожение; изменение; блокирование; копирование; предоставление; распространение персональных данных; а также иные неправомерные действия.

Таким образом, можно сделать вывод, что информационная безопасность является одним из составных элементов комплексной безопасности образовательной организации.

Выводы по Главе I

По итогам первой главы магистерской диссертации главы можно сделать следующие выводы.

1. Раскрыты основные составляющие информационной безопасности в организациях среднего профессионального образования.

Информационная безопасность образовательных организаций отличается от информационной безопасности других предприятий и организаций. Это обусловлено, прежде всего, специфическим характером угроз, а также публичной деятельностью образовательных организаций, которые вынуждены делать доступ к информационным ресурсам легким с целью удобства для граждан.

Сформулированы и классифицированы угрозы, возникающие в информационных системах.

Под угрозами безопасности информационной системы понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации или несанкционированными, непреднамеренными воздействиями на нее.

Как правило, защита от угроз, в основном регламентируется инструкциями, разработанными и утвержденными оператором с учетом особенностей эксплуатации информационных систем организации и действующей нормативной базой учреждения.

2. Раскрыта специфика информационной безопасности в образовательных организациях.

Информационная безопасность в организациях профессионального образования должна учитывать следующие специфические факторы:

- конфиденциальность информации (несанкционированное получение информации, в т.ч. персональных данных педагогов и студентов, служебной информации о самой образовательной организации);

- технические сбои и неполадки вычислительной техники и аппаратуры передачи данных, нарушения энергообеспеченности техники, физическое уничтожение или порча техники и др.;

- вредоносное и нежелательное программное обеспечение, хакерские атаки и спам;

- несанкционированное использование нелицензионного программного обеспечения сотрудниками образовательной организации;

- недисциплинированность и бесконтрольность педагогов, учебно-вспомогательного персонала и студентов в вопросах защиты информации;

- непонимание и незнание проблем информационной безопасности;

- нарушение авторских прав и прав интеллектуальной собственности.

Глава 2. Информационная безопасность, как ключевой фактор реализации программы АИС «Сетевой город. Образование»

2.1 Нормативно-правовое обеспечение АИС «Сетевой город. Образование»

Сетевой Город. Образование – комплексная автоматизированная информационная система, объединяющая в единую сеть образовательные учреждения и органы управления образования в пределах города, сельского или городского района (округа). Тем самым формируется единое информационное образовательное пространство муниципального образования**.**

Права доступа к информации разграничены и гибко настраиваются. Каждый пользователь образовательного учреждения (директор, завуч, учащийся, учитель и т.д.) и родители учащихся имеют индивидуальные имя и пароль и могут входить в систему с любого компьютера, подключенного к муниципальной сети (или сети Интернет). Например, находясь дома или на работе, родитель может отслеживать успеваемость и посещаемость своего ребёнка, общаться с преподавателями и администрацией школы; учащийся может удалённо получать домашние задания, просматривать свой электронный дневник и расписание, и т.д.

Параллельно, в реальном времени к обобщённой информации по школам имеют доступ и специалисты органов управления образования для формирования статистических и иных отчетов в рамках своей компетенции, не требуя от руководителей школ отдельных отчетов с последующей работой по своду информации.

Федеральные нормативные правовые акты:

1. Федеральный закон от 07.07.2010 г. №210 - ФЗ Об организации предоставления государственных и муниципальных услуг.

2. Распоряжение Правительства РФ от 17.12.2009 г. № 1993-р. Свободный перечень первоочередных государственных и муниципальных услуг.

3. Постановление Правительства РФ от 24.10.2011 г. №861 О федеральных государственных информационных системах, обеспечивающих предоставление в электронной форме государственных и муниципальных услуг (осуществление функций).

4. Методические рекомендации по работе с документами в общеобразовательных учреждениях.

5. Письмо МОиН Российской Федерации от 15 февраля 2012 г. № АП - 147/07 О методических рекомендациях по внедрению систем ведения журналов успеваемости в электронном виде.

6. Методические рекомендации Системы ведения журналов успеваемости обучающихся в электронном виде в образовательных учреждениях Российской Федерации.

Региональные нормативные правовые акты:

1. Распоряжение Губернатора Челябинской области от 01.11.2010 г. №732-р «О плане мероприятий по реализации Федерального закона «Об организации предоставления государственных и муниципальных услуг».

2. Постановление Правительства Челябинской области от 13.12.2010 г. №293-П «О Порядке разработки и утверждения административных регламентов предоставления государственных услуг органами исполнительной власти Челябинской области».

3. Распоряжение Правительства Челябинской области от 11.11.2010 г. №331-рп «О Плане перехода на предоставление в электронном виде государственных услуг органами исполнительной власти Челябинской области и государственными учреждениями Челябинской области».

4. Постановление Правительства Челябинской области от 29.06.2011 г. №209-П «О Плане мероприятий по развитию информационного общества и формированию электронного правительства в Челябинской области на 2011-2013 годы».

5. Распоряжение Губернатора Челябинской области от 06.06.2011 г. №549-р «О перечне государственных услуг (функций) органов исполнительной власти Челябинской области».

6. Приказ Министерства образования и науки Челябинской области от 28.07.2016 г. № 01/2445 «О вводе в эксплуатацию автоматизированной системы «Образование Челябинской области»».

7. Приказ Министерства образования и науки Челябинской области от 09.10.2017 г. № 02/3043 «Об утверждении плана функционирования АИС «Образование» на 2017-2018 учебный год».

8. Приказ Министерства образования и науки Челябинской области от 25.09.2017 г. № 01/2866 «Об утверждении положения об автоматизированной информационной системе «Образование Челябинской области».

2.2 Реализация программы АИС «Сетевой город. Образование» на примере муниципалитета Верхнеуфалейский городской округ

С целью формирования на территории Челябинской области единой информационно-образовательной среды, обеспечивающей автоматизацию деятельности Министерства образования и науки Челябинской области; органов местного самоуправления, осуществляющих управление в сфере образования, и образовательных организаций, организацию электронного взаимодействия всех участников образовательных отношений в 2016 году введена в эксплуатацию автоматизированная информационная система «Образование Челябинской области» (АИС «Образование»).

В настоящее время Управление образование Верхнеуфалейского городского округа работает с различными информационными системами: «Сетевой город. Образование», «Е-услуги. Образование» и многие другие информационные системы.

В состав АИС «Образование» входит АИС «Сетевой город. Образование» – модульная комплексная информационная система, предназначенная для предоставления электронных средств поддержки и

сопровождения образовательной деятельности образовательных организаций, реализации государственных и муниципальных услуг в электронном виде в сфере образования, а также являющаяся инструментом сетевого взаимодействия между всеми участниками образовательных отношений и интеграции в единую сеть образовательных организаций и органов управления образованием.

АИС «Сетевой город. Образование» содержит комплект модулей, охватывающих управленческую деятельность муниципальных органов управления образованием, а также образовательную деятельность:

- дошкольных образовательных организаций.
- общеобразовательных организаций.
- организаций дополнительного образования.
- профессиональных образовательных организаций.

Модуль «Профессиональная образовательная организация» (АИС ПОО) предназначен образовательных организаций, осуществляющих образовательную деятельность по образовательным программам среднего профессионального образования и (или) по программам профессионального обучения.

Полное наименование системы: автоматизированная информационная система «Сетевой Город. Образование», модуль «Профессиональная образовательная организация». Условное обозначение системы: АИС «Сетевой Город. Образование», модуль ПОО.

Модуль для профессиональных образовательных организаций АИС ПОО позволяет решать административные задачи профессиональных образовательных организаций и проводить мониторинг текущего учебного процесса.

Модуль предоставляет инструменты для управления: расписанием звонков, занятий, сессий; журналами текущей успеваемости, итоговой и промежуточной аттестации, а также аттестации профессиональной деятельности; курсовыми работами; движением обучающихся - зачислением,

выбытием, переводом, оформлением академических отпусков и т.д.; списком дисциплин и рабочими программами по дисциплинам; образовательными программами и учебными планами; учебными календарями и календарно-тематическими планами; списками сотрудников, студентов, абитуриентов и родителей; списками учебных отделений и групп; должностями и правами доступа пользователей; статистической отчётностью и отчётностью по успеваемости и посещаемости обучающихся.

Внедрение данного модуля позволит:

– повысить качество профессионального образования и достичь новых образовательных результатов;

– автоматизировать управление системой профессионального образования и принимать обоснованные управленческие решения;

– оказывать государственные и муниципальные услуги в электронном виде в сфере образования;

– создать единое информационное пространство для взаимодействия всех участников образовательных отношений.

Установка серверов или какого-либо программного обеспечения в самих образовательных организациях не требуется. Права доступа к информации разграничены, каждый пользователь имеет доступ только к той информации, которую ему определил администратор системы.

Рассмотрим основные моменты организации учебного процесса в Системе пользователями.

1) Работа с Системой начинается с создания данных об образовательной организации.

Указывается:

1. Основная контактная информация, отражающая актуальные данные местонахождения ОО, статуса учреждения, телефоны для связи и ФИО руководителя.

2. Реквизиты, идентифицирующие учёт в налоговых органах.

3. Корпуса и аудитории, позволяющие в последующем составлять расписания занятий с учётом направлений, смен и расположения аудиторий в различных корпусах.

2) Пользователи - это следующий раздел при работе с Системой. Работа с этим меню заключается в создании данных по пунктам:

– права доступа, разграничивающие разрешение или запрещение тех или иных полномочий (например, при планировании обучения);

– должности, помогают определить кадровый состав учреждения и присвоить права доступа для последующей работы пользователей в Системе;

– Студенты, Сотрудники, Абитуриенты. Данная информация помогает в последующем вести учет пользователей, управлять группами обучения, учебными отделениями, рабочими программами дисциплин, расписаниями занятий и сессий, журналами успеваемости, сведениями промежуточной и итоговой аттестации, осуществлять контроль документооборота в части касающейся приказов и составлять отчеты.

3) Обучение.

После формирования пользователей Системы следует создать учебный календарь, который необходим для организации и упорядочивания учебного процесса. Разработав учебный календарь, необходимо перейти к созданию справочника учебных дисциплин. Этот список является основой для формирования учебных планов, которые в свою очередь определяют состав учебных предметов, последовательность их изучения и общий объем отводимого на это времени.

Образовательная программа создается в виде справочника. Это форма, в которой перечисляются основные характеристики (специальность, форма обучения, база приёма, уровень подготовки, срок обучения и тип учебного периода). Сведения образовательной программы взаимоувязаны с пунктом меню Учебные группы.

Подраздел в пункте меню Образовательная программа является очередным шагом при работе с Системой.

4) Следующим шагом является формирование учебных групп.

Сведения из этого пункта меню взаимоувязаны с пунктами меню «Учебные отделения», «Перевод студентов», «Расписание занятий». Функциональными возможностями при создании групп обучения являются:

– Распределение пользователей (студентов или абитуриентов по группам);

– Управление подгруппами и назначение другого преподавателя;

– Управление дисциплинами (эта информация взаимоувязана с данными учебных планов образовательных программ);

– Редактирование журналов успеваемости и ведомостей промежуточной аттестации преподавателями-предметниками;

– Учебные отделения. Этот подпункт меню позволяет объединить группы обучения по признакам (например, очное, заочное или вечернее обучение), назначить куратора (Заведующего) по отделению.

5) Рабочие программы дисциплин разграничивают авторов, соавторов рабочей программы, а также преподавателей дисциплин, использующих данную рабочую программу. Они обуславливают заполнение пункта Тематическое планирование. Однако, заполнение КТП не обязательно в Системе.

6) Заключительным разделом при работе с Системой является меню Занятия.

Расписание звонков - это одно из мероприятий по регулированию образовательного процесса. В нем заполняются все поля (название, начало и окончание действия, начало занятий, длительность занятий и перемен, количество занятий);

Расписание занятий - это форма, способствующая оптимальной организации учебной работы и повышению эффективности преподавательской деятельности. Оно составляется в соответствии с учебным планом.

Расписание сессий - это форма, регулирующая период сдачи экзаменов в учебном заведении. Система позволяет создавать расписание консультаций, экзаменов, зачётов или пересдач.

Журнал успеваемости - это форма, способствующая ведению учета и анализа учебной деятельности, повышению уровня прозрачности учебного процесса. В ней реализованы возможности:

- отображение запланированных занятий по дисциплине;

- администрирование заданий для занятий;

- выставление оценок и посещаемости. Сведения по успеваемости учитываются в ведомости промежуточной аттестации.

После окончания каждого периода обучения в Системе необходимо проводить процедуру перевода учебных групп на следующий период обучения. Информация в этот пункт меню поступает из созданного ранее учебного календаря и сортируется по фазам обучения.

Управление приказами. Этот пункт меню позволяет просматривать все созданные приказы по пользователям Системы. Сведения поступают из меню Пользователи и с помощью удобно настроенных фильтров вы можете формировать запросы на просмотры необходимых документов.

Описание работы в меню «Пользователи», «Обучение», «Занятия» - это базисные процедуры.

7) Отчёты. В Системе имеются различные формы отчетов. Сведения, представленные в этих формах, резюмируют результаты учебной и преподавательской деятельности. При создании различных категорий отчётов используются инструменты (фильтры), благодаря которым отчёт становиться наглядным и способствует созданию мотивационных элементов, влияющих на образовательный процесс.

Чтобы войти в Систему, необходимо открыть браузер и набрать в адресной строке браузера **http://<имя_сервера>/**, где вместо <**имя_сервера>** введите адрес Системы. Для перехода нажмите на клавиатуре клавишу

«**Enter**». На открывшейся странице отображается экран входа в Систему (см. рисунок 3):

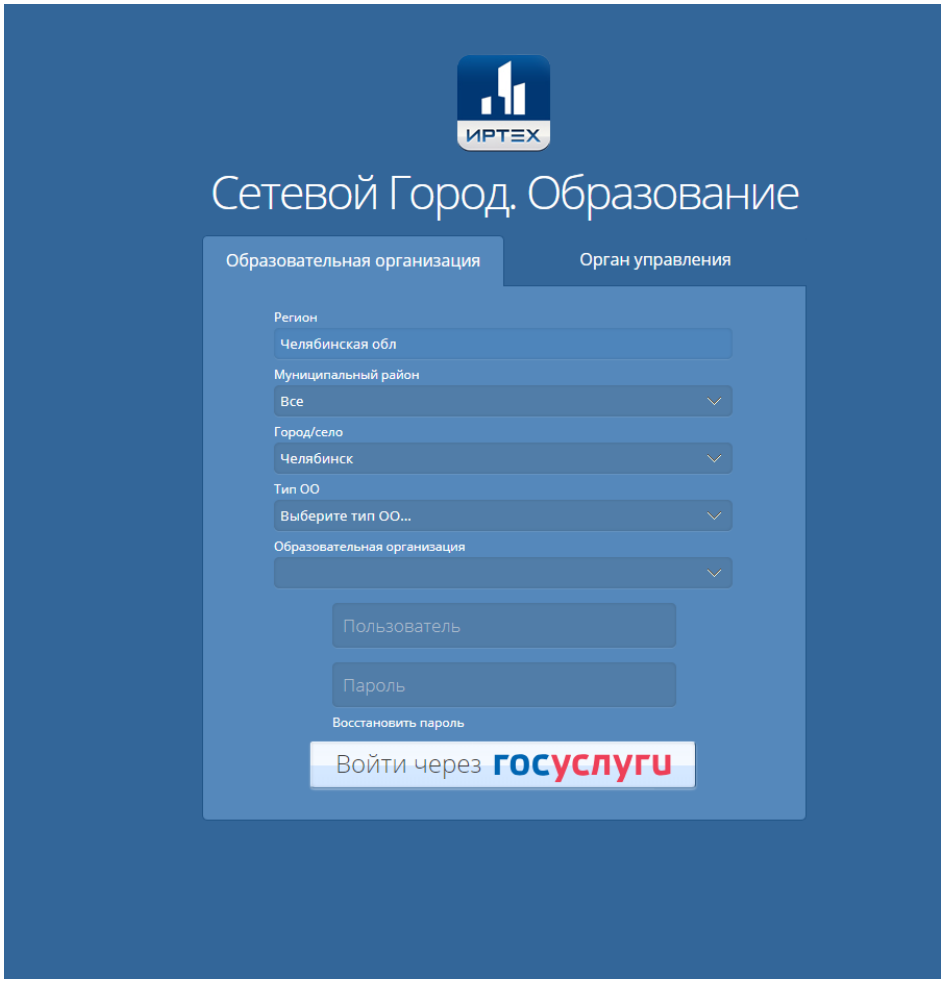

Рис. 3. - Вход в Систему

Для входа в Систему нужно ввести имя учётной записи (логин) и пароль и нажмите кнопку **«Войти»**.

После успешной авторизации открывается экран «**Главная стран**ица».

В Системе по умолчанию предусмотрены следующие роли: Абитуриент, Сотрудник, Студент, Родитель.

Для роли Сотрудник в Системе реализована возможность создания любых должностей с индивидуальным набором прав. В дальнейшем эти должности назначаются конкретным сотрудникам.

Помимо настраиваемой группы прав для роли Сотрудник предусмотрены определенные правила при работе с различными разделами

системы, если данный Сотрудник является преподавателем или куратором учебной группы.

Для регистрации пользователя в Системе необходимо выбрать раздел меню **«Пользователи»** и один из его пунктов: **«Абитуриенты»**, **«Студенты»** или **«Сотрудники»**.

При выборе пункта меню в рабочей области отображается список пользователей выбранной категории, справа от которой отображается блок **«Новый студент»** (**«Новый сотрудник»**) для создания нового пользователя в Системе.

Система позволяет создавать пользователя с ролью **«Родитель»**. Чтобы добавить родителя конкретному студенту, необходимо выбрать его в общем списке щелчком левой кнопки мыши и в личной карточке в блоке «Родители» нажать на кнопку «+». Для доступа в систему создается логин и пароль пользователя с ролью «Родитель» (пароль генерируется Системой автоматически) (рис. 4).

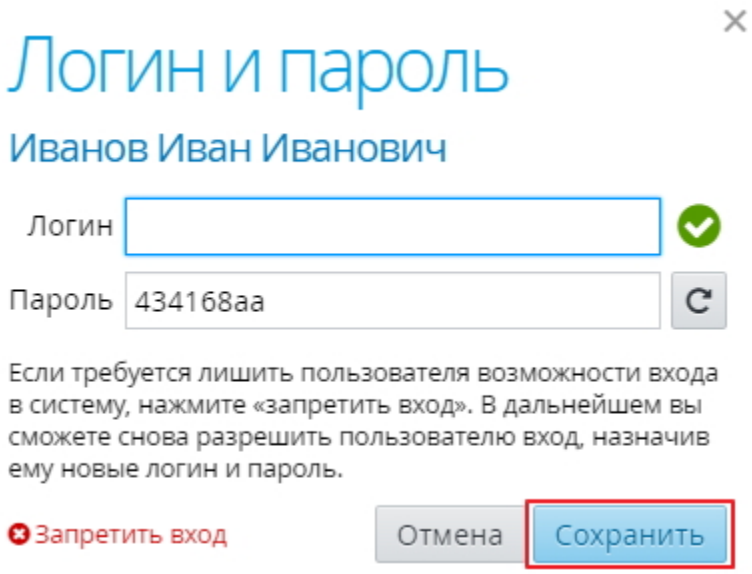

Рис. 4. - Создание доступа в Систему для пользователя с ролью родителя

Пароли не хранятся в Системе в явном виде, поэтому в случае утери пароля его нельзя где-либо увидеть, можно только изменить пароль на новый.

«Е-услуги. Образование» – автоматизированная информационная система (АИС), позволяющая реализовать на уровне региона (муниципального образования) следующие государственные и муниципальные услуги в электронном виде в сфере образования.

АИС «Е-услуги. Образование» интегрирована с системами:

- Единый портал государственных и муниципальных услуг (ЕПГУ);
- Единая система межведомственного электронного взаимодействия (СМЭВ);
- Единая система идентификации и аутентификации (ЕСИА);
- Концентратор услуг;
- АИС «Образование Челябинской области»;
- Федеральная система показателей Электронной очереди (ФСПЭО);
- Региональный сегмент Единой федеральной межведомственной системы учета контингента обучающихся.

В связи с тем, что в данных системах идет обработка персональных данных обучающихся (ФИО, данные свидетельства о рождении, паспорта, дата рождения, место рождения, адрес прописки и проживания, данные родителей) информация должна быть хорошо защищена.

Для этого те компьютеры, где происходит запись детей («Е-услуги. Образование») и выгрузка данных по обучающимся в АИС «Сетевой город. Образование» - должны быть аттестованы.

На них ставятся программные комлексы: VIP Net Client – создается защищенный канал связи. Также ставятся дополнительные средства защиты – программы: Dallas Lock 8.0-K и Kaspersky Endpoint Security 10.

Установка всех программ, разработка пакета документов на данное аттестованное место – ложится на плечи лицензиата ФСБ, лицензиата ФСТЭК. Управление образование Верхнеуфалейского городского округа работает с удостоверяющим центром ООО «ПНК» г. Челябинск на коммерческой основе.

К данным компьютерам допускается ограниченное количество пользователей, это учитывается и в приказах, и в журналах Управления образования Верхнеуфалейского городского округа.

Данные аттестованные места с СКЗИ ставятся в кабинетах, где дополнительно устанавливается сигнализация на разбив стекла и объемники (т.е. на несанкционированное перемещение после закрытия кабинета).

Кабинет после рабочего дня должен опечатываться: шток-чашка, пластилин, печать. Ключи от кабинета помещаются в пенал, пенал опечатывается и сдается на вахту. Ключи в пенале получают и вечером сдают, о чем делаются записи в соответствующем журнале.

Назначаются ответственные пользователи СКЗИ, пользователи СКЗИ и ИСПДн (информационных систем по обработке персональных данных), ответственные за опечатывание кабинета.

Описанные действия и меры прописаны в нормативных правовых актах Управления образования Верхнеуфалейского городского округа.

Выводы по Главе II

Во второй главе магистерской диссертации описана нормативно-правовое обеспечение и реализации программы АИС «Сетевой город. Образование» на примере муниципалитета Верхнеуфалейский городской округ.

Сетевой Город. Образование – комплексная автоматизированная информационная система, объединяющая в единую сеть образовательные учреждения и органы управления образования в пределах города, сельского или городского района (округа). Тем самым формируется единое информационное образовательное пространство муниципального образования**.**

В состав АИС «Образование» входит АИС «Сетевой город. Образование» – модульная комплексная информационная система, предназначенная для предоставления электронных средств поддержки и сопровождения образовательной деятельности образовательных организаций, реализации государственных и муниципальных услуг в электронном виде в сфере образования, а также являющаяся инструментом сетевого взаимодействия между всеми участниками образовательных отношений и интеграции в единую сеть образовательных организаций и органов управления образованием.

Модуль «Профессиональная образовательная организация» (АИС ПОО) предназначен образовательных организаций, осуществляющих образовательную деятельность по образовательным программам среднего профессионального образования и (или) по программам профессионального обучения.

Глава 3. Направления совершенствования информационной безопасности в организациях СПО в рамках реализации программы АИС «Сетевой город. Образование»

3.1 Описание объекта защиты

В качестве объекта защиты было выбран Верхнеуфалейский филиал государственного бюджетного профессионального образовательного учреждения «Каслинский промышленно-гуманитарный техникум».

Верхнеуфалейский филиал государственного бюджетного профессионального образовательного учреждения «Каслинский промышленно-гуманитарный техникум» является обособленным 2 подразделением ГБПОУ «Каслинский промышленно-гуманитарный техникум». Местонахождение филиала: 456800, Челябинская область, г. Верхний Уфалей, ул. Победы, 42.

Директором ГБПОУ «Каслинский промышленно-гуманитарный техникум» является Шебалин Александр Валентинович.

Руководитель Верхнеуфалейского филиала государственного бюджетного профессионального образовательного учреждения «Каслинский промышленно-гуманитарный техникум» – заместитель директора техникума по учебной работе – Ефанова Наталья Николаевна.

Основные задачи Филиала определяются в соответствии с законодательством Российской Федерации и реализуются в соответствии с Уставом Техникума, настоящим Положением в следующей деятельности:

- удовлетворение потребностей личности в получении среднего профессионального образования, и квалификации в соответствии с направлениями профессиональной подготовки в Техникуме, интеллектуальном, культурном, физическом и нравственном развитии;

- удовлетворение потребностей общества в профессионально подготовленных специалистах, создании новых рабочих мест;

- профессиональная переподготовка и повышение квалификации специалистов и рабочих;

- распространение знаний среди населения, повышение его общеобразовательного и культурного уровня, в том числе путем оказания платных образовательных услуг.

Непосредственное управление Филиалом осуществляют заместитель директора по учебной работе, назначаемый приказом директора техникума. Заместитель директора участвует в работе Совета Техникума в качестве его члена и является председателем педагогического Совета Филиала. Заместитель директора по Филиалу:

- по нотариальной доверенности действует от имени техникума, представляет его во всех учреждениях, предприятиях и организациях, независимо от их организационно-правовых форм собственности, в судах, представляет Филиал в отношениях с органами законодательной и исполнительной власти;

- обеспечивает системную образовательную (учебно-воспитательную, производственную) и административно-хозяйственную работу;

- решает учебно-методические, административные, финансовые, хозяйственные и иные вопросы;

- обеспечивает учет, сохранность и пополнение учебно-материальной базы, соблюдение правил санитарно-гигиенического режима и охраны труда, учет и хранение документации;

- по согласованию с директором техникума осуществляет приносящую доход деятельность, используя имущество Филиала;

- планирует, координирует и контролирует работу педагогических и других работников Филиала;

- издает распоряжения и дает указания, обязательные для всех работников Филиала;

- готовит проекты приказов по заработной плате, стимулирующим выплатам сотрудникам, материальным выплатам обучающимся, проекты приказов по учебной работе;

- представляет директору Техникума сведения и материалы по приему и увольнению, поощрению и наказанию работников Филиала;

- осуществляет подбор и расстановку педагогических кадров и других сотрудников Филиала;

- создает условия для повышения их квалификации и совершенствования профессионального мастерства;

- поощряет и стимулирует творческую инициативу работников, поддерживает благоприятный морально-психологический климат в коллективе;

- формирует контингент учащихся, обеспечивает их социальную защиту;

- обеспечивает учет, сохранность имущества и учебно-материальной базы Филиала, соблюдение правил санитарно-гигиенического режима и охраны труда, учет и хранение документации;

- представляет отчеты о деятельности Филиала в техникум;

- готовит гражданам архивные справки, обучающимся справки об учебе и материальных выплатах.

Филиал реализуют образовательные программы среднего профессионального образования и профессиональной подготовки в полном объеме по дневной, очно-заочной (вечерней) и заочной формам обучения, а также дополнительные образовательные услуги согласно лицензии.

В своей образовательной деятельности Филиал используют наиболее эффективные технологии обучения и воспитательные системы.

Доступ педагогических работников к информационно-телекоммуникационной сети Интернет в Техникуме осуществляется с персональных компьютеров (ноутбуков и т.п.), подключенных к сети Интернет, без ограничения времени и потребленного трафика.

Для доступа к информационно-телекоммуникационным сетям в Техникуме педагогическому работнику предоставляются

идентификационные данные (логин и пароль). Предоставление доступа осуществляется системным администратором Техникума

Педагогическим работникам обеспечивается доступ к следующим электронным базам данных: АСУ; информационные справочные системы; поисковые системы.

Доступ к электронным базам данных осуществляется на условиях, указанных в договорах, заключенных Техникумом с правообладателем электронных ресурсов (внешние базы данных).

Информация об образовательных, методических, научных, нормативных и других электронных ресурсах, доступных к пользованию, размещена на сайте Техникума.

В колледже на настоящий момент действует АСУ «ProCollege» созданная для системы среднего профессионального образования. АСУ «ProCollege» обеспечивает:

– информационное сопровождение деятельности приемной комиссии;

– учет контингента и ведение личных дел студентов;

– электронный документооборот (маршрутизация, контроль) на всех уровнях;

– ведение электронных журналов в любой системе оценивания и др.

Проведя анализ сферы деятельности и основных понятий ФЗ «О персональных данных», можно сделать вывод, что все образовательные организации являются операторами персональных данных, так как совершают обработку персональных данных в рамках собственных ИСПДн.

В техникуме используется информационная система персональных данных ИСПДн «Граждане». Цель данной системы предоставление социальных услуг.

По структуре ИСПДн представляет собой локальную информационную систему - комплекс АРМ, объединенных без использования технологии удаленного доступа. В ИСПДн режим обработки ПДн многопользовательский с равными правами доступа пользователей.

ИСПДн состоит из одного АРМ. На ПЭВМ пользователями осуществляется обработка персональных данных граждан, обратившихся в техникум. ИСПДн подключена к сетям связи общего пользования через сертифицированный межсетевой экран.

Пользователями ИСПДн являются работники техникума, которым в соответствии с трудовыми обязанностями необходимо осуществлять обработку персональных данных. Пользователи имеют равные права доступа к ресурсам ИСПДн.

С учетом обрабатываемых категорий персональных данных и прочих характеристик, ИСПДн «Граждане» является информационной системой, для которой нарушение заданной характеристики безопасности ПДн, обрабатываемых в них, может привести к негативным последствиям для субъектов персональных данных.

Таким образом, техникум является объектом информатизации, который должен соответствовать аттестации объекта информатизации информационных систем в соответствии с Федеральным законом № 149-ФЗ от 21 июля 2006 года «Об информации, информационных технологиях и о защите информации», Федеральным законом № 152-ФЗ от 27 июля 2006 года «О персональных данных», Специальными требованиями и рекомендациями по технической защите конфиденциальной информации (Решение Гостехкомиссии России от 23.05.1997 №55), Положением по аттестации объектов информатизации на соответствие требованиям безопасности информации (Гостехкомиссия России, 25.11.1994), Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (Приказ ФСТЭК России от 18 февраля 2013 г. № 21), а также другими действующими нормативно-методическими документами ФСТЭК России.

Аттестационные испытания проводятся 1 раз в 3 года на соответствие положениям и требованиям действующих нормативных правовых актов,

методических документов и национальных стандартов в области защиты информации (перечень документов приводится в Приложении 1).

Аттестационные испытания проводятся в указанном ниже порядке и включают:

1. анализ полноты исходных данных, проверку их соответствия реальным условиям размещения, монтажа и эксплуатации ИСПДн;

2. исследование технологического процесса обработки, хранения и передачи информации, анализ информационных потоков;

3. оценку полноты разработки организационно-распорядительной, проектной и эксплуатационной документации. Проверку соответствия их содержания установленным требованиям;

4. определение состава использованных для обработки, хранения и передачи информации ОТСС;

5. оценку правильности установки уровня защищенности персональных данных при их обработке в ИСПДн;

6. проверку выполнения требований безопасности информации к помещению, в котором проводится обработка информации;

7. проверку ИСПДн на соответствие требованиям по защите информации от несанкционированного доступа;

8. подготовку отчетной документации.

В результате аттестационных испытаний на соответствие требованиям безопасности информации объекта информатизации определяется состояние безопасности и уязвимости существующей системы защиты информации в техникуме.

В случае выявления по результатам испытаний несоответствия объекта информатизации установленным требования по защите информации комиссия может рассмотреть возможность оперативного устранения выявленных недостатков и нарушений. При этом могут рекомендоваться следующие меры:

- доработка организационно-распорядительной документации;

- применение дополнительных организационных и технических мер защиты;

- применение дополнительных сертифицированных средств защиты информации.

3.2 Оценка исходной защищенности ИСПДн в Верхнеуфалейском филиале ГБПОУ «Каслинский промышленно-гуманитарный техникум»

В целях обеспечения информационной безопасности и ее организации, на основании законодательных документов, в образовательной организации следует разрабатывать соответствующие нормативно-правовые акты.

Правовые нормы обеспечения информационной безопасности в конкретной образовательной организации фиксируются в учредительных, организационных и функциональных документах.

Требования обеспечения информационной безопасности отражаются в уставе (учредительном договоре) в виде следующих положений:

– образовательная организация имеет право определять состав, объем и порядок защиты сведений конфиденциального характера, персональных данных обучающихся, работников ОО, требовать от своих сотрудников обеспечения сохранности и защиты этих сведений от внешних и внутренних угроз;

– образовательная организация обязана обеспечить сохранность конфиденциальной информации.

К организационным и функциональным документам следует отнести:

– приказ руководителя образовательной организации о назначении ответственного за обеспечение информационной безопасности;

– должностные обязанности ответственного за обеспечение информационной безопасности;

– перечень защищаемых информационных ресурсов и баз данных;

– инструкцию, определяющую порядок предоставления информации сторонним организациям по их запросам, а также по правам доступа к ней сотрудников ОО.

Кроме того, должен быть определен порядок допуска сотрудников ОО к информации. Такой допуск предусматривает:

– принятие работником обязательств о неразглашении доверенных ему сведений конфиденциального характера;

– ознакомление работника с нормами законодательства РФ и ОО об информационной безопасности и ответственности за разглашение информации конфиденциального характера;

– инструктаж работника специалистом по информационной безопасности;

– контроль работника ответственным за информационную безопасность при работе с информацией конфиденциального характера.

Как показала практика, при проверке организации системы информационной безопасности, как правило, отмечаются следующие недостатки:

– отсутствует перечень сведений, составляющий конфиденциальную информацию;

– отсутствуют должностные обязанности ответственного за информационную безопасность;

– не соблюдается порядок учета носителей информации конфиденциального характера;

– нарушен порядок делопроизводства.

Таким образом, обеспечение информационной безопасности образовательной организации в современных условиях становится одним из основных видов его деятельности. Без использования новых подходов, поиска современных форм и способов обеспечения безопасности образовательной организации решить эти задачи невозможно.

Система защиты персональных данных включает в себя:

- организационные

- и (или) технические меры, определенные с учетом актуальных угроз безопасности ПДн.

Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы.

Согласно методике определения актуальных угроз, угроза имеет среднюю опасность, если реализация угрозы может привести к негативным последствиям для субъектов персональных данных.

Общее определение угрозы безопасности объекта – возможное нарушение характеристики безопасности объекта.

Определение угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Рассмотрим более подробно меры информационной безопасности, необходимые для реализации программы АИС «Сетевой город. Образование» в образовательной организации.

Меры по обеспечению безопасности персональных данных реализуются в рамках системы защиты персональных данных, создаваемой в соответствии с требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119, и должны быть направлены на нейтрализацию актуальных угроз безопасности персональных данных.

Меры по обеспечению безопасности персональных данных реализуются в том числе посредством применения в информационной

системе средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия, в случаях, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности персональных данных.

Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных проводится оператором самостоятельно или с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанная оценка проводится не реже одного раза в 3 года.

В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

– идентификация и аутентификация субъектов доступа и объектов доступа;

– управление доступом субъектов доступа к объектам доступа; ограничение программной среды;

– защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);

– регистрация событий безопасности;

– антивирусная защита;

– обнаружение (предотвращение) вторжений;

– контроль (анализ) защищенности персональных данных;

– обеспечение целостности информационной системы и персональных данных;

– обеспечение доступности персональных данных;

– защита среды виртуализации;

– защита технических средств;

– защита информационной системы, ее средств, систем связи и передачи данных;

– выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;

– управление конфигурацией информационной системы и системы защиты персональных данных.

Состав и содержание мер по обеспечению безопасности персональных данных, необходимых для обеспечения каждого из уровней защищенности персональных данных, приведены в таблице 1.

Таблица 1

Состав и содержание мер по обеспечению безопасности персональных данных, необходимых для обеспечения каждого из уровней защищенности персональных данных

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности персональных данных			
		4	3	2	1
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)					
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+	+	+	+
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных			+	+
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+	+	+	+
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	+	+	+	+
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	+	+	+	+
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	+	+	+	+
II. Управление доступом субъектов доступа к объектам доступа (УПД)					

УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	+	+	+	+
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	+	+	+	+
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами	+	+	+	+
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	+	+	+	+
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	+	+	+	+
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	+	+	+	+
УПД.7	Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры по обеспечению безопасности персональных данных, и о необходимости соблюдения установленных оператором правил обработки персональных данных				
УПД.8	Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему				
УПД.9	Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы				
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу		+	+	+
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации		+	+	+
УПД.12	Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки				
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	+	+	+	+
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа	+	+	+	+
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств	+	+	+	+

УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	+	+	+	+
УПД.17	Обеспечение доверенной загрузки средств вычислительной техники			+	+
	III. Ограничение программной среды (ОПС)				
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения				
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения			+	+
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов				+
ОПС.4	Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов				
	IV. Защита машинных носителей персональных данных (ЗНИ)				
ЗНИ.1	Учет машинных носителей персональных данных			+	+
ЗНИ. 2	Управление доступом к машинным носителям персональных данных			+	+
ЗНИ.3	Контроль перемещения машинных носителей персональных данных за пределы контролируемой зоны				
ЗНИ.4	Исключение возможности несанкционированного ознакомления с содержанием персональных данных,хранящихся на машинных носителях, и (или) использования носителей персональных данных в иных информационных системах				
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители персональных данных				
ЗНИ.6	Контроль ввода (вывода) информации на машинные носители персональных данных				
ЗНИ.7	Контроль подключения машинных носителей персональных данных				
ЗНИ.8	Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания		+	+	+
	V. Регистрация событий безопасности (РСБ)				
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	+	+	+	+
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	+	+	+	+

РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	+	+	+	+
РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти				
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них			+	+
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе				
РСБ. 7	Защита информации о событиях безопасности	+	+	+	+
VI. Антивирусная защита (АВЗ)					
АВЗ.1	Реализация антивирусной защиты	+	+	+	+
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	+	+	+	+
VII. Обнаружение вторжений (СОВ)					
СОВ.l	Обнаружение вторжений			+	+
СОВ.2	Обновление базы решающих правил			+	+
VIII. Контроль (анализ) защищенности персональных данных (АНЗ)					
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей		+	+	+
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	+	+	+	+
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации		+	+	+
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации		+	+	+
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе			+	+
IX. Обеспечение целостности информационной системы и персональных данных (ОЦЛ)					
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации			+	+
ОЦЛ.2	Контроль целостности персональных данных, содержащихся в базах данных информационной системы				
ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций				
ОЦЛ.4	Обнаружение и реагирование на поступление в			+	+

	информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама)				
ОЦЛ. 5	Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и (или) контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов),методов), и исключение неправомерной передачи информации из информационной системы				
ОЦЛ.6	Ограничение прав пользователей по вводу информации в информационную систему				
ОЦЛ.7	Контроль точности, полноты и правильности данных, вводимых в информационную систему				
ОЦЛ.8	Контроль ошибочных действий пользователей по вводу и (или) передаче персональных данных и предупреждение пользователей об ошибочных действиях				
X. Обеспечение доступности персональных данных (ОДТ)					
ОДТ.1	Использование отказоустойчивых технических средств				
ОДТ.2	Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы				
ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование				+
ОДТ.4	Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных			+	+
ОДТ. 5	Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала			+	+
XI. Защита среды виртуализации (ЗСВ)					
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	+	+	+	+
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	+	+	+	+
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре		+	+	+
ЗСВ.4	Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры				

ЗСВ.5	Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией				
ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных			+	+
ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций			+	+
ЗСВ. 8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры			+	+
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре		+	+	+
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей		+	+	+
XII. Защита технических средств (ЗТС)					
ЗТС.1	Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам				
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования				
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены	+	+	+	+
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	+	+	+	+
ЗТС.5	Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов)				
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)					
ЗИС.1	Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты персональных данных, функций по обработке персональных данных и иных функций информационной системы				+
ЗИС.2	Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со				

	стороны процессов с низким приоритетом				
ЗИС.3	Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи	+	+	+	+
ЗИС.4	Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации)				
ЗИС. 5	Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств				
ЗИС.6	Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с персональными данными, при обмене ими с иными информационными системами				
ЗИС. 7	Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода				
ЗИС. 8	Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи				
ЗИС.9	Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации				
ЗИС.10	Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам				
ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов			+	+
ЗИС.12	Исключение возможности отрицания пользователем факта отправки персональных данных другому пользователю				
ЗИС.13	Исключение возможности отрицания пользователем факта получения персональных данных от другого пользователя				
ЗИС.14	Использование устройств терминального доступа для				

	обработки персональных данных				
ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных			+	+
ЗИС.16	Выявление, анализ и блокирование в информационной системы скрытых каналов передачи информации в обход реализованных мер или внутри разрешенных сетевых протоколов				
ЗИС.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы			+	+
ЗИС.18	Обеспечение загрузки и исполнения программного обеспечения с машинных носителей персональных данных, доступных только для чтения, и контроль целостности данного программного обеспечения				
ЗИС.19	Изоляция процессов (выполнение программ) в выделенной области памяти				
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе		+	+	+
XIV. Выявление инцидентов и реагирование на них (ИНЦ)					
ИНЦ.1	Определение лиц, ответственных за выявление инцидентов и реагирование на них			+	+
ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов			+	+
ИНЦ.3	Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами			+	+
ИНЦ.4	Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий			+	+
ИНЦ. 5	Принятие мер по устранению последствий инцидентов			+	+
ИНЦ. 6	Планирование и принятие мер по предотвращению повторного возникновения инцидентов			+	+
XV. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)					
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных		+	+	+
УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты персональных данных		+	+	+
УКФ.3	Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации		+	+	+

	информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных				
УКФ.4	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных		+	+	+

«+» - мера по обеспечению безопасности персональных данных включена в базовый набор мер для соответствующего уровня защищенности персональных данных.

Меры по обеспечению безопасности персональных данных, не обозначенные знаком «+», применяются при адаптации базового набора мер и уточнении адаптированного базового набора мер, а также при разработке компенсирующих мер по обеспечению безопасности персональных данных.

При невозможности технической реализации отдельных выбранных мер по обеспечению безопасности персональных данных, а также с учетом экономической целесообразности на этапах адаптации базового набора мер и (или) уточнения адаптированного базового набора мер могут разрабатываться иные (компенсирующие) меры, направленные на нейтрализацию актуальных угроз безопасности персональных данных.

В случае определения в соответствии с требованиями к защите персональных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119, в качестве актуальных угроз безопасности персональных данных 1-го и 2-го типов дополнительно к мерам по обеспечению безопасности персональных данных, могут применяться следующие меры:

– проверка системного и (или) прикладного программного обеспечения, включая программный код, на отсутствие недекларированных возможностей с использованием автоматизированных средств и (или) без использования таковых;

– тестирование информационной системы на проникновения;

– использование в информационной системе системного и (или) прикладного программного обеспечения, разработанного с использованием методов защищенного программирования.

Технические меры защиты персональных данных реализуются посредством применения средств защиты информации, в том числе программных (программно-аппаратных) средств, в которых они реализованы, имеющих необходимые функции безопасности.

При использовании в информационных системах, сертифицированных по требованиям безопасности информации средств защиты информации:

– в информационных системах 1 уровня защищенности персональных данных применяются средства защиты информации не ниже 4 класса, а также средства вычислительной техники не ниже 5 класса;

– в информационных системах 2 уровня защищенности персональных данных применяются средства защиты информации не ниже 5 класса, а также средства вычислительной техники не ниже 5 класса;

– в информационных системах 3 уровня защищенности персональных данных применяются средства защиты информации не ниже 6 класса, а также средства вычислительной техники не ниже 5 класса;

– в информационных системах 4 уровня защищенности персональных данных применяются средства защиты информации не ниже 6 класса, а также средства вычислительной техники не ниже 6 класса.

Для обеспечения 1 и 2 уровней защищенности персональных данных, а также для обеспечения 3 уровня защищенности персональных данных в информационных системах, для которых к актуальным отнесены угрозы 2-го типа, применяются сертифицированные средства защиты информации, программное обеспечение которых прошло проверку не ниже чем по 4 уровню контроля отсутствия недекларированных возможностей. (п. 12 в ред. Приказа ФСТЭК России от 23.03.2017 N 49)

При использовании в информационных системах новых информационных технологий и выявлении дополнительных угроз

безопасности персональных данных, для которых не определены меры обеспечения их безопасности, должны разрабатываться компенсирующие меры, направленные на нейтрализацию актуальных угроз безопасности персональных данных.

Угрозы безопасности персональных данных - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Угроза может привести к утечке (уничтожению, модификации), а может и нет. Наличие угрозы свидетельствует лишь о наличии возможности несанкционированного доступа к данным.

Методика определения актуальных угроз

Актуальной считается угроза, которая может быть реализована в ИСПДн и представляет опасность для ПДн. Подход к составлению перечня актуальных угроз состоит в следующем.

Для оценки возможности реализации угрозы применяются два показателя: уровень исходной защищенности ИСПДн и частота (вероятность) реализации рассматриваемой угрозы.

Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн.

Исходная степень защищенности определяется следующим образом.

1. ИСПДн имеет высокий уровень исходной защищенности, если не менее 70% характеристик ИСПДн соответствуют уровню «высокий» (суммируются положительные решения по первому столбцу, соответствующему высокому уровню защищенности), а остальные – среднему уровню защищенности (положительные решения по второму столбцу).

2. ИСПДн имеет средний уровень исходной защищенности, если не выполняются условия по пункту 1 и не менее 70% характеристик ИСПДн соответствуют уровню не ниже «средний» (берется отношение суммы положительные решений по второму столбцу, соответствующему среднему уровню защищенности, к общему количеству решений), а остальные – низкому уровню защищенности.

3. ИСПДн имеет низкую степень исходной защищенности, если не выполняются условия по пунктам 1 и 2.

При составлении перечня актуальных угроз безопасности ПДн каждой степени исходной защищенности ставится в соответствие числовой коэффициент, а именно:

0 – для высокой степени исходной защищенности;

5 – для средней степени исходной защищенности;

10 – для низкой степени исходной защищенности.

Выбор средств защиты информации для системы защиты персональных данных осуществляется оператором в соответствии с нормативными правовыми актами**,** принятыми ФСБ России и ФСТЭК России.

Проведем оценку исходной защищенности ИСПДн и АИС для Верхнеуральского филиала ГБПОУ «Каслинский промышленно-гуманитарный техникум».

В таблице 2 представлен перечень автоматизированных информационных систем и ИСПДн техникума.

Таблица 2

Перечень ИСПДН и АИС, обрабатывающих КИ, КТ и ПДн в техникуме

№ п/п	**Наименование информационной системы**	**Описание информационной системы**	**Перечень содержания информационной системы**
1	АСУ «ProCollege»	Программный продукт представляет собой комплексное решение для управления деятельностью учреждений начального и	- Паспортные данные студента - Паспортные данные родителей (родственников) студента

		среднего профессионального образования и охватывает все уровни управленческой деятельности основных подразделений колледжа.	- СНИЛС студента - СНИЛС (родственников) студента - Данные аттестата студента - Контактный телефон - Электронная почта - Достижения - Группы здоровья - Специальность - Приказы о зачислении, отчислении, академических отпусках - Паспортные данные, СНИЛС, ИНН, контактный телефон, стаж работы сотрудников образовательной организации - Образовательные программы, рабочие программы, КТП, расписание занятий, успеваемость студентов
2	Региональная АИС «Сетевой город. Образование»	Автоматизированная информационная система «Сетевой Город. Образование», модуль «Профессиональная образовательная организация Модуль для профессиональных образовательных организаций АИС ПОО позволяет решать административные задачи профессиональных образовательных организаций и проводить мониторинг текущего учебного процесса.	- Паспортные данные студента - Паспортные данные родителей студента - СНИЛС студента - СНИЛС (родственников) студента - Данные аттестата - Контактный телефон - Электронная почта - Достижения - Группы здоровья - Специальность - Приказы о зачислении, отчислении, академических отпусках - Паспортные данные, СНИЛС, ИНН, телефон, стаж работы сотрудников ОО - Образовательные программы, рабочие программы, КТП, расписание занятий, успеваемость студентов
3	ИСПДн «Граждане»	Системы предоставление социальных услуг	- Паспортные данные студента - Паспортные данные

			родителей (родственников) студента - СНИЛС студента - СНИЛС (родственников) студента - Контактный телефон - Электронная почта - Паспортные данные, СНИЛС, ИНН, контактный телефон сотрудников образовательной организации

В таблице 3 представлены показатели исходной защищенности ИСПДн и АИС в техникуме.

Таблица 3

Показатели исходной защищенности ИСПДн и АИС

Технические и эксплуатационные характеристики	Уровень защищенности		
	Высокий	Средний	Низкий
1. По территориальному размещению:			
распределенная, которая охватывает несколько областей, краев, округов или государство в целом;	–	–	+
городская, охватывающая не более одного населенного пункта (города, поселка);	–	–	+
корпоративная распределенная, охватывающая многие подразделения одной организации;	–	+	–
локальная (кампусная), развернутая в пределах нескольких близко расположенных зданий;	–	+	–
локальная, развернутая в пределах одного здания	+	–	–
2. По наличию соединения с сетями общего пользования:			
ИСПДн, имеющая многоточечный выход в сеть общего пользования;	–	–	+
ИСПДн, имеющая одноточечный выход в сеть общего пользования;	–	+	–
ИСПДн, физически отделенная от сети общего пользования	+	–	–
3. По встроенным (легальным) операциям с записями баз персональных данных:			
чтение, поиск;	+	–	–
запись, удаление, сортировка;	–	+	–
модификация, передача	–	–	+
4.По разграничению доступа к персональным данным:			
ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся	–	+	–

Технические и эксплуатационные характеристики	Уровень защищенности		
	Высокий	Средний	Низкий
владельцем ИСПДн, либо субъект ПДн;			
ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн;	–	–	+
ИСПДн с открытым доступом	–	–	+
5. По наличию соединений с другими базами ПДн иных ИСПДн*:*			
интегрированная ИСПДн (организация использует несколько баз ПДн, при этом организация не является владельцем всех используемых баз ПДн);	–	–	+
ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн	+	–	–
6. По уровню обобщения (обезличивания) ПДн:			
ИСПДн, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.);	+	–	–
ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;	–	+	–
ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)	–	–	+
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки:			
ИСПДн, предоставляющая всю базу данных с ПДн;	–	–	+
ИСПДн, предоставляющая часть ПДн;	–	+	–
ИСПДн, не предоставляющая никакой информации.	+	–	–

Исходя из таблицы АИС «Сетевой город. Образование» имеет низкую степень исходной защищенности, так как не выполняются условия по пунктам 1 и 2.

3.3 Программа совершенствования информационной безопасности в Верхнеуфалейском филиале ГБПОУ «Каслинский промышленно-гуманитарный техникум». Задачи службы информационной безопасности

На основе проведенной оценки исходной защищенности ИСПДн и анализа нормативно-правовых требований действующего законодательства нами была разработана Программа совершенствования ИБ в ГБПОУ «Каслинский промышленно-гуманитарный техникум».

Программа совершенствования ИБ в ГБПОУ «Каслинский промышленно-гуманитарный техникум» состоит из 4 этапов.

Этап 1. Разработка организационно-распорядительных и технических документов по защите персональных данных.

1. Алгоритм по применению комплекта документов по защите персональных данных в образовательной организации.
2. Акт классификации информационной системы персональных данных.
3. Акт об уничтожении бумажных носителей персональных данных субъектов персональных данных.
4. Акт об уничтожении электронных носителей персональных данных субъектов персональных данных.
5. Акт присвоения уровня защищенности информационной системы персональных данных.
6. Журнал учета паролей пользователей информационной системы персональных данных.
7. Журнал учета машинных носителей информации.
8. Журнал учета средств защиты информации, эксплуатационной и технической документации к ним.
9. Журнал учёта ключей от сейфов и помещений.
10. Журнал учета обращений субъектов информационной системы персональных данных.

11. Журнал учета проверок юридического лица.

12. Журнал учета работ в информационной системе персональных данных.

13. Инструкция администратора безопасности информационной системы персональных данных.

14. Инструкция о порядке работы с персональными данными.

15. Инструкция ответственного за организацию обработки персональных данных.

16. Инструкция по организации антивирусной защиты.

17. Инструкция по организации парольной защиты.

18. Инструкция по физической охране, контролю доступа в помещения.

19. Инструкция пользователя информационной системы персональных данных.

20. Обязательство о неразглашении конфиденциальной информации.

21. Перечень сведений, содержащих персональные данные.

22. Перечень информационных систем персональных данных.

23. Перечень автоматизированных рабочих мест.

24. Перечень общесистемного и прикладного программного обеспечения, используемого в информационной системе персональных данных.

25. Перечень серверного коммутационного и сетевого оборудования.

26. План внутренних проверок состояния защиты информационных систем персональных данных.

27. План мероприятий по защите персональных данных.

28. Политика обработки и защиты персональных данных.

29. Положение об обработке персональных данных с использованием средств автоматизации.

30. Положение об обработке персональных данных без использования средств автоматизации.

31. Правила работы с обезличенными данными.

32. Приказ о введении в действие организационно-распорядительных документов по защите персональных данных.

33. Приказ об организации работ по обеспечению безопасности персональных данных.

34. Приказ об утверждении мест хранения материальных носителей персональных данных.

35. Приказ об утверждении списка должностных лиц, которым необходим доступ к персональным данным, обрабатываемым в информационной системе.

36. Регламент резервного копирования и восстановления данных.

37. Согласия субъектов на обработку персональных данных (Сотрудник. Кандидат на вакансию. Бывший сотрудник учреждения, Гражданин, Клиент и др.).

38. Список лиц, доступ которых к персональным данным необходим для выполнения служебных (трудовых) обязанностей.

39. Список мест хранения материальных носителей персональных данных.

40. Оценка вреда субъектам ПДн ИСПДн (Акт).

41. Описание технологического процесса обработки персональных данных.

42. Справка по информационным системам персональных данных.

43. Схема внешних и внутренних потоков передачи персональных данных.

44. Справка по трансграничной передаче персональных данных.

45. Уведомление об обработке (о намерении осуществлять обработку) персональных данных. (Информационное письмо).

Этап 2. Повышение осведомленности/ознакомление работников в области персональных данных.

1. Обучение руководителей организации (ответственных за организацию работы с персональными данными).

2. Ознакомление работников, непосредственно осуществляющих обработку персональных данных.

Для обучения сотрудников техникума по организации работы с персональными данными разработано электронное учебно-методическое обеспечение (Приложение 1). Электронное учебно-методическое обеспечение содержит нормативные документы, примеры журналов для работы с ПДн, пакет документов по СКЗИ, пакета документов на аттестацию рабочего места, теоретический материал по организации защиты персональных данных.

Этап 3. Установка и настройка технических средств защиты информации

Техническая защита системы персональных данных осуществляется и заключается:

1.Закупить и установить средства защиты информации, сертифицированных ФСТЭК России и ФСБ России.

2.Обучить ответственного за обработку и защиту персональных данных в техникуме, обучить пользователей СКЗИ.

3.Разработать эксплуатационную документацию на технические средства защиты персональных данных.

К основным средствам защиты персональных данных относится:

– Средство защиты информации от несанкционированного доступа.

– Антивирусное средство защиты.

– Межсетевой экран (защита от сетевых угроз).

– Средство шифрования информации (криптографические).

– Сетевые сканеры безопасности (контроль и анализ уязвимостей).

– Система обнаружения вторжений (обнаружение компьютерных атак).

Средства защиты от несанкционированного доступа (НСД) обеспечивают защиту информации, хранимой и обрабатываемой на персональных компьютерах, рабочих станциях и серверах.

Основная задача средств защиты от НСД - идентификация и аутентификация пользователей, позволяющая регламентировать доступ к защищаемым информационным ресурсам.

Используемые средства защиты от НСД:

Программные:

– Secret Net 8 (« 9100 руб.) + межсетевой экран;

– Dallas Lock 8.0-К (= 4500 руб.) + межсетевой экран.

Программно-аппаратные (модули доверенной загрузки):

– ПАК СЗИ НСД «Аккорд-АМДЗ»;

– ПАК «Соболь»;

– плата «Secret Net Card».

Антивирусные средства защиты - это комплексы приложений для борьбы с вирусами и вредоносными программами.

Используемые сертифицированные антивирусные средства защиты:

– Kaspersky Endpoint Security для бизнеса

– Security Studio Endpoint Protection

– Dr.Web Enterprise Security Suite 6.0 (6500 на 5 компьютеров).

Требования к Исполнителю работ по защите информации:

– Лицензия ФСТЭК России на деятельность потехнической защите конфиденциальной информации.

– Лицензия ФСБ России на деятельность в отношении шифровальных (криптографических) средств.

Рекомендации при выборе Исполнителя:

– Опыт.

– Наличие сертификатов.

– Возможность получения консультаций (тех. поддержка).

Этап 4. Аттестация информационных систем персональных данных

Проведение аттестационных испытании

Оформление Протокола, Заключения и Выдача «Аттестата соответствия».

Расчет стоимости *Защиты ПДн техникума + Аттестация ИСПДн* представлена в таблице 4.

Таблица 4

Расчет стоимости Защиты ПДн техникума + Аттестация ИСПДн

	Наименование товаров и услуг	Цена, руб.	Количество	Стоимость, руб.
I	ОБСЛЕДОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ			
1.1	Проведение обследования (аудит документов, интервью сотрудников, обследование помещений, сети и компьютеров	4 000	1	4 000
1.2	Разработка Частной модели угроз (Граждане)	5 450	1	5 450
1.3	Разработка Частного технического задания (Граждане)	4 450	1	4 450
1.4	Подготовка Уведомления в Управление Роскомнадзора	1 500	1	1 500
II	РАЗБОТКА ОРГАНИЗАЦИОННО-РАСПОРЯДИТЕЛЬНЫХДОКУМЕНТОВ			
2.1	Пакет организационно - распорядительных и эксплуатационных документов по обработке и защите персональных данных учреждения		1	15 000
III	ОБУЧЕНИЕ			бесплатно
IV	ВНЕДРЕНИЕ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ			**30 400**
1.	Средства защиты информации			
3.1	СКЗИ программного комплекса ViPNet Client 4 + **межсетевой экран** Dallas Lock 8.0-К	11 500	5	57 500
3.3	Сертифицированный антивирус Kaspersky		5	1 100
2.	Установка и настройка средств защиты информации			
3.4	Конфигурирование Средств защиты информации	2 500	5	12 500
V	АТТЕСТАЦИЯ ИНФОРМАЦИОННОМ СИСТЕМЫ			
4.1	Организационно-технические мероприятия по проверке соответствия требованиям по безопасности информации с выдачей «***Аттестата соответствия***»	4 990	2	9 800
				80 900

В случае выявления нарушений в области обработки и обеспечения безопасности ПДн, предусмотрена уголовная, административная, дисциплинарная и гражданская ответственность (таблица 5), которая может

применяться в отношении организации, руководителя организации, подразделения или виновного работника.

Таблица 5

Нарушения в области обработки и обеспечения безопасности ПДн

Уголовная ответственность	
Статья 137 УК РФ	Нарушение неприкосновенности частной жизни
Статья 140 УК РФ	Отказ в предоставлении гражданину информации
Статья 272 УК РФ	Неправомерный доступ к компьютерной информации
наказываются штрафом, обязательными работами, исправительными работами, принудительными работами, лишением права занимать определенные должности или заниматься определенной деятельностью, арестом, лишением свободы.	
Административная ответственность	
Статья 5.39 КоАП	Отказ в предоставлении информации
Статья 13.11 КоАП	Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)
Статья 13.12 КоАП	Нарушение правил защиты информации
Статья 13.13 КоАП	Незаконная деятельность в области защиты информации
Статья 13.14 КоАП	Разглашение информации с ограниченным доступом
Статья 19.4 КоАП	Неповиновение законному распоряжению должностного лица органа, осуществляющего надзор (контроль)
Статья 19.4.1 КоАП	Воспрепятствование законной деятельности должностного лица органа государственного контроля (надзора), органа муниципального контроля
Статья 19.7 КоАП	Непредставление сведений (информации)
влечет предупреждение, наложение административного штрафа на граждан, должностных лиц, юридических лиц, конфискацию несертифицированных/сертифицированных средств защиты информации, административное приостановление деятельности.	
Дисциплинарная ответственность	
Статья 90 ТК РФ	Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника
Статья 192 ТК РФ	Дисциплинарные взыскания
за совершение дисциплинарного проступка работодатель имеет право применить дисциплинарные взыскания: замечание, выговор, увольнение по соответствующим основаниям.	
Гражданско-правовая ответственность	
Статья 15 ГК РФ	Возмещение убытков
Статья 151 ГКРФ	Компенсация морального вреда

С 1 июля 2017 года вступили в силу поправки в статью 13.11 Кодекса Российской Федерации об административных правонарушениях (далее – КоАП РФ), которые вносят существенные изменения в положения, устанавливающие ответственность за нарушение законодательства в области персональных данных. Данные поправки значительно увеличивают штрафы

для операторов персональных данных. Для юридических лиц максимальный штраф теперь составляет 75000 рублей.

Исходя из программы совершенствования ИБ в ГБПОУ «КПТТ» (Верхнеуфалейский филиал) перед службой информационной безопасности техникума должны стоять следующие первоочередные задачи:

– администрировать имеющиеся средства безопасности (межсетевые экраны, антивирусные пакеты, системы обнаружения атак и пр.);

– разрабатывать модели и схемы защиты информации, принимать решения о приобретении новых средств безопасности;

– контролировать работу пользователей информационного пространства техникума;

– проводить статистику нарушений информационной безопасности умышленно или неумышленно, проистекает изнутри организации или из внешнего информационного пространства.

Таким образом, реализация систем защиты информации АИС возможна при тщательном учете всех аспектов, включая количественную оценку безопасности и размера ожидаемых потерь. Оценка экономически оптимальных параметров должна являться основой формирования конкретного технического облика СЗИ. Если не проводит тщательного анализа и не оптимизировать размер выделяемых на СЗИ средств, практически всегда руководитель организации оказывается в экономическом проигрыше.

Выводы по Главе III

В третьей главе магистерской диссертации описан объект защиты - Верхнеуфалейский филиал государственного бюджетного профессионального образовательного учреждения «Каслинский промышленно-гуманитарный техникум».

Верхнеуфалейский филиал государственного бюджетного профессионального образовательного учреждения «Каслинский промышленно-гуманитарный техникум» является обособленным 2 подразделением ГБПОУ «Каслинский промышленно-гуманитарный техникум».

Проведена оценка исходной защищенности ИСПДн и АИС для Верхнеуральского филиала ГБПОУ «Каслинский промышленно-гуманитарный техникум». Исходя из полученных данных ИСПДн и АИС в техникуме имеет низкую степень исходной защищенности.

На основе проведенной оценки исходной защищенности ИСПДн и анализа нормативно-правовых требований действующего законодательства нами была разработана Программа совершенствования ИБ в ГБПОУ «Каслинский промышленно-гуманитарный техникум».

Программа совершенствования ИБ в ГБПОУ «Каслинский промышленно-гуманитарный техникум» состоит из 4 этапов.

Этап 1. Разработка организационно-распорядительных и технических документов по защите персональных данных.

Этап 2. Повышение осведомленности/ознакомление работников в области персональных данных.

Этап 3. Установка и настройка технических средств защиты информации.

Этап 4. Аттестация информационных систем персональных данных.

Проведен расчет стоимости защиты ПДн техникума и Аттестации ИСПДн. Определены задачи службы информационной безопасности техникума.

ЗАКЛЮЧЕНИЕ

Магистерское диссертационное исследование решает проблему организации и управления службой информационной безопасности в образовательной организации СПО, в частности организацию защиты ИСПДн и АИС. Результаты проведенного исследования позволили сделать следующие общие выводы:

1. Проблема информационной безопасности представляет собой сложное социально-политическое явление, и ее разрешение во многом зависит от совершенствования системы защиты информации в образовательных организациях СПО.

Информационная безопасность образовательных организаций отличается от информационной безопасности других предприятий и организаций. Это обусловлено, прежде всего, специфическим характером угроз, а также публичной деятельностью образовательных организаций, которые вынуждены делать доступ к информационным ресурсам легким с целью удобства для граждан.

Информационная безопасность АС - состояние рассматриваемой автоматизированной системы, при котором она, с одной стороны, способна противостоять дестабилизирующему воздействию внешних и внутренних информационных угроз, а с другой ее наличие и функционирование не создает информационных угроз для элементов самой системы и внешней среды.

Информационная безопасность в организациях профессионального образования должна учитывать следующие специфические факторы:

- конфиденциальность информации (несанкционированное получение информации, в т.ч. персональных данных педагогов и студентов, служебной информации о самой образовательной организации);

- технические сбои и неполадки вычислительной техники и аппаратуры передачи данных, нарушения энергообеспеченности техники, физическое уничтожение или порча техники и др.;

- вредоносное и нежелательное программное обеспечение, хакерские атаки и спам;

- несанкционированное использование нелицензионного программного обеспечения сотрудниками образовательной организации;

- недисциплинированность и бесконтрольность педагогов, учебно-вспомогательного персонала и студентов в вопросах защиты информации;

- непонимание и незнание проблем информационной безопасности;

- нарушение авторских прав и прав интеллектуальной собственности.

2. С целью формирования на территории Челябинской области единой информационно-образовательной среды, обеспечивающей автоматизацию деятельности Министерства образования и науки Челябинской области; органов местного самоуправления, осуществляющих управление в сфере образования, и образовательных организаций, организацию электронного взаимодействия всех участников образовательных отношений в 2016 году введена в эксплуатацию автоматизированная информационная система «Образование Челябинской области» (АИС «Образование»).

Сетевой Город. Образование – комплексная автоматизированная информационная система, объединяющая в единую сеть образовательные учреждения и органы управления образования в пределах города, сельского или городского района (округа). Тем самым формируется единое информационное образовательное пространство муниципального образования**.**

3. В целях выявления направления совершенствования информационной безопасности образовательной организации проведена оценка исходной защищенности ИСПДн и АИС для Верхнеуральского филиала ГБПОУ «Каслинский промышленно-гуманитарный техникум».

4. На основе проведенной оценки исходной защищенности ИСПДн и анализа нормативно-правовых требований действующего законодательства была разработана Программа совершенствования ИБ в ГБПОУ «Каслинский промышленно-гуманитарный техникум».

Программа совершенствования ИБ в ГБПОУ «Каслинский промышленно-гуманитарный техникум» состоит из 4 этапов.

Этап 1. Разработка организационно-распорядительных и технических документов по защите персональных данных.

Этап 2. Повышение осведомленности/ознакомление работников в области персональных данных.

Этап 3. Установка и настройка технических средств защиты информации.

Этап 4. Аттестация информационных систем персональных данных.

5. В целях повышения эффективности процесса совершенствования информационной безопасности в техникуме было разработано электронное учебно-методическое обеспечение для обучения сотрудников техникума по организации работы с персональными данными, которое может быть применено в других образовательных организациях СПО.

Результаты исследования рекомендуется использовать в практической деятельности образовательных организаций СПО с целью совершенствования информационной безопасности в организациях СПО.

Таким образом, цель работы достигнута, задачи выполнены, гипотеза исследования подтвердилась.

Список использованной литературы

1. Аверченков, В.И. Автоматизация защиты персональных данных в ВУЗе / В.И. Аверченков, М.Ю. Рытов, В.А. Шкаберин, О.М. Голембиовская // Известия Международной ассоциации славянских вузов, № 1, 2011 г. - с. 126-134.

2. Аверченков, В.И. Организационная защита информации: учеб. Пособие / В.И. Аверченков, М.Ю. Рытов. - Брянск: БГТУ, 2013. - 184 с.

3. АИС «Сетевой город. Образование». Модуль профессиональной образовательной организации: руководство пользователя. - Закрытое акционерное общество «ИРТех», Самара. 2017. – 251 с.

4. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка), ФСТЭК, 2008.

5. Банк данных угроз безопасности информации. (Утверждено ФСТЭК России 06.03.2015 №240/22/879).

6. Боровых, И.С. Автоматизированная информационная система «Образование Челябинской области» как единая инфраструктура, обеспечивающая взаимодействие внутренних и внешних информационных систем / И.С. Боровых, Т.А. Орехова, Т.Б. Белякова // Научно-методическое обеспечение оценки качества образования. Научно-методический журнал. – Челябинск, 2017 №1(2). С. 95-98.

7. Вихорев, С.В. Классификация угроз информационной безопасности [Текст] / С.В. Вихров. - URL: http://www.cnews.ru/reviews/free/oldcom/security/elvis_class.shtml/. Дата обращения: 22.12.2018.

8. Волчинская, Е.К. Защита персональных данных: Опыт правового регулирования- М.: Галерия, 2012. - 236 с.

9. Гнедков А.В. Актуальные аспекты организации защиты персональных данных при их обработке в рамках процедур оценки качества образования / А.В. Гнедков, А.Б. Захаров, А.С. Ильин, Е.С. Мухаметьева,

И.В. Худорожков // Научно-методическое обеспечение оценки качества образования. Научно-методический журнал. – Челябинск, 2018 №5(5). С. 129-133.

10. Гнедков А.В. Применение средств криптографической защиты информации при проведении процедур оценки качества образования / А.В. Гнедков, А.Б. Захаров, А.С. Ильин, Е.С. Мухаметьева, И.В. Худорожков // Научно-методическое обеспечение оценки качества образования. Научно-методический журнал. – Челябинск, 2018 №1(4). С. 114-116.

11. Голембиовская, О.М. Автоматизация мониторинга защищенности информационных систем персональных данных [Текст] // Сборник научно-практических статей «Развитие регионов, как фактор укрепления единства и целостности государства. Выпуск №2». - Рыбница: 2012. -С.63-68.

12. Голембиовская, О.М. Организационное и техническое обеспечение защиты персональных данных: монография / В. И. Аверченков, М.Ю. Рытов, Т.Р. Гайнулин, М.В. Рудановский, О.М. Голембиовская - Брянск: БГТУ, 2011. -208 с.

13. Голембиовская, О.М. Разработка автоматизированной системы выбора средств и методов организации защиты персональных данных // Материалы Международной научно-практической конференции «Достижения молодых ученых в развитии инновационных процессов в экономике, науке, образовании». - Брянск: БГТУ, 2010. - 221-224.

14. Голембиовская, О.М. Формализация критериев выбора состава средств защиты информационных систем на основе оценки показателей угроз и уязвимостей [Текст] / О.М. Голембиовская, В.И. Аверченков, М.Ю. Рытов // Информация и безопасность. - Воронеж, № 4, 2011. с. 31-37.

15. Горлов, А.П. Способы и приемы выбора технических средств защиты информации с учетом одновременности реализации угроз: дис. … канд. тех. наук. – Санкт-Петербург, 2016. – 149 с.

16. ГОСТ Р 50922-96. Защита информации. Основные термины и определения.

17. Завгородний, В.И. Комплексная защита информации в компьютерных системах: Учебное пособие. - М.: Логос, 2001. - 264 с.

18. Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации: учебное пособие/ Ю.Н. Загинайлов. – Москва-Берлин: Директ-Медиа, 2015. – 253 с. – ISBN 978-5-4475-3946-7.

19. Зубаиров А.Ф. Создание единой информационной среды для оказания муниципальных услуг в сфере образования в электронном виде / А.Ф. Зубаиров // Научно-методическое обеспечение оценки качества образования. Научно-методический журнал. – Челябинск, 2017 №1(2). С. 105-109.

20. Ильин А.С. Анализ состояния защищенности персональных данных при их обработке в учреждениях системы образования Челябинской области в 2016 году / А.С. Ильин, Д.С. Ильина // Научно-методическое обеспечение оценки качества образования. Научно-методический журнал. – Челябинск, 2017 №1(2). С. 89-94.

21. Ильин, А.С. Обеспечение безопасности информации в образовательной организации в современных условиях / А.С. Ильин, Д.С. Ильина // Научно-методическое обеспечение оценки качества образования – 2016 –№ 1 – 48-51.

22. Корнев, П. А. Алгоритмы категорирования персональных данных для систем автоматизированного проектирования баз данных информационных систем: диссертация кандидата технических наук. - Липецк, 2012. - 152 с.

23. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, ФСТЭК, 2008. -10 с.

24. Методический документ**.** Меры защиты информации в государственных информационных системах. (Утверждено ФСТЭК России 11.02.2014г.).

25. Методы организации защиты информации: учебное пособие для студентов 3–4 курсов всех форм обучения направлений подготовки 230400.55, 230701.51, 090300.65, 220100.55 / Ю. Ю. Громов и др. – Тамбов: Изд-во ФГБОУ ВПО «ТГТУ», 2013. – 80 с.

26. О безопасности [Электронный ресурс]: [федеральный закон: от 05.03.1992 г. № 2446-I, в ред. от 25.12.1992 г. № 4235-I, от 24.12.1993 г. №2288, от 25.07.2002 г. № 116-ФЗ, от 07.03.2005 г. № 15-ФЗ]. - Режим доступа: www.consultant.ru. Дата обращения: 20.12.2018.

27. О персональных данных [Электронный ресурс]: [федеральный закон: от 27.07.2006 г. № 152-ФЗ, в ред. от 04.06.2014 г. № 152-ФЗ]. - Режим доступа: www.consultant.ru. Дата обращения: 20.12.2018.

28. Об информации, информационных технологиях и о защите информации [Электронный ресурс]: [федеральный закон: от 27.07.2006 г. №149-ФЗ, в ред. от 06.04.2011 г. № 149-ФЗ]. - Режим доступа: www.consultant.ru. Дата обращения: 20.12.2018.

29. Обеспечение информационной безопасности организации. – URL: http://www.iccwbo.ru/blog/2016/obespechenie-informatsionnoy-bezopasnosti/. Дата обращения: 20.12.2018.

30. Орехова, Т.А. Аспекты организационно-методического и информационного сопровождения процесса внедрения информационных систем в образовательные организации [Текст] / Т.А. Орехова, Т.Б. Белякова // Научно-методическое обеспечение оценки качества образования. – 2016. – №1 (1). – С.52-56.

31. Официальный сайт Государственного бюджетного профессионального образовательного учреждения «Каслинский промышленно-гуманитарный техникум». – URL: http://xn--80akibgedmg0bnqw.xn--p1ai/.

32. Парошина А.А. Информационная безопасность: стандартизированные термины и понятия / А.А. Парошина. – Владивосток: Изд-во Дальневост. Ун-та, 2010. – 216 с.

33. Положение по аттестации объектов информатизации по требованиям безопасности информации (утв. Гостехкомиссией РФ 25.11.1994) [Электронный ресурс] – Режим доступа: http://www.consultant.ru/document/ cons_doc_LAW_111428/

34. Постановление Правительства Российской Федерации от 17 ноября 2007 г. N 781 г. «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

35. Постановление Правительства Челябинской области от 13.12.2010 г. №293-П «О Порядке разработки и утверждения административных регламентов предоставления государственных услуг органами исполнительной власти Челябинской области»

36. Привалов А. Н., Богатырева Ю. И. Основные угрозы информационной безопасности субъектов образовательного процесса // Известия ТулГУ. Гуманитарные науки. 2012. №3. - URL: https://cyberleninka.ru/article/n/osnovnye-ugrozy-informatsionnoy-bezopasnosti-subektov-obrazovatelnogo-protsessa. Дата обращения: 12.12.2018.

37. Приказ Министерства образования и науки Челябинской области от 09.10.2017 г. № 02/3043 «Об утверждении плана функционирования АИС «Образование» на 2017-2018 учебный год».

38. Приказ Министерства образования и науки Челябинской области от 28.07.2016 г. № 01/2445 «О вводе в эксплуатацию автоматизированной системы «Образование Челябинской области»».

39. Приказ Минкомсвязи от 28.08.2015 №315 «О внесении изменений в Административный регламент Роскомнадзора…» «…О месте нахождения базы данных информации, содержащей персональные данные».

40. Приказ 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 (Приказ ФСБ РФ от 10.07.2014 г. №378).

41. Приказ Роскомнадзора от 19.08.2011г. №706 «Об утверждении Рекомендаций по заполнению образца формы уведомления об обработке (о намерении осуществлять обработку) персональных данных».

42. Приказ ФАПСИ от 13 июня 2001 г. N 152 «Об утверждении Инструкции об организации и обеспечении безопасности хране ния, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» // ГАРАНТ. Дата обращения к ресурсу: 3.01.2019.

43. Приказ Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. № 378 г. Москва «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»: // Российская газета – 2014 – 17 сентября.

44. Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

45. Приказ Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. №17 «Требования о защите информации, не содержащей государственную тайну, содержащейся в государственных информационных системах».

46. Приказ Федеральной службы по техническому и экспортному контролю (ФСГЭК России) Федеральной службы безопасности Российской Федерации (ФСБ России) Министерства информационных технологий и связи Российской Федерации (Мининформсвязи России) от 13 февраля 2008 г. N 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных».

47. Приказ ФСТЭК России от 5 февраля 2010 г. № 58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных».

48. Проталинский О.М., Ажмухамедова И.М. Информационная безопасность ВУЗа / О.М. Проталинский, И.М. Ажмухамедов // Вестник АГТУ. Сер. Управление, вычислительная техника и информатика. 2009. № 1. С. 18-23.

49. Распоряжение Губернатора Челябинской области от 01.11.2010 г. №732-р «О плане мероприятий по реализации Федерального закона «Об организации предоставления государственных и муниципальных услуг».

50. Распоряжение Правительства Челябинской области от 30 декабря 2015 г. № 774- рп «Об утверждении плана мероприятий («дорожная карта») Челябинской области по созданию регионального сегмента единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам» [Электронный ресурс] – Режим доступа: http://old.rcokio.ru/pics/uploads/IT/774.pdf.

51. Система обеспечения информационной безопасности. – URL: http://www.ec-leasing.ru/products/sistemy-obespechiniya-informacionnoi-bezopasnosti/. Дата обращения: 08.01.2019.

52. Системная классификация угроз информационной безопасности. - URL: https://www.securitylab.ru/blog/personal/aguryanov/30012.php. Дата обращения: 10.12.2018.

53. Стандарты информационной безопасности. – URL: https://tvoi.biz/biznes/informatsionnaya-bezopasnost/prakticheskaya-polza-standartov-info.html. Дата обращения: 25.12.2018.

54. Степанов, Е.А. Информационная безопасность и защита информации [Текст]: учеб. пособие / Е.А. Степанов, И.К. Корнеев. – М.: ИНФРА – М, 2013. – 304 с.

55. Угрозы информации. – URL: http://lawbooks.news/telekommunikatsionnyie-sistemyi-kompyuternyie/ugrozyi-informatsii-66006.html. Дата обращения: 12.12.2018.

56. Федеральный закон от 07.07.2010 г. №210 - ФЗ Об организации предоставления государственных и муниципальных услуг.

57. Федеральный закон от 27 июля 2006 N 152-ФЗ (ред. от 21.07.2014) «О персональных данных» (с изм. и доп., вступ. в силу с 01.09.2015).

Приложение

Приложение 1

Для обучения сотрудников техникума по организации работы с персональными данными разработано электронное учебно-методическое обеспечение.

Структура электронного учебно-методического обеспечения представляет собой Web-сайт и состоит из 6 разделов, которые расположены в блоке управления.

Блок управления располагается в левой части сайта и позволяет мгновенно перемещаться между разделами web-сайта.

Электронное учебно-методическое обеспечение содержит нормативные документы, примеры журналов для работы с ПДн, пакет документов по СКЗИ, пакета документов на аттестацию рабочего места, теоретический материал по организации защиты персональных данных (демонстрационный материал).

Главная страница - страница приветствия, содержит блок управления (рис. 1).

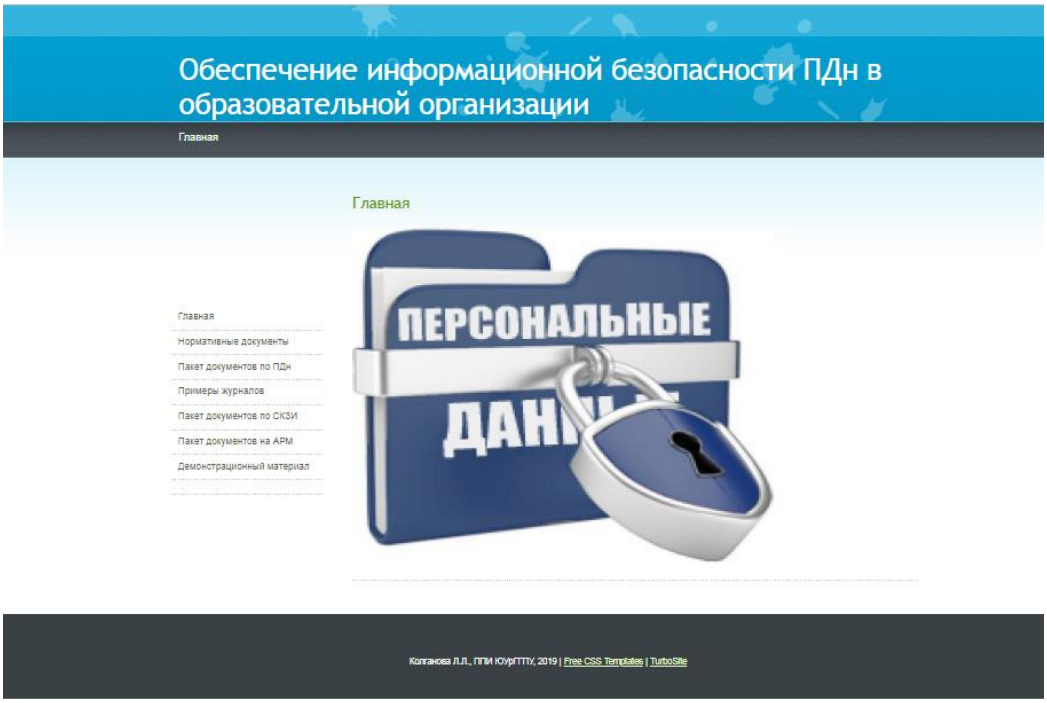

Рисунок 1– Главная страница

Слева на страницы расположено содержание ЭУМО (рис. 2)

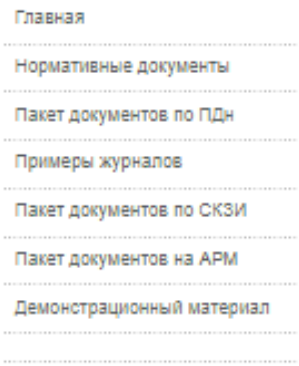

Рисунок 2 – Содержание ЭУМО

Опишем функциональные возможности всех страниц электронного учебно-методического обеспечения.

«Нормативные документы» - содержит перечень нормативных документов, регламентирующих обротку и защиту персональных данных (рис.3).

Рисунок 3– Нормативные документы

Пакет документов по ПДн. При выборе этого раздела открывается страница, содержащая организационно-распорядительные документы по защите персональных данных (рис. 4, 5).

Рисунок 4– Пакет документов по ПДн

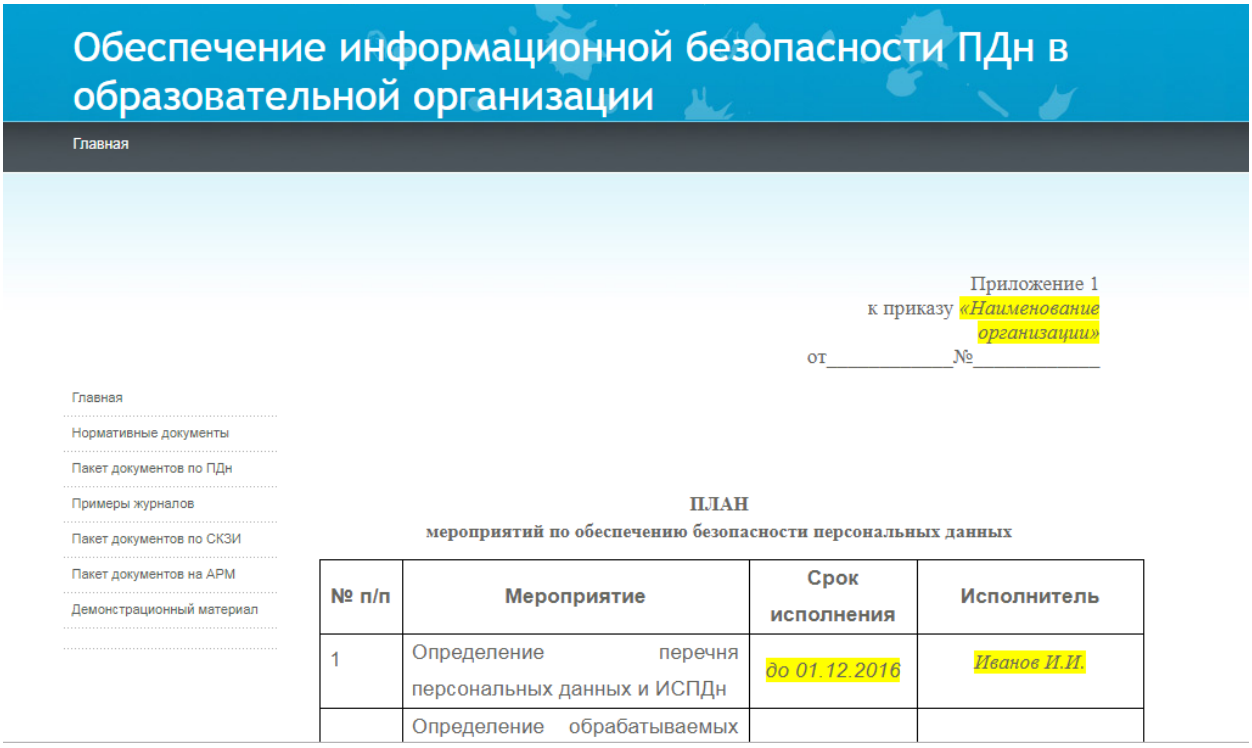

Рисунок 5– Пример Плана мероприятий по обеспечению безопасности ПДн

Примеры журналов. При выборе этого раздела открывается страница, содержащая примеры журналов (рис. 6, 7)

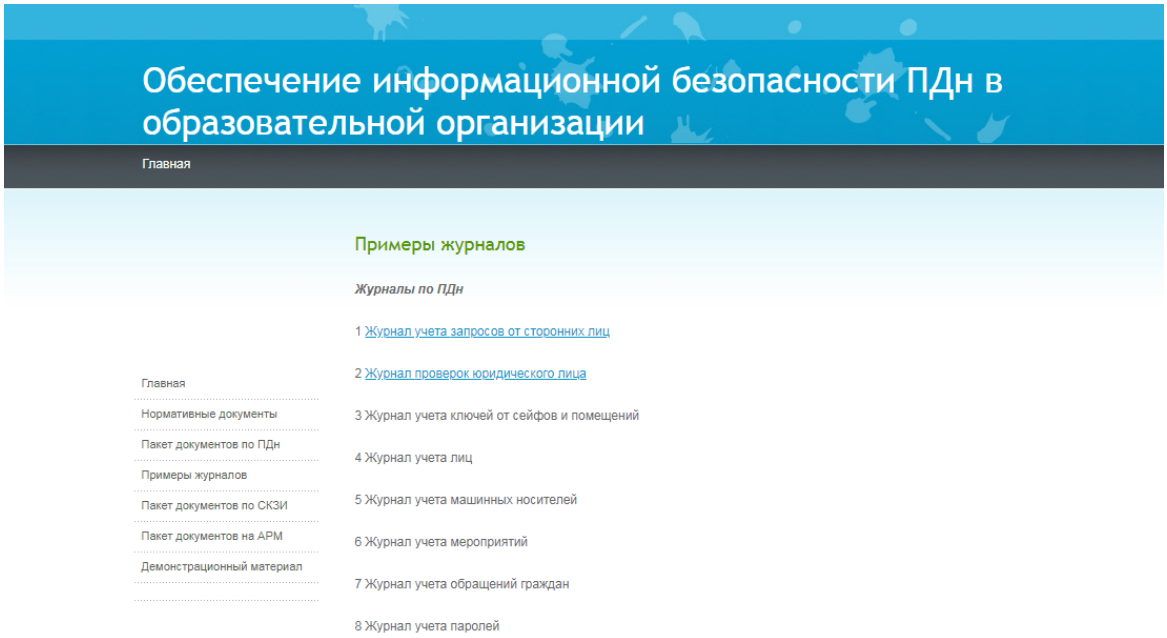

Рисунок 6– Страница с перечнем журналов для работы с ПДн

Рисунок 7– Пример журнала учета запросов от сторонних лиц по получению персональных данных

Пакет документов по СКЗИ. Данный раздел содержит описание документов по СКЗИ (рис. 8,9).

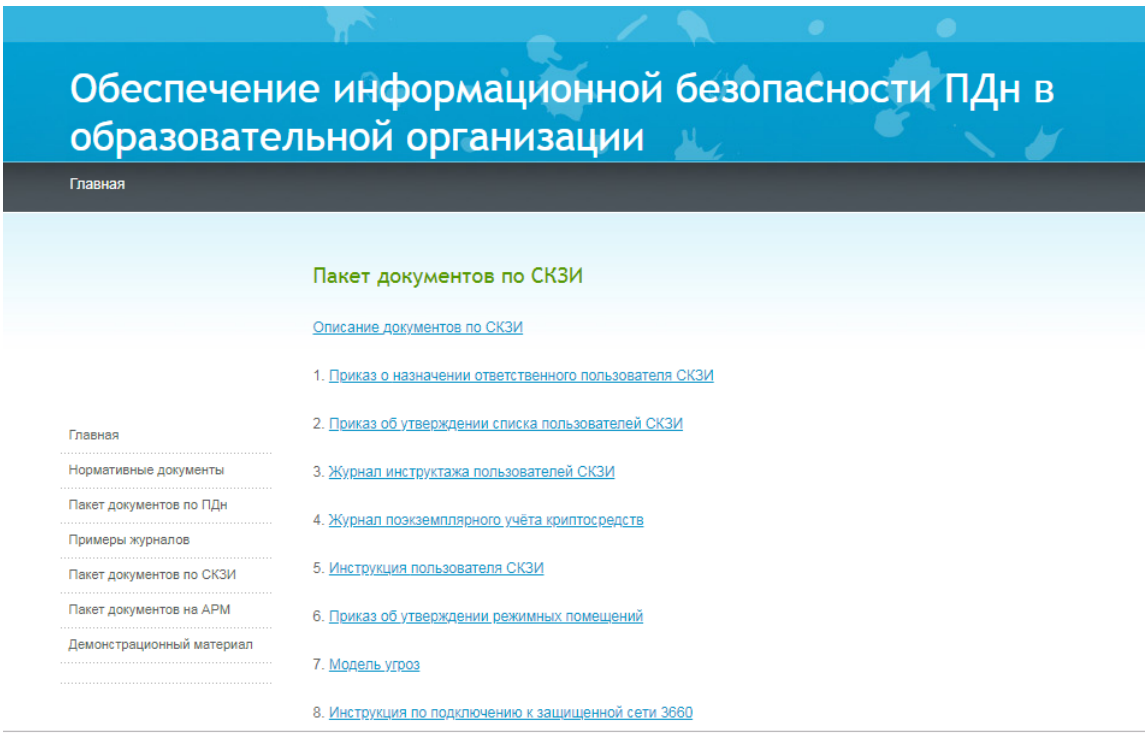

Рисунок 8– Пакеты документов по СКЗИ

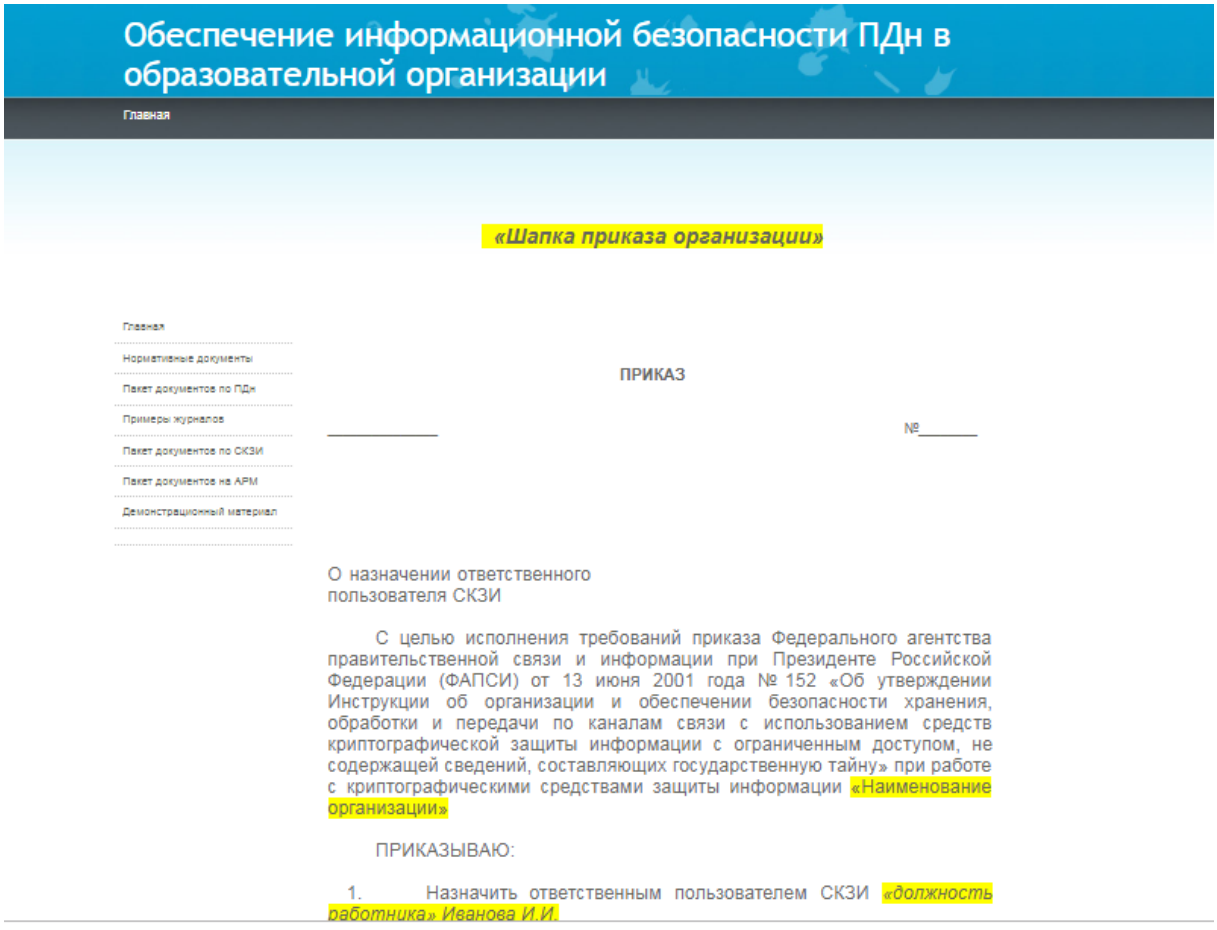

Рисунок 9– Пример приказа о назначении ответственного пользователя СКЗИ

Для организации обучения необходим компьютерный класс, оснащенный следующим образом (таб. 1, 2).

Таблица 1

Перечень оборудования кабинета вычислительной техники

№	Устройство	Наименование	Количество, шт.
1	Системный блок	Intel® Core™ i3-7100 CPU @ 3/90GHz 3/90 GHz, ОЗУ не менее 8 Гб или аналоги, NVIDIA GeForce GT 720, CD/DVD-RW, HDD (Гб) 500	10-15
2	Монитор	23.8" Монитор LG 24MP59G-P	10-15
3	Клавиатура	Logitech K280e	10-15
4	Мышь	Мышь проводная A4Tech X-710BK черный	10-15
5	Принтер	HP LaserJet Pro M28w (W2G55A)	1
6	Проектор	Проектор Canon LV-X320	1
7	Демонстрационный экран	100" (254 см) Экран для проектора DEXP WM-100	1
8	Доска	-	1

Таблица 2

Минимальное программное обеспечение кабинета вычислительной техники для изучения дисциплины «Информационные технологии»

№	Наименование
1	Операционная система Windows 7 и выше
2	Microsoft Office – профессиональный выпуск версии 2010 или 2016
3	Электронное учебно-методическое обеспечение «Обеспечение информационной безопасности ПДн в образовательной организации»

Программно-технические требования к электронному учебно-методическому обеспечению:

- Core i3 и выше;
- Оперативная память: не менее 8 Гb;
- Видеокарта: не менее 2 Гb;
- Операционная система: Windows7/8/10/;
- Манипулятор мышь;
- Наличие пакета MSOffice.