Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Южно-Уральский государственный университет»
(национальный исследовательский университет)

Высшая школа электроники и компьютерных наук

Кафедра «Защита информации»

РАБОТА ПРОВЕРЕНА
Рецензент, зам. директора по ИБ
ООО «ИТ Энигма»
_____ _____ Г.М. Галина
_____2018 г.

ДОПУСТИТЬ К ЗАЩИТЕ
Заведующий кафедрой,
к.т.н., доцент
_____ А.Н. Соколов
_____ 2018 г.

Создание типовой системы защиты персональных данных в образовательных учреждениях Челябинской Области при их подключении к государственной информационной системе «Сетевой город. Образование»

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ – 10.05.03.2018.278.ПЗ ВКР

Консультанты

Безопасность жизнедеятельности,
к.т.н., доцент
_____ Н.В. Глотова
_____ 2018 г.

Руководитель проекта,
н.с. НОЦ «Информационная безопасность» ВШЭКН
_____А.Е. Баринов
_____ 2018 г.

Автор проекта,
студент группы КЭ-530
_____В.М. Яумбаев
_____ 2018 г.

Нормоконтролер,
к.т.н., доцент
_____ В.П. Мартынов
_____ 2018 г.

Челябинск 2018

Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Южно-Уральский государственный университет
(национальный исследовательский университет)»

Высшая школа электроники и компьютерных наук
Кафедра «Защита информации»

Специальность 10.05.03 «Информационная безопасность автоматизированных систем»

УТВЕРЖДАЮ
Заведующий кафедрой
_____ А.Н. Соколов

_____ 2018 г.

З А Д А Н И Е
на выпускную квалификационную работу студента

Яумбаева Вильяна Мирзаяновича

Группа *КЭ-530*

1. Тема работы

Создание типовой системы защиты персональных данных в образовательных учреждениях Челябинской Области при их подключении к государственной информационной системе «Сетевой город. Образование»

Утверждена приказом ректора ЮУрГУ от _____ № _____
(утверждена, прот. заседания кафедры от _____ № _____)

2. Срок сдачи студентом законченной работы _____

3. Исходные данные к работе
Отчет о преддипломной практике, нормативно-правовые документы в области защиты информации, документация предприятия-базы практики

4. Содержание расчетно-пояснительной записки (перечень подлежащих разработке вопросов)

4.1 Проведение предпроектного обследования;

4.2 Теоретическое обоснование выбора средств защиты;

4.3 Разработка проекта типовой системы защиты персональных данных в образовательных учреждениях Челябинской Области при их подключении к ГИС «Сетевой город. Образование».

5. Перечень графического материала (с точным указанием обязательных чертежей, плакатов в листах формата А1)

Презентация «Создание типовой системы защиты персональных данных в образовательных учреждениях Челябинской Области при их подключении к ГИС «Сетевой город. Образование»
в формате PowerPoint 2007 (pptx)
Количество слайдов -

Всего ___ листов

6. Консультанты по работе (проекту), с указанием относящихся к ним разделов работы (проекта)

Раздел	Консультант	Подпись, дата	
		Задание выдал (консультант)	Задание принял (студент)
Безопасность жизнедеятельности	Н.В. Глотова		

7. Дата выдачи задания _____

Руководитель,
н.с. НОЦ «Информационная безопасность» ВШЭКН_____ А.Е. Баринов

Задание принял к исполнению _____ В.М. Яумбаев

КАЛЕНДАРНЫЙ ПЛАН

Наименование этапов выпускной квалификационной работы (проекта)	**Срок выполнения этапов работы**	**Отметки о выполнении руководителя**
Введение		
1 Проведение предпроектного обследования		
2 Теоретическое обоснование выбора средств защиты		
3 Разработка проекта типовой системы защиты персональных данных в образовательных учреждениях Челябинской Области при их подключении к ГИС «Сетевой город. Образование»		
4 Безопасность жизнедеятельности		
Заключение		
Библиографический список		
Предзащита ВКР		
Защита ВКР		

Заведующий кафедрой _____ А.Н. Соколов

Руководитель работы _____ А.Е. Баринов

Студент _____ В.М. Яумбаев

АННОТАЦИЯ

Яумбаев В.М. Создание типовой системы защиты персональных данных в общеобразовательных учреждениях Челябинской области при их подключении к государственной информационной системе «Сетевой город. Образование» – Челябинск: ЮУрГУ, КЭ-530, ___ с., __ ил., __ табл., библиогр. список – __ наим., ___ прил.

Выпускная квалификационная работа выполнена с целью создания типовой системы защиты персональных данных в общеобразовательных учреждениях Челябинской области при их подключении к государственной информационной системе (далее - ГИС) «Сетевой Город. Образование» и последующем обмене данными с информационной системой «Контингент».

В первой главе проведен анализ существующей системы защиты информации, в ходе которого был разработан паспорт предприятия, выявлены объекты защиты, рассмотрены актуальные угрозы, уязвимости.

Во второй главе проведено теоретическое обоснование выбора средств защиты для создания типовой системы защиты персональных данных в общеобразовательных учреждениях Челябинской области при их подключении к ГИС «Сетевой Город. Образование», включающее в себя анализ выявленных угроз, уязвимостей и средств по их устранению.

В третьей главе разработан проект типовой системы защиты информации. В результате были определены объекты поставки, построена матрица ответственности, а также разработана диаграмма Ганта.

В четвертой главе проанализированы наиболее опасные вредные и производственные факторы. Даны общие рекомендации по организации и выбору рабочего места, а также описана пожарная и электробезопасность помещения.

ОГЛАВЛЕНИЕ

СОКРАЩЕНИЯ

АИС	-	автоматизированная информационная система;
АРМ	-	автоматизированное рабочее место;
АС	-	автоматизированная система;
ГИС	-	государственная информационная система
ИСПДн	-	информационная система персональных данных;
ЛВС	-	локальная вычислительная сеть;
НСД	-	несанкционированный доступ;
ОС	-	операционная система;
ПДн	-	персональные данные;
ПО	-	программное обеспечение;
ПЭМИН	-	побочные электромагнитные излучения и наводки;
СЗИ	-	средства защиты информации;
СКЗИ	-	средства криптографической защиты информации;
СЗПДн	-	система (подсистема) защиты персональных данных;
УБПДн	-	угрозы безопасности персональных данных.

ОПРЕДЕЛЕНИЯ

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Доступ к информации – возможность получения информации и ее использования.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и / или выходящей из информационной системы.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

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

Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

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

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

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

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Раскрытие персональных данных – умышленное или случайное нарушение конфиденциальности персональных данных.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

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.

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

ВВЕДЕНИЕ

Потребности человека в доступе к разнообразной информации стремительно растёт, и жизнь современной школы не может обойтись без информатизации учебно-воспитательного процесса. Кроме того, информация ежегодно увеличивается в объёме в несколько раз, и успеть её переработать становится всё труднее. Для удобства и экономии времени работы с ней разрабатываются различные компьютерные программы и системы. Одна из них – государственная информационная система «Сетевой Город. Образование» (ГИС СГО).

Основная задача системы «Сетевой Город. Образование» - это создание открытого информационного пространства для родителей и общественности, что способствует повышению качества образования.

Таким образом, актуальность моей работы связана с необходимостью защиты персональных данных при обмене общеобразовательных учреждений с ГИС СГО.

Объектом выпускной квалификационной работы являются общеобразовательные учреждения.

Предметом выпускной квалификационной работы является информация ограниченного доступа, а именного персональные данные сотрудников и учащихся общеобразовательных учреждений.

Целью дипломной работы является создание типовой системы защиты персональных данных в общеобразовательных учреждениях Челябинской области при их подключении к ГИС СГО.

В соответствии с поставленной целью необходимо решить следующие задачи:

1. Проанализировать деятельность общеобразовательных учреждений, с целью обоснования необходимости разработки мер по защите информации ограниченного доступа.
2. Проанализировать возможные средства защиты и дать обоснование их использования.
3. Разработать проект по созданию типовой системы защиты персональных данных в общеобразовательных учреждениях Челябинской области при их подключении к ГИС СГО.

1. ПРОВЕДЕНИЕ ПРЕДПРОЕКТНОГО ОБСЛЕДОВАНИЯ

1.1. Разработка паспорта

Для создания системы защиты информации было проведено предпроектное обследование нескольких школ, в результате которого был составлен типовой технический паспорт (Приложение Д).

В техническом паспорте приведен состав ОТСС, ВТСС, схемы их размещения, расположение линий коммуникаций, перечень установленных средств защиты информации и программного обеспечения.

В качестве объектов защиты были выбраны три общеобразовательных учреждения, по которым создавалась типовая система защиты ПДн.

1.2. Разработка модели деятельности

В ходе обследования была построена модель деятельности (Приложение Ж). В этой схеме отражаются основные этапы технологического процесса обработки защищаемой информации от подготовки к обработке информации ограниченного доступа до сохранения результатов.

Данная модель необходима для выявления информационных потоков ограниченного доступа.

1.3. Выявление защищаемой информации

В ходе проведения информационно – аналитической работы, а также руководствуясь моделью деятельности, было выявлено, что информация ограниченного доступа, циркулирующая в рамках ГИС «Сетевой город. Образование» подлежит защите на основании Федерального закона от 27.07.2006 №152-ФЗ (ред. от 29.07.2017) «О персональных данных».

На основании проведенного анализа информационно – аналитической деятельности и выполнения требований п. 4, ст. 9 Федерального закона от 27.07.2006 №152-ФЗ (ред. от 29.07.2017) «О персональных данных», был разработан «Пере-

чень персональных данных» (Приложение В), основанием для закрепления которого явилось разработанное в рамках выпускной квалификационной работы «Положение об обработке персональных данных» (Приложение А).

1.4. Описание информационной среды

Руководствуясь классификацией мер по защите информации приведем описание типовой информационной системы в общеобразовательных учреждениях Челябинской области:

– Под организационным обеспечением общеобразовательных учреждений мы понимает ряд документов, регулирующих и регламентирующие взаимодействие работников с техническими средствами и между собой в процессе эксплуатации данной информационной системы. К таким документам относятся должностные инструкции персонала; инструкции по эксплуатации программного обеспечения и технических средств, по проведению контрольных или внештатных мероприятий, системах взаимодействия с персоналом.

– Под программно-аппаратным обеспечением общеобразовательных учреждений мы понимаем комплекс программно-аппаратных средств, обеспечивающих работу с ГИС «Сетевой город. Образование». Для подробного описания данных информационных систем были проведены обследования разных учреждений, результаты которых представлены в Таблице 1 и Таблице 2.

Таблица 1 – Аппаратное обеспечение

№ п/п	Автоматизированное рабочее место	Вид оборудования	Модель	Расположение
1	2	3	4	5
1	АРМ1 ГИС «Сетевой город. Образование»	Монитор	DNS H1910	Кабинет психолога
		Системный блок	-	
		Принтер	Epson EPL-6200L	
		Клавиатура	A4Tech KL-23MU	
		Мышь	A4Tech X5-3D	
2	АРМ2 ГИС «Сетевой город. Образование»	Монитор	Proview	Кабинет 38
		Системный блок	-	
		Клавиатура	R-Style	
		Мышь	Oklick	

Продолжение таблицы 1

1	2	3	4	5
3	АРМ3 ГИС «Сетевой город. Образование»	Монитор	View Sonic	Кабинет 2
		Системный блок	-	
		Клавиатура	Logitech	
		Мышь	Sven	

Таблица 2 – Программное обеспечение

№ п/п	Наименование	Место установки
1	Windows 7 Professional	АРМ1 ГИС «Сетевой город. Образование»
2	OpenOffice	
3	Internet explorer	
4	Microsoft Windows 8	АРМ2 ГИС «Сетевой город. Образование»
5	Microsoft Office Professional Plus 2010	
6	Яндекс.Браузер	
7	Microsoft Windows 7 Professional	АРМ3 ГИС «Сетевой город. Образование»
8	Microsoft Office 2007	
9	Mozilla firefox	

1.5. Выявление объектов защиты

Первым шагом в проектировании новой системы защиты является определение характеристик защищаемого объекта. При определении характеристик объекта должна быть собрана информация по возможно большему числу связанных с ним вопросов. Вначале это представляется очень сложной и многоплановой задачей, однако известно несколько аспектов, на которых следует сосредоточить внимание, чтобы получить нужную информацию. Они включают в себя:

– физические условия;

– рабочие процессы на объекте;

– правила, регламентирующие работу и процедуры, принятые на объекте;

– требования органов государственного регулирования и вышестоящего руководства;

– вопросы аварийной безопасности;

– юридические вопросы;

– корпоративные цели и задачи.

Объекты защиты информации выявляются на основе перечня защищаемой информации, а также в результате анализа средств, методов и процессов обработки информации. В результате проведенной работы был составлен перечень объектов защиты:

– Помещение для хранения и работы с информацией ограниченного доступа;

– Автоматизированное рабочее место;

– Средства ввода – вывода и отображения информации;

– Линии и средства связи, системы обеспечения функционирования СВТ и деятельности общеобразовательного учреждения;

– Носители информации;

– Информационные инфраструктуры;

– Персонал.

1.6. Разработка модели угроз выявленных объектов

Модель угроз информационной безопасности – это описание существующих угроз информационной безопасности, их актуальности, возможности реализации и последствий.

Модель угроз персональных данных при их обработке в ИСПДн «ГИС «Сетевой город. Образование» строится на основании анализа ИСПДн.

В модели угроз представлено описание структуры ИСПДн, состава и режима обработки ПДн, оценка исходного уровня защищенности, анализ угроз безопасности персональных данных.

Анализ УБПДн включает:

– описание угроз;

– оценку вероятности возникновения угроз;

– оценку реализуемости угроз;

– оценку опасности угроз;

– определение актуальности угроз.

1.7. Разработка модели угроз выявленных объектов

Расчет рисков важных объектов защиты ПДн в общеобразовательных учреждениях был выполнен на основе документа «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» ФСТЭК.

1.7.1. Вероятность реализации угроз безопасности персональных данных

Под вероятностью реализации угрозы понимается определяемый экспертным путем показателя, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для ИСПДн в складывающихся условиях обстановки.

Числовой коэффициент (Y2) для оценки вероятности возникновения угрозы определяется по 4 вербальным градациям этого показателя:

– маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (Y2 = 0);

– низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (Y2 = 2);

– средняя вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны (Y2 = 5);

– высокая вероятность – объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты (Y2 = 10).

1.7.2. Реализуемость угроз

Под общим уровнем защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн (Y1).

В Таблице 3 представлены характеристики уровня исходной защищенности для ИСПДн.

Таблица 3 – Исходный уровень защищенности

Технические и эксплуатационные характеристики	Уровень защищенности
1	2
По территориальному размещению	Высокий
По наличию соединения с сетями общего пользования	Средний
По встроенным (легальным) операциям с записями баз персональных данных	Низкий
По разграничению доступа к персональным данным	Средний
По наличию соединений с другими базами ПДн иных ИСПДн	Высокий
По уровню (обезличивания) ПДн	Низкий
По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки	Высокий

ИСПДн имеет средний уровень исходной защищенности, так как не менее 70% характеристик ИСПДн соответствуют уровню не ниже «средний».

Показатель исходной защищенности Y1 = 5.

По итогам оценки уровня защищенности (Y1) и вероятности реализации угрозы (Y2), рассчитывается коэффициент реализуемости угрозы (Y) и определяется возможность реализации угрозы. Коэффициент реализуемости угрозы Y будет определяться соотношением Y = (Y1 + Y2)/20

Оценка реализуемости угроз безопасности персональных представлена в Таблице 4.

Таблица 4 – Реализуемость угроз

Тип угроз безопасности ПДн	Коэффициент реализуемости угрозы (Y)	Возможность реализации
1	2	3
Угрозы несанкционированного доступа к информации		
Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн		
Кража ПЭВМ	0,35	низкая
Кража носителей информации	0,35	низкая
Кража ключей и атрибутов доступа	0,35	низкая
Кражи, модификации, уничтожения информации	0,35	низкая
Вывод из строя узлов ПЭВМ, каналов связи	0,35	низкая
Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	0,35	низкая
Несанкционированное отключение средств защиты	0,35	низкая
Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)		
Действия вредоносных программ (вирусов)	0,5	средняя
Недекларированные возможности системного ПО и ПО для обработки персональных данных	0,35	низкая

Продолжение таблицы 4

1	2	3
Установка ПО не связанного с исполнением служебных обязанностей	0,35	низкая
Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера		
Утрата ключей и атрибутов доступа	0,35	низкая
Непреднамеренная модификация (уничтожение) информации сотрудниками	0,35	низкая
Непреднамеренное отключение средств защиты	0,35	низкая
Выход из строя аппаратно-программных средств	0,35	низкая
Сбой системы электроснабжения	0,35	низкая
Стихийное бедствие	0,35	низкая
Угрозы преднамеренных действий внутренних нарушителей		
Доступ к информации, модификация, уничтожение лиц, не допущенных к ее обработке	0,5	средняя
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	0,35	низкая
Угрозы несанкционированного доступа по каналам связи		

Продолжение таблицы 4

1	2	3
Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации	0,35	низкая
Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	0,5	средняя
Угрозы выявления паролей по сети	0,5	средняя
Угрозы навязывание ложного маршрута сети	0,35	низкая
Угрозы подмены доверенного объекта в сети	0,35	низкая
Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	0,35	низкая
Угрозы типа «Отказ в обслуживании»	0,5	средняя
Угрозы удаленного запуска приложений	0,5	средняя
Угрозы внедрения по сети вредоносных программ	0,5	средняя

1.7.3. Оценка опасности угроз

Оценка опасности УБПДн производится на основе опроса специалистов по защите информации и определяется вербальным показателем опасности, который имеет три значения:

– низкая опасность - если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;

– средняя опасность - если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;

– высокая опасность - если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Оценка опасности угроз безопасности персональных данных представлена в Таблице 5.

Таблица 5 – Опасность угроз персональных данных

Тип угроз безопасности ПДн	Опасность угрозы
1	2
Угрозы несанкционированного доступа к информации	
Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн	
Кража ПЭВМ	Низкая
Кража носителей информации	Низкая
Кража ключей и атрибутов доступа	Низкая
Кражи, модификации, уничтожения информации	Низкая
Вывод из строя узлов ПЭВМ, каналов связи	Низкая
Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	Низкая
Несанкционированное отключение средств защиты	Низкая
Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)	
Действия вредоносных программ (вирусов)	Средняя
Не декларированные возможности системного ПО и ПО для обработки персональных данных	Низкая
Установка ПО, не связанного с исполнением служебных обязанностей	Низкая

Продолжение таблицы 5

1	2
Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера	
Утрата ключей и атрибутов доступа	Низкая
Непреднамеренная модификация (уничтожение) информации сотрудниками	Низкая
Непреднамеренное отключение средств защиты	Низкая
Выход из строя аппаратно-программных средств	Низкая
Сбой системы электроснабжения	Низкая
Стихийное бедствие	Низкая
Угрозы преднамеренных действий внутренних нарушителей	
Доступ к информации, модификация, уничтожение лиц, не допущенных к ее обработке	Средняя
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	Низкая
Угрозы несанкционированного доступа по каналам связи	
Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:	Низкая
Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	Средняя
Угрозы выявления паролей по сети	Средняя
Угрозы навязывание ложного маршрута сети	Низкая
Угрозы подмены доверенного объекта в сети	Низкая

Продолжение таблицы 5

Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	Низкая
Угрозы типа «Отказ в обслуживании»	Средняя
Угрозы удаленного запуска приложений	Средняя
Угрозы внедрения по сети вредоносных программ	Средняя

1.7.4. Оценка опасности угроз

В соответствии с правилами отнесения угрозы безопасности к актуальной, для ИСПДн определяются актуальные и неактуальные угрозы, Таблица 6.

Таблица 6 – Определение актуальности угроз

Возможность реализации угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

Оценка актуальности угроз безопасности представлена в Таблице 7.

Таблица 7 – Актуальность угроз безопасности персональных данных

Тип угроз безопасности ПДн	Актуальность угрозы
1	2
Угрозы несанкционированного доступа к информации	
Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн	
Кража ПЭВМ	Не актуальная
Кража носителей информации	Не актуальная
Кража ключей и атрибутов доступа	Не актуальная
Кражи, модификации, уничтожения информации	Не актуальная

Продолжение таблицы 7

1	2
Вывод из строя узлов ПЭВМ, каналов связи	Не актуальная
Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	Не актуальная
Несанкционированное отключение средств защиты	Не актуальная
Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)	
Действия вредоносных программ (вирусов)	Актуальная
Не декларированные возможности системного ПО и ПО для обработки персональных данных	Не актуальная
Установка ПО, не связанного с исполнением служебных обязанностей	Не актуальная
Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера	
Утрата ключей и атрибутов доступа	Не актуальная
Непреднамеренная модификация (уничтожение) информации сотрудниками	Не актуальная
Непреднамеренное отключение средств защиты	Не актуальная
Выход из строя аппаратно-программных средств	Не актуальная
Сбой системы электроснабжения	Не актуальная
Стихийное бедствие	Не актуальная
Угрозы преднамеренных действий внутренних нарушителей	
Доступ к информации, модификация, уничтожение лиц, не допущенных к ее обработке	Актуальная

Продолжение таблицы 7

1	2
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	Не актуальная
Угрозы несанкционированного доступа по каналам связи	
Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации	Не актуальная
Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	Актуальная
Угрозы выявления паролей по сети	Актуальная
Угрозы навязывание ложного маршрута сети	Не актуальная
Угрозы подмены доверенного объекта в сети	Не актуальная
Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	Не актуальная
Угрозы типа «Отказ в обслуживании»	Актуальная
Угрозы удаленного запуска приложений	Актуальная
Угрозы внедрения по сети вредоносных программ	Актуальная

1.8. Разработка технического задания

В ходе проведения информационно-аналитической работы деятельности общеобразовательных учреждений Челябинской области, а также на основании информации полученной в ходе беседы с заместителями директоров по методической работе, а также с системными администраторами, было разработано техническое задание на создание типовой системы защиты ПДн в образовательных учреждениях (Приложение Г).

Ввиду отсутствия утвержденного стандарта на разработку технического задания по защите ИСПДн в работе руководствуемся ГОСТом 34 серии.

Данное техническое задание разрабатывалось на основе ГОСТ 34.602-1989 «Техническое задание на создание автоматизированной системы» и содержит следующие разделы:

1. Общие сведения;
2. Назначение и цели создания системы защиты персональных данных;
3. Характеристика объекта защиты;
4. Требования к системе защиты персональных данных;
5. Состав и содержание работ по созданию системы защиты персональных данных;
6. Порядок контроля и приемки системы защиты персональных данных;
7. Требования к составу и содержанию работ по подготовке объекта автоматизации к вводу системы защиты персональных данных в действие;
8. Требования к документированию;
9. Источники разработки.

1.9. Вывод по первой главе

В результате проведенных предпроектных обследований общеобразовательных учреждений Челябинской области, была проделана следующая работа:

– Составлен типовой технический паспорт информационных систем персональных данных (Приложение Д);

– Разработана типовая модель деятельности, отражающая процесс обработки информации ограниченного доступа (Приложение З);

– Разработан перечень персональных данных, подлежащих защите в информационной системе персональных данных (Приложение В);

– Разработана типовая модель угроз безопасности персональных данных и произведена оценка их актуальности;

– Разработано типовое техническое задание на создание системы защиты персональных данных в общеобразовательных учреждениях Челябинской области (Приложение Г).

2. ТЕОРИТИЧЕСКОЕ ОБОСНОВАНИЕ ВЫБОРА СРЕДСТВ ЗАЩИТЫ

2.1. Обзор возможных методов устранения уязвимостей

Одним из этапов обеспечения защиты персональных данных обрабатываемых в ГИС «Сетевой город. Образование» является определение и анализ используемых в настоящее время методов и средств, необходимых для устранения выявленных угроз и уязвимостей. Руководствуясь разработанной моделью угроз в пункте 1.7 настоящей работы, а также Приказом ФСТЭК от 18 февраля 2013 г. № 21, рассмотрим наиболее эффективные варианты их минимизации.

2.1.1. Угроза доступа к информации, ее модификации и уничтожение лицами, не имеющими прав доступа

Угроза осуществляется внешними нарушителями там, где расположены элементы ИСПДн и средства защиты, а также происходит работа пользователей.

Данную угрозу можно устранить установкой средства защиты от несанкционированного доступа (далее – НСД), прошедшего процедуру оценки соответствия требованиям ФСТЭК. Дополнительно в комплексе со средством защиты от НСД необходима реализация организационных и инженерно-технических мер таких как:

- установка замков на дверь помещения, в котором ведется обработка персональных данных;
- установка охранно-пожарной сигнализации;

Для того чтобы определиться со средством защиты, был проведен сравнительный анализ 2 – х наиболее часто используемых средств защиты от НСД, приведенный в Таблице 8.

Таблица 8 – Сравнительный анализ средств защиты от НСД

Критерии сравнения / Средства ЗИ	Dallas Lock 8.0-K	Secret Net Studio
Стоимость, руб.	От 7500	От 8000
Наличие сертификата ФСТЭК	+	+
Класс защищенности	По 5 классу защищенности	По 5 классу защищенности
Уровень контроля НДВ	По 4 уровню контроля	По 4 уровню контроля
Класс автоматизированных систем	До класса 1Г включительно	До класса 1Г включительно
Поддержка ОС семейства Windows	+	+

С точки зрения технического уровня, из числа рассмотренных средств защиты информации от НСД, бесспорным преимуществом ни одно СЗИ от НСД не обладает. Однако необходимо учитывать, удобство использования СЗИ. Исходя из субъективного мнения, использование Dallas Lock 8.0-K является наиболее приятным.

Исходя из всего вышесказанного, в качестве системы защиты персональных данных обрабатываемых в ГИС «Сетевой город. Образование» от несанкционированного доступа в процессе её хранения и обработки, рекомендуется установка программного комплекса средств защиты информации Dallas Lock 8.0-K.

2.1.2. Угроза воздействия вредоносных программ (вирусов)

Программой с потенциально опасными последствиями или вредоносной программой (вирусом) называют некоторую самостоятельную программу (набор инструкций), которая способна выполнять следующие функции:

а) скрывать признаки своего присутствия в программной среде компьютера;

б) обладать способностью к самодублированию, ассоциированию себя с другими программами и (или) переносу своих фрагментов в иные области оперативной или внешней памяти;

в) разрушать (искажать произвольным образом) код программ в оперативной памяти;

г) выполнять без инициирования со стороны пользователя (пользовательской программы в штатном режиме ее выполнения) деструктивные функции (копирования, уничтожения, блокирования и т.п.);

д) сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);

е) искажать произвольным образом, блокировать и (или) подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

Данную угрозу можно устранить установкой антивирусного средства, прошедшего процедуру оценки соответствия требованиям ФСТЭК.

Для того чтобы определиться со средством антивирусной защиты, был проведен сравнительный анализ 3 – х наиболее часто используемых средств антивирусной защиты, приведенный в Таблице 9.

Таблица 9 – Сравнительный анализ средств антивирусной защиты

Критерии сравнения / Средства ЗИ	Kaspersky Endpoint Security 10	Dr.Web Enterprise Security Suite версия 6.0	ESET NOD32 Secure Enterprise Pack
1	2	3	4
Стоимость, руб.	От 500	От 900	От 2725
Наличие сертификата ФСТЭК	+	+	+
Общий уровень обнаружения вредоносного программного обеспечения	98.67%	82.89%	95.97%
Среднее время реакции на новые угрозы, часы	0-2	6-8	4-6
Лечение активного заражения	60%	61%	60%

Продолжение таблицы 9

1	2	3	4
Занимаемая оперативная память в обычном режиме работы, кВ	4500	8338	29124
Время сканирования данных, мин.	28	79	23

По данным таблицы 9 можно сделать вывод о том, что каждое из выбранных средств обладает своими преимуществами. Но для данной информационной системы наиболее выгодным и менее затратным будет установка Kaspersky Endpoint Security 10 для Windows, так как в нашей информационной системе присутствует одно АРМ, то дистрибутив и лицензия от компании Kaspersky будет наиболее выгодна.

Исходя из всего выше сказанного, в качестве антивирусного средства рекомендуется установка Kaspersky Endpoint Security 10 для Windows, выбор антивирусного средства зависит от решения заказчика.

2.1.3. Угроза сканирования, направленная на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.

Сущность процесса реализации угрозы заключается в передаче запросов сетевым службам хостов ИСПДн и анализе ответов от них. Цель – выявление используемых протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, определение активных сетевых сервисов, подбор идентификаторов и паролей пользователей.

Данную угрозу можно устранить установкой средства межсетевого экранирования, прошедшего процедуру оценки соответствия требованиям ФСБ.

На момент проведения предпроектного обследования во всех общеобразовательных учреждениях Челябинской области уже было установлено СКЗИ ViPNet Client 4 (КС2) включающее средство межсетевого экранирования. Так как данное средство имеется ряд преимуществ по сравнению с другими средствами защиты, а

также было предоставлено бесплатно для общеобразовательных учреждений Челябинской области от Регионального центра оценки качества и информатизации образования, рекомендуется использовать СКЗИ ViPNet Client 4, а именно в состав программного комплекса входят:

– драйвер сетевой защиты, взаимодействующий непосредственно с драйвером сетевого интерфейса компьютера осуществляющий контроль и фильтрацию трафика обмена компьютера с внешней сетью;

– сервис управления драйвером сетевой защиты, обеспечивающий функционирование узла в сети ViPNet;

– драйвер шифрования IP-пакетов, осуществляющий шифрование и имитозащиту IP-пакетов;

– приложение ViPNet Client Монитор, предоставляющее пользовательский интерфейс (GUI) для настройки параметров работы ПК ViPNet Client и программный интерфейс для взаимодействия с ПК ViPNet SafeDisk-V;

– сервис регистрации пользователя, обеспечивающий обработку событий аутентификации пользователя ПК ViPNet Client;

– транспортный модуль ViPNet MFTP, реализующий обмен управляющей, адресной и ключевой информацией с программным обеспечением централизованного управления сетью ViPNet (ПО ViPNet Administrator, ПО ViPNet Policy Manager), отправку, прием и маршрутизацию электронных документов (почтовых конвертов), отправку, прием и маршрутизацию электронных документов (почтовых конвертов);

– служба ViPNet Контроль приложений, осуществляющая контроль сетевой активности приложений и позволяющая реализовывать политики доступа приложений в сеть;

– прикладное ПО ViPNet Деловая почта для обмена зашифрованными и подписанными сообщениями;

– криптопровайдер ViPNet CSP, совместимый с MS CryptoAPI, и предоставляющий криптографические функции прикладному ПО, что является необходимым для работы с ГИС «Сетевой город. Образование» в общеобразовательных учреждениях.

2.1.4. Угроза выявления паролей по сети

Цель реализации угрозы состоит в получении НСД путем преодоления парольной защиты. Злоумышленник может реализовывать угрозу с помощью целого ряда методов, таких как простой перебор, перебор с использованием специальных словарей, установка вредоносной программы для перехвата пароля и перехват пакетов (sniffing). В основном для реализации угрозы используются специальные программы, которые пытаются получить доступ хосту путем последовательного подбора паролей. В случае успеха, злоумышленник может создать для себя «проход» для будущего доступа, который будет действовать, даже если на хосте изменить пароль доступа.

Данную угрозу можно минимизировать использованием антивирусного средства, а также средства межсетевого экранирования, прошедшего процедуру оценки соответствия требованиям ФСТЭК и ФСБ.

На основании проведенного анализа средств защиты в пунктах 2.1.2 и 2.1.3 настоящей работы, в качестве антивирусного средства рекомендуется установка Kaspersky Endpoint Security 10 для Windows, а в качестве средства межсетевого экранирования рекомендуется использовать программный комплекс ViPNet Client 4 (КС2).

2.1.5. Угроза типа «Отказ в обслуживании»

Эти угрозы основаны на недостатках сетевого программного обеспечения, его уязвимостях, позволяющих нарушителю создавать условия, когда операционная система оказывается не в состоянии обрабатывать поступающие пакеты.

Могут быть выделены несколько разновидностей таких угроз:

а) скрытый отказ в обслуживании, вызванный привлечением части ресурсов

ИСПДн на обработку пакетов, передаваемых злоумышленником со снижением пропускной способности каналов связи, производительности сетевых устройств, нарушением требований к времени обработки запросов;

б) явный отказ в обслуживании, вызванный исчерпанием ресурсов ИСПДн при обработке пакетов, передаваемых злоумышленником (занятие всей полосы пропускания каналов связи, переполнение очередей запросов на обслуживание), при котором легальные запросы не могут быть переданы через сеть из-за недоступности среды передачи, либо получают отказ в обслуживании ввиду переполнения очередей запросов, дискового пространства памяти и т.д;

в) явный отказ в обслуживании, вызванный нарушением логической связности между техническим средствами ИСПДн при передаче нарушителем управляющих сообщений от имени сетевых устройств, приводящих к изменению маршрутно-адресных данных или идентификационной и аутентификационной информации;

г) явный отказ в обслуживании, вызванный передачей злоумышленником пакетов с нестандартными атрибутами или имеющих длину, превышающую максимально допустимый размер, что может привести к сбою сетевых устройств, участвующих в обработке запросов, при условии наличия ошибок в программах, реализующих протоколы сетевого обмена.

Результатом реализации данной угрозы может стать нарушение работоспособности системы защиты ПДн в ИСПДн, передача с одного адреса такого количества запросов на подключение к техническому средству в составе ИСПДн, которое максимально может «вместить» трафик (направленный «шторм запросов»), что влечет за собой переполнение очереди запросов и отказ одной из сетевых служб или полная остановка ИСПДн из-за невозможности системы заниматься ничем другим, кроме обработки запросов.

Данную угрозу можно устранить установкой средства межсетевого экранирования, прошедшего процедуру оценки соответствия требованиям ФСБ.

На основании проведенного анализа средств защиты в пункте 2.1.3 настоящей работы, в качестве средства межсетевого экранирования рекомендуется использовать программный комплекс ViPNet Client 4 (КС2).

2.1.6. Угроза внедрения по сети вредоносных программ

К вредоносным программам, внедряемым по сети, относятся вирусы, которые для своего распространения активно используют протоколы и возможности локальных и глобальных сетей. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию. «Полноценные» сетевые вирусы при этом обладают еще и возможностью запустить на выполнение свой код на удаленном компьютере или, по крайней мере, «подтолкнуть» пользователя к запуску зараженного файла.

Вредоносными программами, обеспечивающими осуществление НСД, могут быть:

а) программы подбора и вскрытия паролей;

б) программы, реализующие угрозы;

в) программы, демонстрирующие использование недекларированных возможностей программного и программно-аппаратного обеспечения ИСПДн;

г) программы-генераторы компьютерных вирусов;

д) программы, демонстрирующие уязвимости средств защиты информации и др.

Данную угрозу можно устранить установкой антивирусного средства, прошедшего процедуру оценки соответствия требованиям ФСТЭК.

На основании проведенного анализа средств защиты в пункте 2.1.2 настоящей работы, в качестве антивирусного средства рекомендуется установка Kaspersky Endpoint Security 10 для Windows.

2.1.7. Угроза удаленного запуска приложений

Угроза заключается в стремлении запустить на хосте ИСПДн различные предварительно внедренные вредоносные программы: программы-закладки, вирусы,

«сетевые шпионы», основная цель которых - нарушение конфиденциальности, целостности, доступности информации и полный контроль за работой хоста. Кроме того, возможен несанкционированный запуск прикладных программ пользователей для несанкционированного получения необходимых нарушителю данных, для запуска управляемых прикладной программой процессов и др.

Выделяют три подкласса данных угроз:

а) распространение файлов, содержащих несанкционированный исполняемый код;

б) удаленный запуск приложения путем эксплуатации уязвимостей, например, путем переполнения буфера приложений-серверов;

в) удаленный запуск приложения путем использования возможностей удаленного управления системой, предоставляемых скрытыми программными и аппаратными закладками, либо используемыми штатными средствами.

Типовые угрозы первого из указанных подклассов основываются на активизации распространяемых файлов при случайном обращении к ним. Примерами таких файлов могут служить: файлы, содержащие исполняемый код в вид документы, содержащие исполняемый код в виде элементов ActiveX, Java-апплетов, интерпретируемых скриптов (например, тексты на JavaScript); файлы, содержащие исполняемые коды программ. Для распространения файлов могут использоваться службы электронной почты, передачи файлов, сетевой файловой системы.

При угрозах второго подкласса используются недостатки программ, реализующих сетевые сервисы (в частности, отсутствие контроля за переполнением буфера). Настройкой системных регистров иногда удается переключить процессор после прерывания, вызванного переполнением буфера, на исполнение кода, содержащегося за границей буфера. Примером реализации такой угрозы может служить внедрение широко известного «вируса Морриса».

При угрозах третьего подкласса нарушитель использует возможности удаленного управления системой, предоставляемые скрытыми компонентами, например,

«троянскими» программами, либо штатными средствами управления и администрирования компьютерных сетей. В результате их использования удается добиться удаленного контроля над станцией в сети.

Данную угрозу можно минимизировать использованием антивирусного средства, а также средства межсетевого экранирования, прошедшего процедуру оценки соответствия требованиям ФСТЭК и ФСБ.

На основании проведенного анализа средств защиты в пунктах 2.1.2 и 2.1.3 настоящей работы, в качестве антивирусного средства рекомендуется установка Kaspersky Endpoint Security 10 для Windows, а в качестве средства межсетевого экранирования рекомендуется установить программный комплекс ViPNet Client 4 (КС2).

2.2. Вывод по второй главе

В результате выявленных уязвимостей в общеобразовательных учреждениях при их подключении к ГИС «Сетевой город. Образование» приводящих к реализации той или иной угрозы, согласно составленной модели угроз персональных данных при их обработке в ИСПДн «ГИС «Сетевой город. Образование», были определены и рекомендованы мероприятия, препятствующие возникновению неблагоприятных последний от выявленных угроз, а именно:

1. От угрозы доступа к информации, ее модификация и уничтожение лицами, не имеющими прав доступа: предложены организационные меры, а также установка программного комплекса средств защиты информации от несанкционированного доступа Dallas Lock 8.0-K;

2. От угрозы воздействия вредоносных программ (вирусов): предложена установка антивирусного средства Kaspersky Endpoint Security 10 для Windows;

3. От угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.: предложено использование уже имеющего средства межсетевого экранирования программный комплекс ViPNet Client 4 (КС2);

4. От угрозы выявления паролей по сети: предложена установка антивирусного средства Kaspersky Endpoint Security 10 для Windows, а также средства межсетевого экранирования программный комплекс ViPNet Client 4 (КС2).

5. От угрозы типа «Отказ в обслуживании»: предложено использовать средство межсетевого экранирования в составе программного комплекса ViPNet Client 4 (КС2);

6. От угрозы внедрения по сети вредоносных программ: предложена установка антивирусного средства Kaspersky Endpoint Security 10 для Windows;

7. От угрозы удаленного запуска приложений: предложена установка антивирусного средства Kaspersky Endpoint Security 10 для Windows, а также средства межсетевого экранирования программный комплекс ViPNet Client 4 (КС2).

В результате оценки необходимых средств защиты информации для типовой системы защиты ПДн в общеобразовательных учреждениях Челябинской области при их подключении к ГИС «Сетевой город. Образование» было выявлено семь обязательных мероприятий, направленных на предотвращение и минимизацию угроз ПДн в ГИС «Сетевой город. Образование».

3. РАЗРАБОТКА ПРОЕКТА ТИПОВОЙ СИСТЕМЫ ЗАЩИТЫ ПДН В ОБЩЕОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЯХ ЧЕЛЯБИНСКОЙ ОБЛАСТИ ПРИ ИХ ПОДКЛЮЧЕНИИ К ГИС «СЕТЕВОЙ ГОРОД. ОБРАЗОВАНИЕ»

3.1. Описание объекта защиты

Объектом защиты являются ПДн, обрабатываемые в ИСПДн «ГИС «Сетевой город. Образование». Общие, информационные, технические и эксплуатационные характеристики типовой защищаемой ИСПДн приведены в Таблице 11.

Таблица 11 – Общие, информационные, технические и эксплуатационные характеристики защищаемой ИСПДн

№ п/п	Общие, информационные, технические и эксплуатационные характеристики ИС	Описание
I. Информационные характеристики		
1.	Категории обрабатываемых персональных данных	специальные категории ПДн
2.	Типы актуальных угроз	Актуальны угрозы 3-го типа
3.	Количество субъектов	Менее 100000 субъектов
4.	Категории субъектов	Не сотрудники
5.	Необходимость обеспечения уровня защищенности (УЗ)	Необходимо обеспечение 3-го уровня защищенности
6.	Наличие контролируемой зоны (да/нет)	Да
II. Общие характеристики		
7.	Территориальное размещение	Локальная – элементы системы (сетевое оборудование, рабочие станции) расположены в пределах одного здания
8.	Режим обработки данных	Многопользовательский
9.	Разграничение доступа (с/без)	С разграничением доступа к информации
10.	Наличие соединения с сетями общего пользования	Система функционирует в единой сети передачи данных
11.	Наличие подключения к сети Интернет	Рабочие станции системы имеют выход в сеть международного информационного обмена - Интернет
III. Технические характеристики рабочих станций		

Продолжение таблицы 11

№ п/п	Общие, информационные, технические и эксплуатационные характеристики ИС	Описание
12.	Общее количество рабочих станций	1 АРМ
13.	Аппаратное обеспечение	АРМ под управлением операционных систем семейства Microsoft Windows 7 Professional 64bit
14.	Программное обеспечение	Программное обеспечение: 1. Лицензионное системное ПО на базе операционной системы Microsoft Windows 7 Professioal 64bit. 2. Лицензионное прикладное ПО в составе офисного пакета Microsoft Office 2013. 3. Свободно распространяемое ПО.

3.1. Резюме проекта

Данный проект, направлен на создание типовой системы защиты ПДн в общеобразовательных учреждениях Челябинской области при их подключении к ГИС «Сетевой город. Образование» разработан, согласно утвержденному техническому заданию (Приложение Г).

Для того чтобы создать систему защиты ПДн для работы с ГИС «Сетевой город. Образование», был разработан, ряд организационных, инженерно-технических и программно-аппаратных мер. С помощью матрицы ответственности за каждым конкретным этапом работы зафиксированы ответственные лица, а также определены объекты поставки на систему защиты ПДн в общеобразовательных учреждениях Челябинской области при их подключении к ГИС «Сетевой город. Образование». Целью данного проекта является создание типовой системы защиты ПДн в общеобразовательных учреждениях Челябинской области при их подключении к ГИС «Сетевой город. Образование», включающая в себя внедрение программных средств, обеспечивающих защиту от НСД, воздействия вредоносных программ (вирусов), а также от ряда угроз по сети. Все внедренные программные средства прошли процедуру оценки соответствия требованиям ФСБ и ФСТЭК.

3.2. Объекты поставки

3.2.1. Организационно – распорядительная документация

Данным проектом предусмотрено, создание нового пакета организационно – распорядительных документов в области защиты персональных данных для каждого общеобразовательного учреждения (далее - ОУ) Челябинской области, а именно:

– Типовой технический паспорт ИСПДн в ОУ (Приложение Д)

– Типовое описание технологического процесса (Приложение Б)

– Перечень ПДн обрабатываемых в ИСПДн (Приложение В)

– Положение об обработке ПДн в ОУ (Приложение А)

– Техническое задание на создание типовой системы защиты ПДн в общеобразовательных учреждениях Челябинской области (Приложение Г).

Дополненный список организационно – распорядительной документации указан в Приложении 1 к Приложению Г.

3.2.2. Программно-аппаратные и инженерно-технические меры

Для реализации программно-аппаратных и инженерно-технических мер по защите информации необходимо установить:

– программный комплекс средств защиты информации от НСД Dallas Lock 8.0-K;

– средство антивирусной защиты Kaspersky Endpoint Security 10 для Windows;

3.2.3. Обучение персонала

Проектом предусмотрено обучение сотрудников новым требованиям в сфере защиты информации, а также в сфере защиты персональных данных, с четким обоснованием их необходимости и значимости для работы с ГИС «Сетевой город. Образование» по результатам внедрения вновь разработанных организационно – распорядительных документов, предусмотренных пунктом 3.3.1 данной выпускной квалификационной работы.

3.3. Структура разбиения работ

Структура разбиения работ позволяет согласовать план проекта с потребностями заказчика, представленными в виде описаний работ.

Структура декомпозиции работ по созданию системы защиты ПДн общеобразовательных учреждений при их подключении к ГИС «Сетевой город. Образование»:

1. Назначение ответственного за организацию обработки ПДн;
2. Назначение администратора безопасности ИСПДн;
3. Создание комиссии по вопросам обеспечения безопасности ПДн;
4. Определение перечня ИСПДн;
5. Определение перечня, обрабатываемых ПДн;
6. Определение ответственности лиц, участвующих в обработке;
7. Разработка организационно-распорядительных документов по защите персональных данных;
8. Разработка форм согласий субъектов ПДн на обработку ПДн;
9. Определить места хранения материальных носителей персональных данных;
10. Определение круга лиц, участвующих в обработке ПДн;
11. Определение прав разграничения доступа пользователей ИСПДн, необходимых для выполнения должностных обязанностей;
12. Организация информирования и обучения сотрудников о порядке обработки и обеспечения безопасности ПДн;
13. Проведение оценки возможного вреда субъектам, чьи персональные данные обрабатываются в ИСПДн;
14. Определение уровня защищенности ПДн, обрабатываемых в ИСПДн;
15. Анализ актуальности угроз безопасности персональных данных;
16. Определение методов, средств и способов защиты ПДн, выбор помещений для установки аппаратных средств ИСПДн в помещениях, с целью исключения НСД лиц, не допущенных к обработке ПДн;
17. Закупка, установка и настройка средств защиты информации;

18. Контроль защищенности;

19. Обучение пользователей.

3.4. Структурная схема организации проекта

Для точного и своевременного выполнения проекта, необходима скоординированная работа всех задействованных сотрудников. Для этого была определена структурная схема организации проекта. Структурная схема организации представлена на рисунке 1.

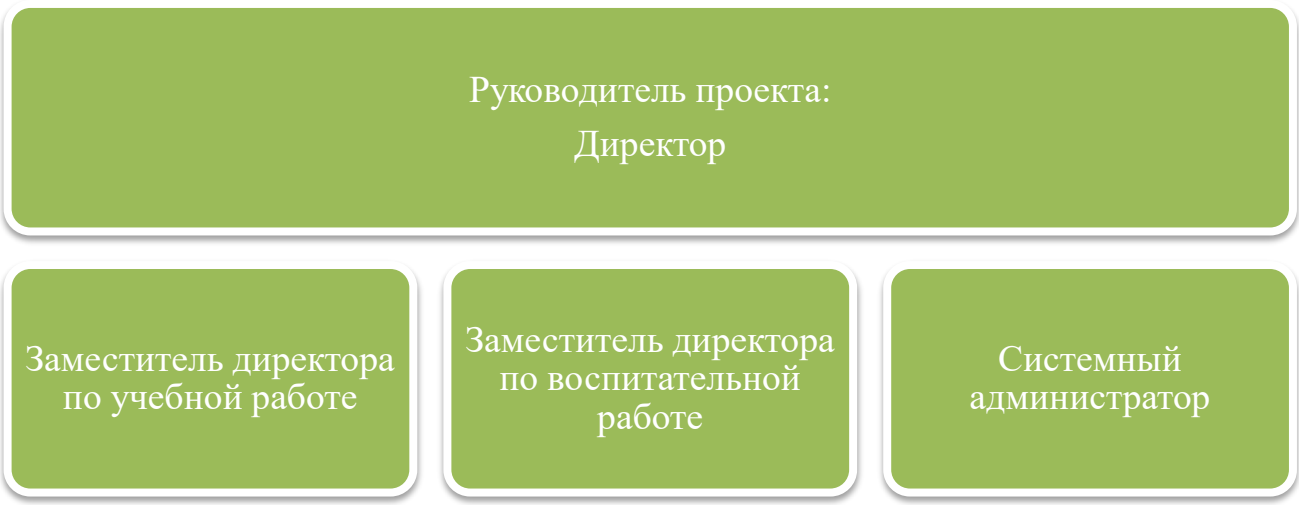


Рисунок 1 – Структурная схема организации проекта по созданию системы защиты ПДн в общеобразовательном учреждении Челябинской области

3.5. Матрица ответственности

Все действия исполнителей по созданию системы защиты ПДн в общеобразовательных учреждениях Челябинской области при их подключении к ГИС «Сетевой город. Образование» делятся на условные группы:

- управление (У);
- исполнение (И);
- контроль (К).

Матрица ответственности представлена в Таблице 12.

Таблица 12 – Матрица ролей пользователей

Исполнитель / Работа	Директор	Заместитель директора по учебной работе	Заместитель директора по воспитательной работе	Системный администратор
1	К/И			
2	К/И			
3	К/И			
4	К	И/К		
5	К	И/К		
6	К	И		
7	К	И		
8	К	И		
9	К	К		И
10	К	К/И		
11	К	К/И		И
12	К	К/И		
13	К/И	К/И	И	
14	К/И	К/И	И	
15	К	К/И		И
16	К	К/И		И
17	К	К		И/У
18	К/У	К		И
19	К	У/К		И

3.6. Диаграмма Ганта и сетевой график

Диаграмма Ганта используется для иллюстрации плана, примерного графика работ по организации системы защиты ПДн в общеобразовательном учреждении Челябинской области. Пример диаграммы Ганта по организации системы защиты ПДн в общеобразовательных учреждениях Челябинской области представлена в Приложении Е.

Сетевой график – это динамическая модель производственного процесса, отражающая технологическую зависимость и последовательность выполнения комплекса работ, увязывающая их свершение во времени с учётом затрат ресурсов и стоимости работ с выделением при этом узких (критических) мест.

Сетевой график является детализированным наглядным представлением обо всех работах проекта, включая временные и ресурсные оценки. Пример сетевого

графика по организации системы защиты ПДн в общеобразовательных учреждениях представлен в Приложении Ж. По итогам составления диаграммы Ганта и сетевого графика можно определить примерные сроки выполнения проекта в общеобразовательных учреждениях. Примерный срок выполнения проекта по организации системы защиты ПДн в общеобразовательном учреждении Челябинской области при его подключении к ГИС «Сетевой город. Образование» составил 31 день.

3.7. Вывод по третьей главе

В ходе выполненных работ был разработан проект по созданию типовой системы защиты ПДн в общеобразовательных учреждениях Челябинской области при их подключении к ГИС «Сетевой город. Образование». Для системы актуальны угрозы 3-го типа. Необходимо обеспечить 3-й уровень защищенности. Целью данного проекта является создание типовой системы защиты ПДн в общеобразовательных учреждениях Челябинской области, включающая в себя внедрение программных средств, обеспечивающих защиту от НСД, воздействия вредоносных программ (вирусов), а также от ряда угроз по сети. Все внедренные программные средства прошли процедуру оценки соответствия требованиям ФСБ и ФСТЭК.

Определены объекты поставки типовой системы защиты ПДн в общеобразовательных учреждениях, включающие организационно – распорядительную документацию, программно – аппаратные и инженерно – технические меры.

Весь проект при реализации в учреждении был разбит на девятнадцать этапов по созданию системы защиты ПДн в общеобразовательных учреждениях Челябинской области. Каждому этапу работы должен быть назначен ответственный за неё и/или исполнитель, определенный в структурной схеме организации проекта. Структура разбиения работ, а также примерные сроки их выполнения наглядно представлены на сетевом графике и диаграмме Ганта.

4. БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ

4.1. Введение

Объектом выпускной квалификационной работы являются общеобразовательные учреждения Челябинской области.

Предметом выпускной квалификационной работы является информация ограниченного доступа, а именного персональные данные сотрудников и учащихся общеобразовательных учреждений обрабатываемые в ИСПДн «ГИС «Сетевой город. Образование», которая состоит из одного АРМ в каждой школе, находящегося в отдельном выделенном помещении.

Целью дипломной работы является создание типовой системы защиты ПДн в общеобразовательных учреждениях Челябинской области при их подключении к ГИС «Сетевой город. Образование».

4.2. Требования к освещению помещения и рабочих мест

В соответствии с СанПиН 2.2.2/2.4.1340-03 «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы» искусственное освещение в помещениях эксплуатации мониторов и ПЭВМ должно осуществляться системой общего равномерного освещения. Освещенность на поверхности стола в зоне размещения рабочего документа должна быть 300-500 люкс (далее – лк). Допускается установка светильников местного освещения для подсветки документов. Местное освещение не должно создавать бликов на поверхности и увеличивать освещенность экрана более 300 лк. Также следует ограничивать отраженную блёскость на рабочих поверхностях (экран, стол, клавиатура и др.) за счет правильного выбора типов светильников и расположения рабочих мест по отношению к источникам естественного и искусственного освещения, при этом яркость бликов на экране ПЭВМ не должна превышать 30 кд/м^2 и яркость потолка не должна превышать 200 кд/м^2.

Для освещения помещений с ПЭВМ рекомендуется применять светильники с зеркальными параболическими решетками, укомплектованными электронными пускорегулирующими аппаратами (ЭПРА). Общее освещение при использовании

люминесцентных светильников следует выполнять в виде сплошных или прерывистых линий светильников, расположенных сбоку от рабочих мест, параллельно линии зрения пользователя и линии оконных проёмов при рядном расположении рабочих мест, оснащенных ПЭВМ с ВДТ. При периметральном расположении компьютеров линии светильников должны располагаться локализовано над рабочим столом ближе к его переднему краю, обращенному к оператору. Коэффициент пульсации не должен превышать 5%.

4.3. Требования к уровню шума

Основным источником шума в помещениях, оборудованных вычислительной техникой, являются работающие принтеры, множительная техника, оборудование для кондиционирования воздуха, а также вентиляторы систем охлаждения и трансформаторы, входящие в состав компьютеров. Шум вредно воздействует не только на органы слуха, но и на весь организм в целом. Повышенный уровень шума приводит к разрушению нервной системы, преждевременному утомлению, ослаблению внимания и памяти, замедлению психических реакций, изменению скорости пульса и дыхания, сердечно – сосудистым заболеваниям.

Уровень шума на рабочих местах, при выполнении основных и вспомогательных производственных работ с использованием ПЭВМ не должен превышать показателей, устанавливаемых нормами СанПиН 2.2.2/2.4.1340-03 предельно допустимых значений для данных видов работ в соответствии с действующими санитарно-эпидемиологическими нормативами [22]. В соответствии с нормами СанПиН 2.2.4.3359-16 нормативным эквивалентным уровнем звука на рабочих местах является 80дБА.

В соответствии с нормами, ограничивающими предельно допустимое звуковое давление для рабочих мест, оснащённых ПЭВМ: шумящее оборудование, уровни шума которого превышают нормативные, должно размещаться вне помещений с ПЭВМ.

4.4. Микроклимат

Для рабочих мест, на которых работа с ПЭВМ является основным видом выполняемых работ и связана с непрерывным эмоциональным напряжением, согласно СанПиН 2.2.2/2.4.1340-03 должны быть обеспечены оптимальные параметры микроклимата для работ категории 1а.

Нормативные требования к показателям микроклимата рабочих мест производственных помещений приведены в СанПиН 2.2.4.3359-16 «Санитарно-эпидемиологические требования к физическим факторам на рабочих местах» [23].

Оптимальные величины параметров микроклимата для категории работ 1а приведены в таблице 13.

Таблица 13 – Оптимальные величины параметров микроклимата для категории работ 1а (СанПиН 2.2.4.3359-16).

Период года	Категория работ по уровням энергозатрат, Вт	Температура воздуха, °С	Температура поверхностей, °С	Относительная влажность воздуха, %	Скорость движения воздуха, м/с
Холодный	1а (до 139)	22−24	21−25	60−40	0,1
Теплый	1а (до 139)	23−25	22−26	60−40	0,1

В соответствии с СанПиН 2.2.2/2.4.1340-03, в помещениях, оборудованных ПЭВМ, должна проводиться ежедневная влажная уборка, а также проветривание после каждого часа работы на ПЭВМ.

4.5. Электробезопасность

По степени опасности поражения электрическим током согласно «Правилам устройства электроустановок» (ПУЭ) рабочее помещение относится к классу помещений с повышенной опасностью, так как имеется возможность одновременного прикосновения человека к имеющим соединения с землей металлоконструкциям здания с одной стороны и металлическим корпусам электрооборудования с другой.

Если физический доступ к токоведущим частям оборудования затруднён, то основной причиной возникновения данного опасного фактора может являться прикосновение к металлическим нетоковедущим частям (например, корпусу ПЭВМ), которые могут оказаться под напряжением в результате повреждения изоляции. В соответствии с правилами электробезопасности, должен осуществляться постоянный контроль состояния электропроводки, предохранительных щитов, шнуров, с помощью которых включаются в электросеть компьютеры, осветительные приборы, другие электроприборы.

Для предотвращения образования и защиты от статического электричества в помещениях с ПЭВМ необходимо использовать аэроионизаторы и увлажнители воздуха. В отделке помещений следует отдавать предпочтение антистатическим материалам. Полы должны иметь антистатическое покрытие.

В соответствии с документом «Правила устройства электроустановок» (ПУЭ) электробезопасность работающих обеспечивается конструкцией электроустановок; техническими способностями и средствами защиты, организационными средствами защиты. Предусмотрены следующие технические способы и средства защиты от поражения электрическим током:

– обеспечение недоступности токоведущих частей, находящихся под напряжением для случайного прикосновения;

– устранение опасности поражения при появлении напряжения на нетоковедущих частях электрооборудования посредствами зануления.

4.6. Пожарная безопасность

В соответствии с федеральным законом от 22 августа 2008 г. № 123-ФЗ «Технический регламент о требованиях пожарной безопасности» пожары классифицируются по виду горючего материала и подразделяются на следующие классы:

– пожары твердых горючих веществ и материалов (A);

– пожары металлов (D);

– пожары горючих веществ и материалов электроустановок, находящихся под напряжением (E)[24].

К опасным факторам пожара, воздействующим на людей и имущество, относятся:

– пламя и искры;

– тепловой поток;

– повышенная температура окружающей среды;

– повышенная концентрация токсичных продуктов горения и термического разложения;

– пониженная концентрация кислорода;

– снижение видимости в дыму.

Здание и сооружения должны быть обеспечены первичными средствами пожаротушения. Они предназначены для использования работниками организаций, личным составом подразделений пожарной охраны и иными лицами в целях борьбы с пожарами и подразделяются на следующие типы:

– переносные и передвижные огнетушители;

– пожарные краны и средства обеспечения их использования;

– пожарный инвентарь;

– покрывала для изоляции очага возгорания.

В соответствии с ГОСТ 12.1.004–91 ССБТ «Пожарная безопасность. Общие требования», возможно применение следующих мероприятий по пожарной безопасности:

– применение средств пожарной сигнализации;

– применение быстродействующих устройств защитного отключения возможных источников возгорания (электрооборудования);

– эвакуация людей:

– должно быть не меньше двух эвакуационных выхода из здания;

– эвакуационные выходы должны располагаться рассредоточено;

– ширина участков путей эвакуации должна быть не менее 1 м, а дверь на путях эвакуации – не менее 0,8 м;

– высота прохода – не менее 2 м;

– разработка мероприятий на случай возникновения пожара.

В начальной стадии пожара для тушения электропроводки (под напряжением до 100 В) допустимо использовать порошковые огнетушители.

Организационные мероприятия, устраняющие причины возникновения пожаров: обучение рабочих и служащих противопожарным правилам, проведение лекций и инструкций.

Технические мероприятия: соблюдение противопожарных правил и норм при устройстве оборудования отопления, вентиляции и т.д.

Мероприятия режимного характера: запрещение курения в не установленных местах, проведения сварочных работ в пожарных помещениях.

Эксплуатационные мероприятия: правильная эксплуатация машин, транспорта, оборудования и правильное содержание зданий, территорий. В общеобразовательных учреждениях для пожаротушения применяются пенные огнетушители.

4.7. Организация рабочего места

Организация рабочего места – это система мероприятия по его планированию, оснащению средствами и предметами труда, размещению их в определенном порядке, обслуживанию рабочего места и его аттестации.

Под оснащением рабочего места понимается совокупность находящихся на нём средств труда: основного технологического и вспомогательного оборудования, технологической и организационной оснастки, средств связи и сигнализации и средств по охране труда и технике безопасности.

Рабочие места с персональными компьютерами по отношению к световым проёмам должны располагаться так, чтобы естественные свет падал сбоку, желательно слева.

Схемы размещения рабочих мест с персональными компьютерами должны учитывать расстояния между рабочими столами с мониторами: расстояние между боковыми поверхностями мониторов не менее 1,2 м, а расстояние между экраном монитора и тыльной частью другого монитора не менее 2,0 м.

Рабочий стол может быть любой конструкции, отвечающей современным требованиям эргономики и позволяющей удобно разместить на рабочей поверхности оборудование с учетом его количества, размеров и характера выполняемой работы. Целесообразно применение столов, имеющих отдельную от основной столешницы специальную рабочую поверхность для размещения клавиатуры.

В соответствии с СанПиН 2.2.2/2.4.1340–03 «Гигиенические требования к персональным электронно-вычислительным машинами и организации работы»:

1) Высота рабочей поверхности стола для взрослых пользователей должна регулироваться в пределах 680 – 800 мм; при отсутствии такой возможности высота рабочей поверхности стола должна составлять 725 мм;

2) Модульными размерами рабочей поверхности стола для ПЭВМ, на основании которых должны рассчитываться конструктивные размеры, следует считать: ширину 800, 1000, 1200 и 1400 мм, глубину 800 и 1000 мм при нерегулируемой его высоте, равной 725 мм;

3) Рабочий стол должен иметь пространство для ног высотой не менее 600 мм, шириной – не менее 500 мм, глубиной на уровне колен – не менее 450 мм и на уровне вытянутых ног – не менее 650 мм;

4) Конструкция рабочего стула должна обеспечивать:

- ширину и глубину поверхности сиденья не менее 400 мм;
- поверхность сиденья с закругленным передним краем;
- регулировку высоты поверхности сиденья в пределах 400 – 550 мм и углов наклона вперед до 15° и назад до 5°;
- высоту опорной поверхности спинки 300 ± 20 мм, ширину – не менее 380 мм и радиус кривизны горизонтальной плоскости – 400 мм;
- регулировку расстояния спинки от переднего края сиденья в пределах 260 – 400 мм;
- стационарные или съемные подлокотники длиной не менее 250 мм и шириной – 50 – 70 мм;

– регулировку подлокотников по высоте над сиденьем в пределах 230 ± 30 мм и внутреннего расстояния между подлокотниками в пределах 250 – 500 мм;

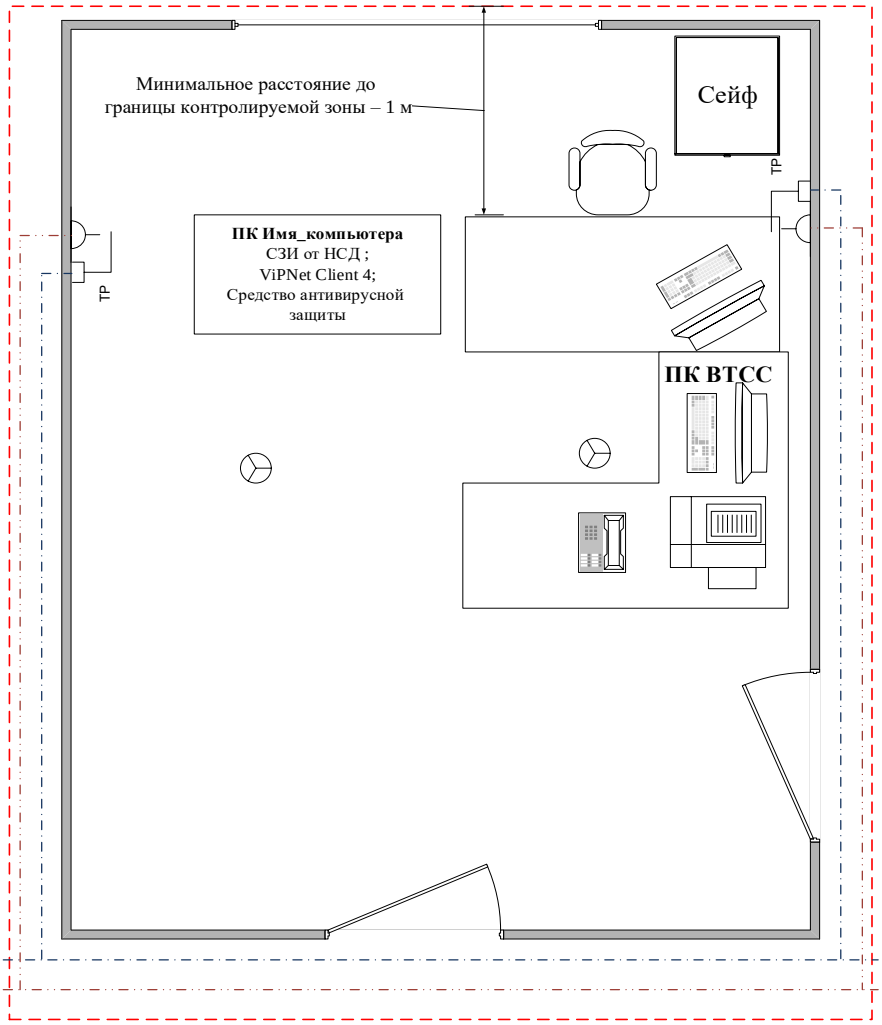
5) Рабочее место пользователя ПЭВМ следует оборудовать подставкой для ног, имеющей ширину не менее 300 мм, глубину не менее 400 мм, регулировку по высоте в пределах до 150 мм и по углу наклона опорной поверхности подставки до 20°. Поверхность подставки должна быть рифленой и иметь по переднему краю бортик высотой 10 мм;

6) Клавиатуру следует располагать на поверхности стола на расстоянии 100 – 300 мм от края, обращенного к пользователю, или на специальной регулируемой по высоте рабочей поверхности, отделенной от основной столешницы.

Организация рабочих мест школ Челябинской области соответствует установленным требованиям.

4.8. Сравнение параметров рабочего места с допустимыми нормами.

Для определения соответствия условий труда требованиям нормативных документов проведем сравнительный анализ требований, установленных к рабочим местам (Таблица 14), оборудованным ПЭВМ и фактических параметров рабочего места. Так как тема выпускной квалификационной работы является типовой системы защиты ПДн, то для сравнения рабочего места с требованиями возьмем АРМ одного из общеобразовательных учреждений Челябинской области. Схема размещения рабочего места приведена на Рисунке 2. Площадь помещения 25м2, оконный проем, шириной 1,8м размещается по центру. В помещении присутствует естественное и искусственное освещение.



Условные обозначения:

ПЭВМ

Телефонный аппарат

Принтер, МФУ

Розетка электрической сети

Телефонная розетка, розетка локальной сети

Датчик пожарной сигнализации

Сеть электропитания

Телефонная/Локальная сеть

Граница контролируемой зоны

Рисунок 2 – Схема рабочего места.

В результате проведенного анализа требований были выявлены общие требования к организации рабочих мест пользователей, требования к помещениям для работы с ПЭВМ, основные требования к освещению на рабочих местах, уровню шума и микроклимату. На основе проведенного анализа было установлено, что условия труда на рабочем месте соответствуют вышеперечисленным требованиям.

Таблица 14 – Сравнение параметров рабочего места с допустимыми нормами.

Нормируемые параметры	Допустимые нормы	Фактические значения
Высота рабочей поверхности стола	от 680 до 800мм, либо 725мм	725мм
Модульные размеры рабочей поверхности стола	Ширина 800, 1000, 1200, 1400мм, глубина 800 и 1000мм	Ширина 1400мм глубина 1000 мм
Ширина и глубина поверхности сиденья	Не менее 400мм	Ширина 600мм Глубина 530мм
Площадь на одно рабочее место	не менее 4,5м2	5,5м2
Падение естественного света	Преимущественно слева	Слева
Освещенность поверхности стола	300-500 лк	350 лк
Уровень звука	80 дБА	60 дБА
Параметры микроклимата (кат. 1а)	Температура воздуха 22-24° С Влажность воздуха 40-60%	Температура 23° С Влажность воздуха 57%

4.9. Вывод по четвертой главе

Был проведен анализ организованных условий труда в помещениях школ, в котором расположен объект информатизации, на соответствие требованиям СанПиН 2.2.4.3359-16 «Санитарно-эпидемиологические требования к физическим факторам на рабочих местах», СанПиН 2.2.2/2.4.1340-03 «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы», персональным электронно-вычислительным машинам и организации работы», ГОСТ Р 12.1.019-2009 ССБТ «Электробезопасность. Общие требования и номенклатура видов защиты», ФЗ № 123 «Технический регламент о требованиях пожарной безопасности» по следующим направлениям:

– микроклимат;

– защита от шума;

– освещение помещения;

– электробезопасность;

– противопожарная безопасность;

– организация рабочего места.

В результате проведенного анализа было установлено, что условия труда в исследуемых школах Челябинской области соответствуют требованиям.

ЗАКЛЮЧЕНИЕ

В ходе выполнения выпускной квалификационной работы было проведено предпроектное обследование общеобразовательных учреждений на основании, которого был составлен типовой паспорт предприятия (Приложение Д). Опираясь на собранные нами сведения, было выявлено, что обрабатываемая информация ограниченного доступа сосредоточена на АРМ подключаемом к ГИС «Сетевой город. Образование». Вследствие этого была построена типовая модель деятельности общеобразовательного учреждения (Приложение З). В рамках проведения информационно – аналитической работы деятельности общеобразовательного учреждения, а также руководствуясь составленной моделью деятельности общеобразовательных учреждений (Приложение З) был выявлен вид защищаемой информации – персональные данные. На основании анализа ИСПДн была составлена типовая модель угроз и уязвимостей безопасности персональных данных при их обработке в ИСПДн. В результате было разработано техническое задание на создание типовой системы защиты ПДн в общеобразовательных учреждениях (Приложение Г).

В результате выявленных уязвимостей в общеобразовательных учреждениях при их подключении к ГИС «Сетевой город. Образование» приводящих к реализации той или иной угрозы, согласно составленной модели угроз, техническому заданию и уязвимостей безопасности персональных данных при их обработке в ИСПДн, были определены обязательные мероприятия, препятствующие возникновению неблагоприятных последний от выявленных угроз, а именно:

1. От угрозы доступа к информации, ее модификация и уничтожение лицами, не имеющими прав доступа: предложены организационные меры, а также установка программного комплекса средств защиты информации от несанкционированного доступа Dallas Lock 8.0-K;

2. От угрозы воздействие вредоносных программ (вирусов): предложена установка антивирусного средства Kaspersky Endpoint Security 10 для Windows;

3. От угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.: предложено

использование средства межсетевого экранирования программный комплекс ViP-Net Client 4 (КС2);

4. От угрозы выявления паролей по сети: предложена установка антивирусного средства Kaspersky Endpoint Security 10 для Windows, а также использование средства межсетевого экранирования программный комплекс ViPNet Client 4 (КС2).

5. От угрозы типа «Отказ в обслуживании»: предложено использование средства межсетевого экранирования программный комплекс ViPNet Client 4 (КС2);

6. От угрозы внедрения по сети вредоносных программ: предложена установка антивирусного средства Kaspersky Endpoint Security 10 для Windows;

7. От угрозы удаленного запуска приложений: предложена установка антивирусного средства Kaspersky Endpoint Security 10 для Windows, а также использование средства межсетевого экранирования программный комплекс ViPNet Client 4 (КС2).

В ходе выполненных работ был разработан проект по созданию типовой системы защиты ПДн в общеобразовательных учреждениях при их подключении к ГИС «Сетевой город. Образование». Для системы актуальны угрозы 3-го типа. Необходимо обеспечить 3-й уровень защищенности. Целью данного проекта является создание типовой системы защиты ПДн в общеобразовательных учреждениях Челябинской области при их подключении к ГИС «Сетевой город. Образование», включающая в себя внедрение программных средств, обеспечивающих защиту от НСД, воздействия вредоносных программ (вирусов), а также от ряда угроз по сети. Все внедренные программные средства прошли процедуру оценки соответствия требованиям ФСБ и ФСТЭК.

Определены объекты поставки типовой системы защиты ПДн в общеобразовательных учреждениях, включающие организационно – распорядительную документацию, программно – аппаратные и инженерно – технические меры.

Весь проект при реализации в учреждении был разбит на девятнадцать этапов по созданию типовой системы защиты ПДн в общеобразовательных учреждениях

при их подключении к ГИС «Сетевой город. Образование». Каждому этапу работы был назначен ответственный за неё и/или исполнитель, определенный в структурной схеме организации проекта. Структура разбиения работ, а также примерные сроки их выполнения наглядно представлены на сетевом графике и диаграмме Ганта.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. «Стратегия развития информационного общества в Российской Федерации» от от 07 февраля 2008 г. № Пр-2012 [Электронный ресурс]. – Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_92004/, свободный. – Загл. с экрана.;

2. ГОСТ 12.1.004–91 ССБТ «Пожарная безопасность. Общие требования» [Электронный ресурс]. – Режим доступа : http://docs.cntd.ru/document/9051953, свободный. – Загл. с экрана.;

3. ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплексность и обозначение документов при создании автоматизированных систем» [Электронный ресурс]. – Режим доступа : http://www.rugost.com/index.php?catid=22&id=91:34201-89&Itemid=53&option=com_content&view=article, свободный. – Загл. с экрана.;

4. ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания» [Электронный ресурс]. – Режим доступа : http://www.rugost.com/index.php?catid=22&id=95:-34601-90----&Itemid=53&option=com_content&view=article, свободный. – Загл. с экрана.;

5. ГОСТ 34.602-1989 «Техническое задание на создание автоматизированной системы» [Электронный ресурс]. – Режим доступа : http://www.rugost.com/index.php?option=com_content&view=article&id=96:gost-34602-89&catid=22&Itemid=53, свободный. – Загл. с экрана.;

6. ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы» [Электронный ресурс]. – Режим доступа : http://www.rugost.com/index.php?option=com_content&view=article&id=96:gost-34602-89&catid=22&Itemid=53, свободный. – Загл. с экрана.;

7. ГОСТ Р 51583-2000 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения» [Электронный ресурс]. – Режим доступа : http://www.iso27000.ru/standarty/gost-r-nacionalnye-

standarty-rossiiskoi-federacii-v-oblasti-zaschity-informacii/gost-r-51583-2000-poryadok-sozdaniya-avtomatizirovannyh-sistem-v-zaschischennom-ispolnenii, свободный. – Загл. с экрана.;

8. ГОСТ Р 51624-2000 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие требования» [Электронный ресурс]. – Режим доступа : http://itsec2012.ru/gosudarstvennyy-standart-rossiyskoy-federacii-gost-r-51624-2000-zashchita-informacii, свободный. – Загл. с экрана.;

9. Конституция Российской Федерации [Электронный ресурс]. – Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_28399/, свободный. – Загл. с экрана.;

10. Постановление Правительства РФ от 01 ноября 2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс]. – Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_137356/, свободный. – Загл. с экрана.;

11. Постановление Правительства РФ от 10.07.2013 г. №582 «Об утверждении Правил размещения на официальном сайте образовательной организации в информационно-телекоммуникационной сети «Интернет» и обновления информации об образовательной организации» [Электронный ресурс]. – Режим доступа : http://base.garant.ru/70413268/, свободный. – Загл. с экрана.;

12. Постановление Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» [Электронный ресурс]. – Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_80028/, свободный. – Загл. с экрана.;

13. Приказ ФСБ России от 10 июля 2014 г. №378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации,

необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» [Электронный ресурс]. – Режим доступа : https://rg.ru/2014/09/17/zashita-dok.html, свободный. – Загл. с экрана.;

14. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс]. – Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_146520/, свободный. – Загл. с экрана.;

15. Распоряжение Правительства РФ от 25.10.2014 г. № 2125-р «Об утверждении Концепции создания единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам» [Электронный ресурс]. – Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_170330/, свободный. – Загл. с экрана.;

16. Руководящий документ ФСТЭК России «Методика определения акту-альных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс]. – Режим доступа : http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380-metodika-opredeleniya-aktualnykh-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-fstek-rossii-2008-god, свободный. – Загл. с экрана.;

17. СанПиН 2.2.2/2.4.1340-03 «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы» [Электронный ресурс]. – Режим доступа : https://rg.ru/2003/06/21/134.html, свободный. – Загл. с экрана.;

18. СанПиН 2.2.4.3359-16 «Санитарно-эпидемиологические требования к физическим факторам на рабочих местах» [Электронный ресурс]. – Режим доступа :

http://www.consultant.ru/document/cons_doc_LAW_203183/, свободный. – Загл. с экрана.;

19. Федеральный закон от 22 августа 2008 г. № 123-ФЗ «Технический регламент о требованиях пожарной безопасности» [Электронный ресурс]. – Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_78699/, свободный. – Загл. с экрана.;

20. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]. – Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61801/, свободный. – Загл. с экрана.;

21. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» [Электронный ресурс]. – Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61801/, свободный. – Загл. с экрана.;

22. ФСБ РФ от 21 января 2008 г. № 149/6/6-622 «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс]. – Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_126991/, свободный. – Загл. с экрана.;

23. ФСТЭК России от 15 февраля 2008 г. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс]. – Режим доступа : http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/379, свободный. – Загл. с экрана.

ПРИЛОЖЕНИЕ А

УТВЕРЖДАЮ

Директор
МБОУ «СОШ»

_____ / /

«26» апреля 2017 г.

УТВЕРЖДАЮ

Заместитель директора
ООО «ИТ Энигма»

_____/М.М. Неверов /

«26» апреля 2017 г.

Описание технологического процесса обработки информации на объекте информатизации – ИСПДн «МБОУ СОШ»

ОТП
Листов: 9

1. Владелец объекта информатизации

муниципальное бюджетное общеобразовательное учреждение «Средняя общеобразовательная» Челябинской области (далее – Учреждение).

2. Расположение объекта информатизации

Челябинская обл.

3. Список используемых сокращений

АРМ	– автоматизированное рабочее место;
ИСПДн	– информационная система персональных данных;
МНИ	– машинные носители информации;
НСД	– несанкционированный доступ;
ОИ	– объект информатизации (вычислительной техники);
ОС	– операционная система;
ПО	– программное обеспечение;
ПК	– программный комплекс;
ПДн	– персональные данные;
СЗИ	– средство защиты информации.
СКЗИ	– средство криптографической защиты информации.
САВЗ	– средство антивирусной защиты

4. Назначение ОИ

Обеспечение защищенного информационного обмена при использовании комплексной автоматизированной информационной системы, объединяющей в единую информационную сеть образовательные организации всех типов и органы управления образованием.

5. Решаемые задачи

– техническое функционирование ИСПДн;

– обеспечение безопасного хранения и использования сведений, содержащихся в ИСПДн;

– обеспечение работоспособности защищенных каналов связи;

– обработка ПДн участников учебно-воспитательного процесса в Учреждении.

6. Расположение ОИ. Организация охраны и контроля доступа

ОИ расположен по адресу, указанному в пункте 2 настоящего Описания. Элементы ОИ размещены в кабинете 38 Учреждения. В здании установлена пожарная сигнализация. Здание охраняется сторожем. В здании имеется «тревожная кнопка», ведется видеонаблюдение. После окончания работы (в нерабочее время) МНИ и документы, содержащие ПДн, хранятся в сейфах / металлических шкафах / шкафах / ящиках рабочих мест. Нахождение сотрудников в кабинете 38 Учреждения во внерабочее время не допускается. Нахождение посетителей в кабинете 38 Учреждения допускается только в рабочее время и только в присутствии сотрудников Учреждения.

7. Состав ИСПДн

В состав ИСПДн «МБОУ СОШ. СГО» входят:

– машинные носители информации (накопители на жестких магнитных дисках (НЖМД), оптические диски, flash-носители);

– АРМ в целом;

– активное и пассивное сетевое оборудование;

– коммуникационные порты системного блока (RJ45, USB-порты);

– файлы (в т.ч. временные и технологические) и каталоги с файлами, содержащие защищаемые сведения;

– распечатанные документы, содержащие защищаемые сведения;

– приводы (устройства чтения/записи) оптических дисков;

– каталоги (файлы) с общесистемным и прикладным программным обеспечением;

– каталоги (файлы) системы защиты информации от несанкционированного доступа (СЗИ от НСД Dallas Lock 8.0-К).

Питание АРМ обеспечивается от сети электропитания 220В. Электропитание здания организовано от трансформаторной подстанции, которая находится за пределами контролируемой зоны. К трансформаторной подстанции подключены сторонние потребители.

Объект информатизации состоит из АРМ, используемого для обработки и хранения ПДн.

Состав, тип, заводские номера оборудования, его размещение, граница контролируемой зоны приведены в Техническом паспорте ИСПДн «МБОУ СОШ. СГО» от 26.04.2017 г.

8. Субъекты ИСПДн

Субъектами доступа в ИСПДн являются:

– администратор безопасности ИСПДн;

– ответственный за обеспечение безопасности ПДн;

– пользователи, работающие в ИСПДн;

– обслуживающий персонал, осуществляющий техническое обслуживание средств вычислительной техники.

9. Используемые программные средства

В качестве штатных средств доступа к информации в ИСПДн предусмотрены:

– стандартные средства операционных систем: Microsoft Windows 7 Professional;

– прикладное программное обеспечение: Microsoft Office Professional Plus 2010, Internet explorer.

Копия лицензионной версии ОС хранится у ответственного лица в Учреждении.

10. Антивирусная защита

Антивирусная защита осуществляется администратором безопасности ИСПДн с применением разрешенных программных средств в соответствии с Инструкцией по организации антивирусной защиты. Полный перечень используемых средств антивирусной защиты представлен в Техническом паспорте ИСПДн «МБОУ СОШ. СГО» от 26.04.2017 г.

Обновление антивирусных баз производится ежедневно автоматически. Полная проверка проводится первого числа каждого месяца (либо при восстановлении работоспособности АРМ в случае пропущенной задачи), быстрая проверка – ежедневно при включении компьютера. Включен постоянный антивирусный контроль.

11. Источники данных

Источниками данных ИСПДн «МБОУ СОШ. СГО» являются:

– сведения, вводимые с клавиатуры;

– персональные данные на отчуждаемых МНИ;

– персональные данные, поступившие по защищенным каналам связи.

12. Обеспечение безопасности информации

В целях защиты информации в ИСПДн «МБОУ СОШ. СГО» установлены средства защиты информации, приведенные в таблице 1.

Таблица 1 – Средства защиты информации

№ п/п	Наименование продукции	Заводской (инвентарный) номер	Сведения о сертификате, знаке соответствия (ЗС)
1	СЗИ от НСД	-	Сертификат соответствия СЗИ
2	Программный комплекс ViPNet Client 4	-	Сертификат соответствия ФСБ России № СФ/515-2907 от 17.06.2016 г, действителен до 29.04.2019 г. Сертификат соответствия ФСБ России № СФ/124-2876 от 30.03.2016 г., действителен до 31.12.2018 г.
3	САВЗ	-	Сертификат соответствия САВЗ

Настройку СЗИ для конкретных пользователей, контроль работы, обновление антивирусных баз, диагностику и устранение неисправностей или сбоев в работе программного или аппаратного обеспечения осуществляет администратор безопасности ИСПДн.

Функции, права, обязанности администратора безопасности ИСПДн, а также порядок ремонта и модернизации регламентируются специально разработанными инструкциями, утвержденными руководителем Учреждения.

Доступ пользователей к работе в ИСПДн «МБОУ СОШ. СГО» осуществляется в строгом соответствии с Приказом «Об утверждении списка пользователей ИСПДн».

Допускается наличие только постоянных пользователей.

Права доступа пользователей к программам, каталогам, файлам определены в документации по разрешительной системе доступа персонала к защищаемым ресурсам и реализованы средствами СЗИ от НСД Dallas Lock 8.0-К.

13. Доступ к информационным ресурсам

13.1 Общая часть

Доступ пользователей ИСПДн «МБОУ СОШ. СГО» (далее – пользователь ИСПДн) к информационным ресурсам определяется на основании Приказа «Об утверждении списка пользователей ИСПДн» и Перечня ПДн, обрабатываемых в ИСПДн, утверждённого руководителем Учреждения.

Права доступа к информационным ресурсам назначаются каждому пользователю ИСПДн на основании разрешительной системы доступа, разрабатываемой ответственным за обеспечение безопасности ПДн.

Разграничение прав доступа пользователей ИСПДн к информационным ресурсам и установление полномочий этим пользователям ИСПДн реализуется ответственным за обеспечение безопасности ПДн средствами СЗИ от НСД Dallas Lock 8.0-К.

Вход в систему осуществляется по уникальному паролю конкретного пользователя ИСПДн (не менее 6 символов). При успешном входе в систему пользователь ИСПДн получает права доступа к устройствам, каталогам, файлам и программам, установленные администратором безопасности ИСПДн.

При увольнении пользователя ИСПДн или переходе в другое подразделение ответственный за обеспечение безопасности ПДн на основании приказа в последний день работы пользователя ИСПДн (или иной день, указанный в приказе), производится удаление учетной записи пользователя ИСПДн и всех его ресурсов (за исключением необходимых для работы других пользователей ИСПДн).

13.2 Начало сеанса работы

Перед началом сеанса работы пользователь включает АРМ и проходит процедуру аутентификации в СКЗИ ViPNet Client 4 и в СЗИ от НСД Dallas Lock 8.0-К.

В процессе аутентификации в СКЗИ ViPNet Client 4 пользователь использует свой личный пароль. Смена личного пароля производится при смене пользователя.

В процессе аутентификации в СЗИ от НСД Dallas Lock 8.0-К пользователь использует свой личный пароль. Смена личного пароля производится не реже 1 раза в 180 дней. Контроль данного процесса осуществляется администратором безопасности ИСПДн.

13.3 Регистрация пользователей и назначение прав доступа

Регистрация пользователей и назначение прав доступа производится администратором безопасности ИСПДн. Пользователем ИСПДн является сотрудник Учреждения.

Зарегистрированный пользователь ИСПДн устанавливает свой личный пароль или получает пароль у ответственного за обеспечение безопасности ПДн.

Права доступа устанавливаются пользователю средствами ОС и СЗИ от НСД Dallas Lock 8.0-К в соответствии с разрешительной системой доступа, разработанной администратором безопасности ИСПДн.

Удаление пользователя выполняется однократно при необходимости выведения сотрудника из числа пользователей ИСПДн.

13.4 Работа с файлами документов, внесение изменений, хранение, передача

Документы, содержащие ПДн, предоставляются в Учреждение участниками учебно-воспитательного процесса. Сотрудники Учреждения вносят ПДн в ИСПДн и обрабатывают полученные данные в целях, указанных в Положении об обработке

персональных данных. ПДн участников учебно-воспитательного процесса заносятся в комплексную автоматизированную информационную систему, объединяющую в единую информационную сеть образовательные организации всех типов и органы управления образованием, доступ к которой осуществляется по защищенному каналу связи посредством СКЗИ ViPNet Client 4. Участники учебно-воспитательного процесса имеют удаленный доступ к просмотру своих ПДн.

Для обмена электронными письмами, содержащими ПДн, используется программа ViPNet Деловая почта, входящая в состав ПК ViPNet Client 4. Этой возможностью могут воспользоваться только те пользователи сети ViPNet, у которых есть связь друг с другом.

13.5 Уничтожение файлов, содержащих персональные данные

Удаление ПДн и временных файлов производится штатными средствами ОС при включенном режиме затирания данных СЗИ от НСД Dallas Lock 8.0-К.

При установке СЗИ от НСД Dallas Lock 8.0-К активирована функция затирания данных с применением не менее одного цикла затирания.

Запрещается удалять информацию с машинных носителей информации иными программными средствами.

13.6 Завершение сеанса работы

По завершении работы пользователь выполняет штатную процедуру завершения работы в ОС, выключает рабочую станцию и помещает отчуждаемые МНИ и документы, содержащие ПДн, в сейф / металлический шкаф / шкаф / ящик рабочего места.

СОСТАВИЛИ

Наименование организации	Должность	Фамилия, Имя, Отчество	Подпись	Дата
ООО «ИТ Энигма»	Ведущий специалист по защите информации			

СОГЛАСОВАНО

Наименование организации	Должность	Фамилия, Имя, Отчество	Подпись	Дата
ООО «ИТ Энигма»	Заместитель директора по информационной безопасности			

УТВЕРЖДАЮ

Директор
МБОУ «СОШ»

_____
(подпись)

«____»_____
2017 г.

ПРИЛОЖЕНИЕ Б

ПОЛОЖЕНИЕ

ОБ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Содержание

ОБЩИЕ ПОЛОЖЕНИЯ

1.1.Настоящее Положение по обработке персональных данных (далее – Положение) муниципального бюджетного общеобразовательного учреждения «Средняя общеобразовательная школа» Челябинской области (далее – Учреждения) разработано в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Гражданским кодексом Российской Федерации, Федеральным законом «Об информации, информационных технологиях и о защите информации» №149 от 27.07.2006, Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ и устанавливает порядок приема, учета, сбора, поиска, обработки, накопления и хранения документов, содержащих сведения, отнесенные к персональным данным субъектов Учреждения.

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

1.3.Учреждение является оператором персональных данных лиц, указанных в пункте 2.1 настоящего Положения. На основании договора Учреждение может поручать обработку персональных данных третьим лицам. Существенным условием договора об оказании услуг по обработке персональных данных является обязанность обеспечения этими лицами конфиденциальности и безопасности персональных данных субъектов.

1.4.Настоящее Положение вступает в силу с момента его утверждения руководителем Учреждения и действует бессрочно, до замены его новым Положением.

1.5.Все изменения в Положение вносятся приказом руководителя.

ОСНОВНЫЕ ПОНЯТИЯ И СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1 Под субъектами персональных данных подразумеваются следующие лица:

– лица (далее – сотрудники), имеющие трудовые отношения с Учреждением;

– участники учебно-воспитательного процесса.

2.2 Обработка персональных данных осуществляется:

– без использования средств автоматизации;

– с использованием средств информационной системы персональных данных «МБОУ СОШ. СГО».

2.3 Состав персональных данных, обрабатываемых в информационной системе персональных данных (далее – ИСПДн) Учреждения, определяется «Перечнем персональных данных, обрабатываемых в информационных системах персональных данных».

2.4.Под обработкой персональных данных понимаются действия (операции) с персональными данными, включающие:

- сбор, хранение, уточнение (обновление, изменение);
- систематизацию, накопление;
- использование, распространение (в том числе передачу);
- обезличивание, блокирование, уничтожение.

2.5.Обработка персональных данных сотрудника осуществляется для обеспечения соблюдения законов и иных нормативных правовых актов, содействия сотруднику в трудоустройстве, обучении, продвижении по работе, обеспечения личной безопасности работника, контроля качества и количества выполняемой работы и обеспечения сохранности имущества, оплаты труда, пользования льготами, предусмотренными законодательством РФ и актами Учреждения, а также для осуществления основной деятельности Учреждения.

2.6.Обработка персональных данных участников учебно-воспитательного процесса, осуществляется с целью осуществления учебно-воспитательной деятельности Учреждения.

2.7.Комплекс документов, сопровождающий процесс оформления трудовых отношений работника в Учреждении при его приеме, переводе и увольнении.

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

– паспорт или иной документ, удостоверяющий личность;

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

– страховое свидетельство государственного пенсионного страхования;

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

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

– свидетельство о присвоении ИНН (при его наличии у работника).

2.7.2. При оформлении работника в Учреждение, главным специалистом заполняется унифицированная форма Т-2 «Личная карточка работника», в которой отражаются следующие анкетные и биографические данные работника:

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

– сведения о воинском учете;

– данные о приеме на работу;

В дальнейшем в личную карточку вносятся:

– сведения о переводах на другую работу;

– сведения об аттестации;

– сведения о повышении квалификации;

– сведения о профессиональной переподготовке;

– сведения о наградах (поощрениях), почетных званиях;

– сведения об отпусках;

– сведения о социальных гарантиях;

– сведения о месте жительства и контактных телефонах.

2.7.3. В Учреждении создаются и хранятся следующие группы документов, содержащие персональные данные работников в единичном или сводном виде:

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

2.7.3.2. Организационно-распорядительная документация Учреждения (Положения, должностные инструкции работников, приказы руководителя); документы по планированию, учету, анализу и отчетности в части работы с персоналом Учреждения.

2.8. Комплекс документов, сопровождающий учебно-воспитательный процесс.

2.8.1. Информация, представляемая участниками учебно-воспитательного процесса в Учреждение, должна иметь документальную форму.

2.8.2. В дальнейшем в ИСПДн Учреждения обрабатываются персональные данные согласно «Перечню персональных данных, обрабатываемых в информационных системах персональных данных».

СБОР, ОБРАБОТКА И ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1 Порядок получения персональных данных.

3.1.1. Все персональные данные сотрудников Учреждения и прочих физических лиц следует получать у них самих. Если персональные данные возможно получить только у третьей стороны, то субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Должностное лицо Учреждения должно сообщить о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа субъекта дать письменное согласие на их получение.

3.1.2. Учреждение не имеет права получать и обрабатывать персональные данные сотрудников и прочих физических лиц об их расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни.

3.1.3. Учреждение вправе обрабатывать персональные данные физических лиц только с их письменного согласия.

3.1.4. Согласие субъекта не требуется в следующих случаях:

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

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

– обработка персональных данных необходима для предоставления государственной или муниципальной услуги в соответствии с Федеральным законом от 27 июля 2010 года № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», для обеспечения предоставления такой услуги, для регистрации субъекта персональных данных на едином портале государственных и муниципальных услуг;

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

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

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

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

3.2 Порядок обработки, передачи и хранения персональных данных.

3.2.1. Субъект предоставляет должностному лицу Учреждения достоверные сведения о себе. Должностное лицо проверяет достоверность сведений, сверяя данные, предоставленные субъектом, с имеющимися у субъекта документами.

3.2.2. Руководитель и сотрудники Учреждения (операторы) при обработке персональных данных сотрудника должны соблюдать следующие общие требования:

3.2.2.1.Обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, осуществления учебно-воспитательной деятельности, содействия сотрудникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности сотрудников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

3.2.2.2.При определении объема и содержания обрабатываемых персональных данных оператор должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ и иными федеральными законами.

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

3.2.2.4.Защита персональных данных субъекта от неправомерного их использования или утраты обеспечивается Учреждением как оператором за счет своих средств в порядке, установленном федеральным законом.

3.2.2.5.Сотрудники и их представители должны быть ознакомлены под подпись с документами Учреждения, устанавливающими порядок обработки персональных данных, а также об их правах и обязанностях в этой области.

3.2.2.6.Во всех случаях отказ субъекта от своих прав на сохранение и защиту персональных данных недействителен.

3.2.3. Все меры конфиденциальности при сборе, обработке и хранении персональных данных распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

3.2.4. Информация о субъектах ПДн, зафиксированная в автоматизированных системах и на бумажных носителях должна храниться в условиях, исключающих несанкционированный доступ к ней.

ПЕРЕДАЧА И ХРАНЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1 При передаче персональных данных субъекта Учреждение должно соблюдать следующие требования:

4.1.1. Не сообщать персональные данные субъекта третьей стороне без письменного согласия субъекта, за исключением случаев, когда это необходимо в

целях предупреждения угрозы жизни и здоровью сотрудника, а также в случаях, установленных федеральным законом.

4.1.2. Предупредить лиц, получивших персональные данные субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получившие персональные данные субъекта, обязаны соблюдать режим конфиденциальности. Данное Положение не распространяется на обмен персональными данными субъектов в порядке, установленном федеральными законами.

4.1.3. Осуществлять передачу персональных данных субъектов в пределах Учреждения в соответствии с настоящим Положением.

4.1.4. Разрешать доступ к персональным данным субъектов только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные участников учебно-воспитательного процесса, которые необходимы для выполнения конкретной функции.

4.1.5. Передавать персональные данные представителям в порядке, установленном законодательством Российской Федерации, и ограничивать эту информацию только теми персональными данными субъекта, которые необходимы для выполнения указанными представителями их функции.

4.1.6. Не допускается отвечать на вопросы, связанные с передачей персональной информации, по телефону или факсу.

4.2 Хранение и использование персональных данных:

4.2.1. Персональные данные субъектов обрабатываются и хранятся на бумажных носителях в помещениях Учреждения и на учтённых машинных носителях в соответствии с Инструкцией по учёту машинных носителей.

4.2.2. Персональные данные субъектов могут быть получены, проходить дальнейшую обработку и передаваться на хранение, как на бумажных носителях, так и в электронном виде.

4.2.3. ПДн субъектов должны удаляться из Информационных систем персональных данных Учреждения по достижении целей обработки, при этом допускается хранить документы, содержащие ПДн, срок хранения которых регулирует законодательством РФ.

4.3 При получении персональных данных не от субъекта (за исключением случаев, если персональные данные были предоставлены Учреждению на основании федерального закона или если персональные данные являются общедоступными), Учреждение до начала обработки таких персональных данных обязано предоставить субъекту следующую информацию:

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

– цель обработки персональных данных и ее правовое основание;

– предполагаемые пользователи персональных данных;

– установленные Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» права субъекта персональных данных.

ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ

5.1Перечень лиц, имеющих право доступа к персональным данным, определяется «Списком лиц, которым необходим доступ к персональным данным», утверждённым руководителем Учреждения.

5.2Субъект персональных данных, чьи персональные данные обрабатываются в информационной системе Учреждения, имеет право:

5.2.1. Получать доступ к своим персональным данным и знакомиться с ними, включая право на безвозмездное получение копий любой записи, содержащей персональные данные этого субъекта.

5.2.2. Требовать от Учреждения уточнения, исключения или исправления неполных, неверных, устаревших, недостоверных, незаконно полученных или не являющих необходимыми для оператора персональных данных.

5.2.3. Получать от оператора:

– сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;

– перечень обрабатываемых персональных данных и источник их получения;

– сроки обработки персональных данных, в том числе сроки их хранения;

– сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

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

5.2.5. Копировать и делать выписки персональных данных субъекта разрешается исключительно в служебных целях с письменного разрешения руководителя Учреждения.

5.3Передача информации третьей стороне возможна только при письменном согласии субъекта персональных данных.

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

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

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

6.3. Защита персональных данных представляет собой жестко регламентированный и динамически технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности компании.

6.4. Защита персональных данных от неправомерного их использования или утраты должна быть обеспечена оператором за счет его средств в порядке, установленном федеральным законом.

6.5. «Внутренняя защита».

6.5.1. Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами. Регламентация доступа персонала к конфиденциальным сведениям, документам входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководителем и сотрудниками Учреждения.

6.5.2. Для обеспечения внутренней защиты персональных данных необходимо соблюдать ряд мер:

– ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;

– строгое избирательное и обоснованное распределение документов и информации между работниками;

– рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;

– знание работником требований нормативно-методических документов по защите информации и сохранении тайны;

– наличие необходимых условий в помещении для работы с конфиденциальными сведениями;

– определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;

– организация порядка уничтожения информации;

– своевременное выявление нарушения требований разрешительной системы доступа сотрудникам Учреждения

– воспитательная и разъяснительная работа с сотрудниками по предупреждению утраты ценных сведений при работе с конфиденциальными документами.

6.6. «Внешняя защита».

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

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

6.6.3. Для обеспечения внешней защиты персональных данных необходимо соблюдать ряд мер:

– порядок приема, учета и контроля деятельности посетителей;

– пропускной режим организации;

– учет и порядок выдачи удостоверений;

– технические средства охраны, сигнализации;

– порядок охраны территории, зданий, помещений, транспортных средств;

– требования к защите информации при интервьюировании и собеседованиях.

6.7. Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных.

6.8. По возможности персональные данные обезличиваются.

6.9. Кроме мер защиты персональных данных, установленных законодательством, работодатели, работники и их представители могут вырабатывать совместные меры защиты персональных данных.

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

7.1.Сотрудники Учреждения, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с федеральными законами.

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

Приложение: на 1 л. в 1.экз.

Окончание Приложения Б

ПРИЛОЖЕНИЕ № 1

к Положению от

_____

ЛИСТ ОЗНАКОМЛЕНИЯ

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

ПРИЛОЖЕНИЕ В

УТВЕРЖДАЮ

Директор
МБОУ «СОШ»

_____
(подпись)

«_ __ _»__ _____ 2017 г.

ПЕРЕЧЕНЬ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ МБОУ «СОШ»

ПЕРЕЧЕНЬ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ МБОУ «СОШ»

№	Персональные данные	Субъекты ПДн	Наименование ИСПДн, где допускается обработка ПДн	Место хранения
1	2	3	4	5
1	**Обрабатываются иные категории ПДн менее чем 100 000 субъектов ПДн, не являющихся сотрудниками оператора**			
1.1	Школы: ФИО учащегося, паспортные данные учащегося, сведения об успеваемости, сведения о посещении центров дополнительного образования, ФИО родителей (законных представителей) учащегося, паспортные данные родителей (законных представителей) учащегося, контактные данные родителей (законных представителей) учащегося, адрес мест жительства и регистрации; ФИО сотрудников, паспортные данные, сведения об образовании и трудовой деятельности, контактные данные, адрес мест жительства и регистрации.	Участники учебно-воспитательного процесса	«МБОУ СОШ. СГО»	ПК Kab40_PC1, 2 этаж, кабинет 38

Председатель комиссии:

_____ подпись _____ расшифровка

Члены комиссии:

_____ подпись _____ расшифровка

_____ подпись _____ расшифровка

_____ подпись _____ расшифровка

«__» _____ 2017 г.

Окончание Приложения В

ПРИЛОЖЕНИЕ Г

УТВЕРЖДАЮ

Должность
руководителя организации

_____ И.О. Фамилия

«___»_____ 2018 г.

УТВЕРЖДАЮ

Заместитель директора
ООО «ИТ Энигма»

_____ М.М. Неверов

«___»_____ 2018 г.

Система защиты персональных данных информационной системы персональных данных

«МОУ СОШ»

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

Листов: 22

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Полное наименование и обозначение системы: Система защиты персональных данных государственной информационной системы персональных данных «Сетевой город. Образование».

1.2. Сокращенное наименование системы: СЗПДн.

1.3. Заказчик: Общеобразовательное учреждение.

1.4. Исполнитель: ООО «ИТ Энигма».

1.5. Сроки начала и окончания работ: сроки начала и окончания работ определяются договором между Заказчиком и Исполнителем.

1.6. Порядок оформления и предъявления Заказчику результатов работ определяется на основании действующих стандартов и договорных документов между Заказчиком и Исполнителем.

1.7. При разработке ТЗ использовались следующие нормативно-технические документы и методические материалы:

а) Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

б) Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

в) Постановление Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

г) Постановление Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

д) Приказ ФСТЭК России 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»;

е) Приказ Гостехкомиссии России от 30 августа 2002 г. № 282 «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)»;

ж) Приказ Федеральной службы по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия от 28 апреля 2008 г. № 154 «Об утверждении Положения о ведении реестра операторов, осуществляющих обработку персональных данных»;

з) Руководящий документ ФСТЭК России «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных»;

и) Руководящий документ ФСТЭК России «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных»;

к) Руководящий документ ФСБ России «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации»;

л) Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

м) Руководящий документ Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»;

н) Руководящий документ 50-34.698-90 «Автоматизированные системы. Требования к содержанию документов»;

о) ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания»;

п) ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплексность и обозначение документов при создании автоматизированных систем»;

р) ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения».

2. НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1 Назначение системы защиты персональных данных (далее - СЗПДн)

2.1.1 Назначением СЗПДн является защита персональных данных (далее - ПДн), обрабатываемых техническими средствами, от хищения, утраты, утечки, уничтожения, искажения (в том числе нарушения целостности), подделки и блокирования доступа за счёт комплексного использования организационных, программных, программно-аппаратных средств и мер защиты.

2.1.2 Объектом защиты СЗПДн является ИСПДн, описание которой приведено в разделе 3 настоящего ТЗ.

2.1 Цели создания СЗПДн

2.1.2 Целями создания СЗПДн являются:

а) реализация мер по защите ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных;

б) приведение ИСПДн в соответствие требованиям законодательства России в области защиты персональных данных.

2.1.3 В результате создания СЗПДн должно быть обеспечено:

а) соответствие требованиям для обеспечения 3-го уровня защищенности персональных данных при их обработке в ИСПДн;

б) нейтрализация актуальных угроз безопасности, определенных в Модели угроз безопасности персональных данных при их обработке в информационной системе персональных данных «ГИС «Сетевой город. Образование»».

2.2.3 Критерии оценки достижения поставленных целей по созданию СЗПДн приведены в Таблице 1. Цели создания системы признаются достигнутыми в случае, если достигнуты указанные в таблице значения всех показателей.

Таблица 1 – критерии оценки достижения поставленных целей по созданию СЗПДн

№ п/п	Наименование показателя	Критерий оценки	Значения показателя
1.	Степень нейтрализации угроз безопасности информации, обрабатываемой ИСПДн, признанных актуальными по результатам моделирования угроз	Разрабатываемая частная модель угроз и модель нарушителя безопасности персональных данных государственной информационной системы персональных данных	Система должна обеспечивать нейтрализацию всех угроз безопасности информации, обрабатываемой в ИСПДн, признанных актуальными по результатам моделирования угроз
2.	Применение сертифицированных средств защиты информации	«Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденные приказом ФСТЭК России от 11.02.2013 № 17	Для обеспечения защиты информации, содержащейся в ИСПДн, должны применяться средства защиты информации, прошедшие процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения

№ п/п	Наименование показателя	Критерий оценки	Значения показателя
			безопасности информации
3.	Степень выполнения требований по защите информации, предъявляемых к ИСПДн соответствующего класса защищенности (определяется Заказчиком)	«Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденные приказом ФСТЭК России от 11.02.2013 № 17	Система обеспечения безопасности информации должна обеспечивать выполнение требований по защите информации, соответствующих документально закрепленному классу защищенности
4.	Степень выполнения требований по обеспечению соответствующего уровня защищенности персональных данных, обрабатываемых в ИСПДн (определяется Заказчиком)	Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденные постановлением Правительства РФ от 01.11.2012 № 1119	Система защиты информации должна обеспечивать выполнение требований по обеспечению документально закрепленного требуемого уровня защищенности персональных данных
5.	Степень выполнения требований к классам применяемых средств защиты информации	Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденные приказом ФСТЭК России от 11.02.2013 № 17	Должны применяться средства защиты информации от несанкционированного доступа, средства межсетевого экранирования, средства анализа защищенности информации и средства антивирусной защиты класса, соответствующего документально закрепленному классу защищенности информационной системы

3. ХАРАКТЕРИСТИКА ОБЪЕКТА ЗАЩИТЫ

3.1 Объектом защиты являются ПДн, обрабатываемые в ИСПДн «ГИС «Сетевой город. Образование»». Общие, информационные, технические и эксплуатационные характеристики защищаемой ИСПДн приведены в Таблице 2.

Таблица №2 – Общие, информационные, технические и эксплуатационные характеристики защищаемой ИСПДн

№ п/п	Общие, информационные, технические и эксплуатационные характеристики ИС	Описание
I. Информационные характеристики		
1.	Категории обрабатываемых персональных данных	специальные категории ПДн
2.	Типы актуальных угроз	Актуальны угрозы 3-го типа
3.	Количество субъектов	Менее 100000 субъектов
4.	Категории субъектов	Не сотрудники
5.	Необходимость обеспечения уровня защищенности (УЗ)	Необходимо обеспечение 3-го уровня защищенности
6.	Наличие контролируемой зоны (да/нет)	Да
II. Общие характеристики		
7.	Территориальное размещение	Локальная – элементы системы (сетевое оборудование, рабочие станции) расположены в пределах одного здания
8.	Режим обработки данных	Многопользовательский
9.	Разграничение доступа (с/без)	С разграничением доступа к информации
10.	Наличие соединения с сетями общего пользования	Система функционирует в единой сети передачи данных
11.	Наличие подключения к сети Интернет	Рабочие станции системы имеют выход в сеть международного информационного обмена - Интернет
IV. Технические характеристики рабочих станций		
12.	Общее количество рабочих станций	1 АРМ

№ п/п	Общие, информационные, технические и эксплуатационные характеристики ИС	Описание
13.	Аппаратное обеспечение	АРМ под управлением операционных систем семейства Microsoft Windows 7 Professional 64bit
14.	Программное обеспечение	Программное обеспечение: 4. Лицензионное системное ПО на базе операционной системы Microsoft Windows 7 Professioal 64bit. 5. Лицензионное прикладное ПО в составе офисного пакета Microsoft Office 2013. 6. Свободно распространяемое ПО.

1.

7. ТРЕБОВАНИЯ К СЗПДН

4.1 Требования к СЗПДн в целом

4.1.1 Требования к структуре и функционированию

4.1.1.1 В состав СЗПДн должны входить следующие подсистемы:

а) Подсистема управления доступом;

б) Подсистема регистрации и учета;

в) Подсистема обеспечения целостности;

г) Подсистема межсетевого экранирования;

д) Подсистема защиты каналов передачи данных;

е) Подсистема антивирусной защиты;

ж) Подсистема контроля (анализа) защищенности информации.

4.1.1.2 Структура СЗПДн может изменяться и уточняться по результатам разработки Модели угроз на предпроектной стадии с учетом обоснования необходимых изменений в ТЗ.

4.1.1.3 Подсистема управления доступом. Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа

к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль соблюдения этих правил.

4.1.1.4 Подсистема регистрации и учета. Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

4.1.1.5 Подсистема обеспечения целостности. Меры по обеспечению целостности информационной системы и информации должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащейся в ней информации, а также возможность восстановления информационной системы и содержащейся в ней информации.

4.1.1.6 Подсистема антивирусной защиты. Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

4.1.1.7 Подсистема межсетевого экранирования. Меры по межсетевому экранированию должны обеспечивать безопасность внутренней (защищаемой) сети и полный контроль над внешними подключениями и сеансами связи.

4.1.1.8 Подсистема защиты каналов передачи данных. Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных.

4.1.1.9 Подсистема контроля (анализа) защищенности информации. Меры по контролю (анализу) защищенности информации должны обеспечивать

контроль уровня защищенности информации, содержащейся в информационной системе, путем проведения мероприятий по анализу защищенности информационной системы и тестированию ее системы защиты информации.

4.1.2 Требования к численности и квалификации персонала СЗПДн, режиму его работы

4.1.2.1 Квалификация и численность персонала должна быть достаточной для осуществления им настройки общесистемных и сетевых сервисов СЗПДн и настройки СЗИ СЗПДн.

4.1.2.2 Персонал СЗПДн должен осуществлять обслуживание и эксплуатацию СЗПДн по рабочим дням в рабочее время, с возможностью выхода в нерабочее время для проведения сервисного обслуживания или восстановления работоспособности элементов СЗПДн.

4.1.3 Показатели назначения

4.1.3.1 Системно-технические решения СЗПДн должны обеспечить минимизацию вероятности реализации угроз, описанных в Модели угроз для данной ИСПДн.

4.1.3.2 Экономический эффект от создания СЗПДн должен проявляться в снижении вероятной величины материального и морального ущерба по отношению к субъектам и оператору ПДн.

4.1.4 Требования к надежности

4.1.4.1 Должна быть обеспечена возможность резервного копирования конфигураций и журналов регистрации событий компонентов ИСПДн.

4.1.5 Требования безопасности

4.1.5.1 Конструкция используемого оборудования должна обеспечивать защиту эксплуатирующего персонала от поражения электрическим током.

4.1.5.2 Размещение оборудования на штатных местах должно обеспечивать его безопасное обслуживание и эксплуатацию.

4.1.5.3 Все средства защиты информации, используемые в составе СЗПДн, должны пройти процедуру оценки соответствия в установленном порядке, либо иметь действующие сертификаты соответствия требованиям по безопасности информации ФСТЭК России и ФСБ России в пределах их компетенций.

4.1.6 Требования к эргономике и технической эстетике

Автоматизированные рабочие места СЗПДн должны обеспечивать возможность непрерывной работы сотрудников в течение рабочего времени в соответствии с требованиями постановления Главного государственного санитарного врача РФ от 3 июня 2003 г. № 118 «О введении в действие санитарно-эпидемиологических правил и нормативов СанПиН 2.2.2/2.4.1340-03» с изменениями от 25 апреля 2007 г.

Разрабатываемая система защиты информации не должна вносить значительных задержек в работу пользователей ИСПДн.

Программные и программно-аппаратные средства защиты информации должны обладать интуитивно-понятным интерфейсом управления, иметь документацию на русском языке.

Регламент работы пользователей в части СЗИ, а также порядок реагирования на события информационной безопасности должны быть описаны в эксплуатационной документации на СЗИ.

При работе СЗИ пользователь должен быть предупрежден о работе защитных механизмов и о возникающих событиях информационной безопасности.

4.1.7 Требования к транспортабельности для подвижных систем

4.1.7.1 Должны быть предусмотрены следующие виды технического обслуживания: оперативное обслуживание, профилактические работы.

4.1.7.2 Оперативное обслуживание должно предусматривать ежедневный контроль функционирования аппаратно-технических средств. Оперативное обслуживание не должно нарушать выполнения функций СЗПДн в целом.

4.1.7.3 Профилактическое обслуживание должно предусматривать периодическую проверку и обслуживание составных частей СЗПДн, для которых такое обслуживание предусмотрено эксплуатационной документацией.

4.1.7.4 Объем и порядок выполнения технического обслуживания технических и программных средств СЗПДн должны определяться эксплуатационной документацией.

4.1.7.5 Физический доступ неуполномоченных лиц к сетевому и серверному оборудованию должен быть ограничен.

4.1.7.6 Требования к эксплуатации, техническому обслуживанию, ремонту и хранению могут уточняться на этапе проектирования СЗПДн.

4.1.8 Требования по сохранности информации при авариях

4.1.8.1 Сохранность информации при авариях в СЗПДн должна обеспечиваться методом резервного копирования;

4.1.8.2 Решения по обеспечению сохранности информации в СЗПДн при авариях должны быть разработаны на стадии проектирования СЗПДн.

4.1.9 Требования к защите от влияния внешних воздействий

4.1.9.1 Защита ИСПДн от влияния внешних воздействий должна осуществляться в рамках общих организационно-технических мероприятий по обеспечению безопасности и физической защите на объектах Заказчика.

4.1.10 Требования к патентной чистоте

4.1.10.1 При создании СЗПДн должны соблюдаться положения законодательных актов Российской Федерации по соблюдению авторских прав и защите специальных знаков.

4.1.10.2 При поставке программного обеспечения должны быть выполнены требования части IV Гражданского Кодекса Российской Федерации, а также международные патентные соглашения.

4.1.11 Требования по стандартизации и унификации

4.1.11.1 Решения по использованию технических средств и ПО в СЗПДн должны использовать однотипные компоненты в целях обеспечения снижения расходов на обслуживание и ремонт, взаимозаменяемости используемых компонентов, удобства эксплуатации.

4.1.11.2 Должна обеспечиваться совместимость технических средств и ПО СЗПДн с техническими средствами и ПО, используемыми в ИСПДн «ГИС «Сетевой город. Образование»».

4.1.11.3 При применении технических средств и ПО особое внимание должно быть уделено унификации программных и аппаратных решений. Предпочтение должно отдаваться использованию готовых, проверенных на практике решений.

4.2 Требования к функциям, выполняемым СЗПДн

4.2.1 Требования к подсистеме управления доступом

а) должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в операционную систему ИСПДн «ГИС «Сетевой город. Образование»» по паролю условно-постоянного действия, длиной не менее шести буквенно-цифровых символов.

4.2.2 Требования к подсистеме регистрации и учета

а) должна осуществляться регистрация входа (выхода) субъекта доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения ИСПДн «ГИС «Сетевой город. Образование»». В параметрах регистрации указываются дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;

б) должен проводиться учет всех защищаемых носителей информации с помощью их любой маркировки и с занесением учетных данных в журнал (учетную карточку).

4.2.3 Требования к подсистеме обеспечения целостности

а) должна быть обеспечена целостность программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность программных средств проверя-

ется при загрузке системы по наличию имен (идентификаторов) компонентов системы защиты персональных данных, целостность программной среды обеспечивается отсутствием в информационной системе средств разработки и отладки программ;

б) должна осуществляться физическая охрана ИСПДн «ГИС «Сетевой город. Образование»» (устройств и носителей информации), предусматривающая контроль доступа в помещения ИСПДн «ГИС «Сетевой город. Образование»» посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения ИСПДн «ГИС «Сетевой город. Образование»» и хранилище носителей информации;

в) должны быть в наличии средства восстановления СЗПДн, предусматривающие ведение двух копий программных средств защиты информации, их периодическое обновление и контроль.

4.2.4 Требования к подсистеме антивирусной защиты

а) в ИСПДн «ГИС «Сетевой город. Образование»» должны использоваться сертифицированные средства антивирусной защиты.

4.2.5 Требования к подсистеме межсетевого экранирования

а) средства межсетевого экранирования должны осуществлять контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

4.2.6 Требования к подсистеме защиты каналов передачи данных

а) средства защиты каналов передачи данных должны обеспечивать контроль содержания информации, передаваемой из информационной системы, а также обеспечивать подлинность сетевых соединений, в том числе для защиты от подмены сетевых устройств и сервисов.

4.2.7 Требования к подсистеме контроля (анализа) защищенности информации

а) средства контроля (анализа) защищенности информации должны обеспечивать контроль уровня защищенности информации, содержащейся в информационной системе, путем проведения мероприятий по анализу защищенности информационной системы и тестированию ее системы защиты информации.

б) в ИСПДн используются организационные меры контроля (анализа) защищенности информации.

4.3 Требования к видам обеспечения

4.3.1 Требования к программному обеспечению

4.3.1.1 Выбор программных средств защиты должен проводиться с учетом средств защиты, эксплуатируемых у Заказчика.

4.3.1.2 Средства защиты информации, входящие в состав СЗПДн, должны быть сертифицированы на соответствие требованиям руководящих документов ФСТЭК и ФСБ России.

4.3.1.3 При создании СЗПДн должно использоваться только лицензионное общее и специальное программное обеспечение, и операционные системы.

4.3.1.4 Требования к программному обеспечению, используемому для защиты информации в ИСПДн «ГИС «Сетевой город. Образование»» (средств защиты информации, в том числе и встроенных в общесистемное и прикладное ПО) в части необходимости обеспечения контроля отсутствия в нем недекларированных возможностей (НДВ) должны быть определены в ТЗ.

4.3.2 Требования к техническому обеспечению

4.3.2.1 Выбор аппаратных (программно-аппаратных) средств защиты должен проводиться с учетом средств защиты, эксплуатируемых у Заказчика.

4.3.3 Требования к организационному обеспечению

4.3.3.1 Мониторы АРМ должны располагаться таким образом, чтобы препятствовать возможности несанкционированного визуального съема информации с них.

4.3.3.2 Должна осуществляться физическая охрана устройств и носителей информации ИСПДн «ГИС «Сетевой город. Образование»», предусматривающая:

а) контроль доступа в помещения ИСПДн «ГИС «Сетевой город. Образование»» посторонних лиц;

б) наличие надежных препятствий для несанкционированного проникновения в помещение ИСПДн «ГИС «Сетевой город. Образование»» и хранилище носителей информации, особенно в нерабочее время.

4.3.3.3 Организационное обеспечение ИСПДн должно быть достаточным для эффективного выполнения персоналом возложенных на него обязанностей при осуществлении автоматизированных и связанных с ними неавтоматизированных функций системы.

4.3.3.4 Заказчиком должны быть определены должностные лица, ответственные за:

а) обработку ПДн в ИСПДн;

б) администрирование элементов ИСПДн;

в) обеспечение безопасности ПДн в ИСПДн.

4.3.3.5 К работе в ИСПДн должны допускаться сотрудники, имеющие навыки работы на персональном компьютере, ознакомленные с правилами эксплуатации и прошедшие обучение с работой в ИСПДн.

5. СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО СОЗДАНИЮ СЗПДН

5.1 Проектирование СЗПДн, поставка оборудования, монтаж оборудования

5.1.1 Проектирование СЗПДн:

Исполнитель должен выполнить работы по разработке технического проекта СЗПДн.

На стадии обследование ИСПДн:

а) уточняется перечень ПДн, подлежащих защите;

б) уточняется информация о категориях и составе ПДн, обрабатываемых автоматизированными и неавтоматизированными способами;

в) проводится анализ состава ПДн в ИСПДн, собирается информация о защищенности ПДн;

г) уточняются условия расположения объекта защиты относительно границ контролируемой зоны;

д) уточняются конфигурация и топология ИСПДн и систем связи в целом и их компонентов, физические, функциональные и технологические связи как внутри этих систем, так и с другими системами различного уровня и назначения;

е) уточняются состав технических средств и систем, предполагаемых к использованию в СЗПДн, условия их расположения, общесистемные и прикладные программные средства;

ж) уточняются режимы обработки информации в ИСПДн в целом и в отдельных ее компонентах;

з) для ИСПДн производится анализ собранной информации об угрозах и их показателях для разработки Модели угроз;

и) уточняется класс защищенности ИСПДн;

к) уточняется уровень защищенности ИСПДн;

л) разрабатывается Модель угроз для ИСПДн на основе методических рекомендаций ФСТЭК России;

м) уточняется степень участия сотрудников в обработке информации, характер их взаимодействия между собой и со службой ИБ.

Также разрабатывается пакет организационно-распорядительной документации на ИСПДн (Приложение №1).

5.1.2 Поставка оборудования:

Все поставляемое оборудование должно пройти процедуру оценки соответствия требованиям по безопасности информации и иметь сертификат ФСТЭК России и ФСБ России (в соответствии с требованиями нормативно-методических документов).

5.1.3 Монтаж оборудования

Если в процессе выполнения работ по монтажу оборудования возникают какие-либо нештатные ситуации, а также ситуации, которые могут повлечь приостановление вышеуказанных работ, Исполнитель совместно с Заказчиком принимают все необходимые меры по устранению и ликвидации причин, которые привели к таким ситуациям.

5.2 Передача прав на использование программного обеспечения, входящего в состав СЗПДн

Все программное обеспечение, права на которые передаются Заказчику, должно пройти процедуру оценки соответствия требованиям по безопасности информации и иметь сертификат ФСТЭК России или ФСБ России (в соответствии с требованиями нормативно-методических документов).

5.3 Пусконаладочные работы, опытная эксплуатация СЗПДн, аттестация ИСПДн по требованиям безопасности информации

5.3.1 Пусконаладочные работы

Должен быть проведен анализ защищенности сетевых сегментов ИСПДн (в пределах ЛВС Заказчика) с использованием средств анализа защищенности.

Если в процессе выполнения пусконаладочных работ СЗПДн возникают какие-либо нештатные ситуации, а также ситуации, которые могут повлечь приостановление вышеуказанных работ, Исполнитель совместно с Заказчиком принимают все возможные меры по устранению и ликвидации причин, которые привели к таким ситуациям.

5.3.2 Опытная эксплуатация

Опытная эксплуатация включает в себя комплексную проверку готовности СЗПДн. Опытная эксплуатация имеет своей целью проверку алгоритмов, отладку

работы СЗПДн и технологического процесса обработки данных при использовании СЗПДн.

По окончании опытной эксплуатации возможна доработка СЗПДн.

В случае необходимости проводится обучение персонала Заказчика использованию СЗИ, применяемых в ИСПДн.

6. ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ

6.1 Контроль и приемка работ должны осуществляться на основании заключенного договора.

6.2 Содержание отчетных материалов согласуется на уровне специалистов Заказчика и специалистов Исполнителя данного вида работ в соответствии с заключенным договором. Исполнитель работ должен быть заранее проинформирован Заказчиком о порядке и сроках согласования отчетных материалов, перечне вопросов, которые подлежат согласованию, составе согласующих подразделений и организаций и степени их компетенции при согласовании тех или иных разделов отчетной документации.

6.3 В случае необходимости может быть проведена защита предлагаемых решений в процессе технического совещания специалистов Исполнителя и Заказчика.

6.4 Настоящее ТЗ может быть уточнено или изменено в процессе работы. Уточнения и изменения ТЗ производятся по согласованию сторон. Оформление изменений осуществляется выпуском дополнений, которые являются неотъемлемой частью настоящего ТЗ.

6.5 Согласование и утверждение изменений производится в том же порядке, что и согласование и утверждение ТЗ.

6.6 Замечания по отчетным материалам должны быть представлены Исполнителю с техническим обоснованием в письменной форме.

6.7 Сроки приемки работ определяются календарным планом, согласованным в договоре с Заказчиком.

6.8 Прием и сдача проводимых работ осуществляются совместно Исполнителем и Заказчиком на основании заключенного договора.

7 ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

7.1 Виды, комплектность и содержание документов в части должны учитывать требования ГОСТ 34.201-89 и РД 50-34.698.

7.2 Комплект проектных материалов предоставляется Заказчику в электронном виде и на твердой копии. Вся разрабатываемая проектная документация должна быть выполнена на русском языке.

8. ИСТОЧНИКИ РАЗРАБОТКИ

8.1 При разработке проектных решений необходимо руководствоваться официальными документами фирм-производителей применяемых аппаратных средств и программного обеспечения, документами третьих сторон, осуществляющих тестирование и эксплуатацию решений.

8.2 Проектные решения должны обеспечивать соблюдение нормативно-правовых актов, согласно п.1.7 настоящего ТЗ и иных нормативно-правовых актов.

Продолжение Приложения Г

Приложение №1

К Техническому заданию

Перечень организационно-распорядительной документации

№ Наименование документа
01 Приказ о создании комиссии по приведению ИСПДн
02 Приказ о назначении администратора безопасности
03 Приказ о назначении ответственного
04 Инструкция администратора безопасности
05 Инструкция ответственного за обеспечение безопасности
06 Акт определения уровня защищенности ПДн в ИСПДн
07 Приказ об утверждении списка лиц
08 Инструкция пользователя ИСПДн
09 Перечень персональных данных
10 Положение об обработке ПДн
11 Положение по неавтоматизированной обработке ПДн
12 Политика обработки ПДн
13 Инструкция по организации антивирусной защиты
14 Инструкция по организации парольной защиты
16 Инструкция по физической охране
17 Приказ об утверждения плана мероприятий защите ПДн
18 Приказ об утверждении мест хранения материальных носителей
19 Инструкция по учету машинных носителей
20 Журнал учета машинных носителей ПДн
21 Акт об уничтожении ПДн
22 Журнал учета обращений граждан
23 Инструкция по проведению внутренних проверок
24 Положение об уничтожении
25 Согласие субъекта на обработку ПДн не сотрудники
25 Согласие субъекта на обработку ПДн сотрудники
26 Приказ об установлении границ контролируемой зоны
27 Рекомендации по заполнению Уведомления об обработке

СОСТАВИЛИ

Наименование организации	Должность	Фамилия, Имя, Отчество	Подпись	Дата
ООО «ИТ Энигма»	Специалист по защите информации			

СОГЛАСОВАНО

Наименование организации	Должность	Фамилия, Имя, Отчество	Подпись	Дата
ООО «ИТ Энигма»	Заместитель директора по информационной безопасности			

ПРИЛОЖЕНИЕ Д

УТВЕРЖДАЮ

Директор
МБОУ «СОШ»

_____ /

_____ 2018 г.

УТВЕРЖДАЮ

Заместитель директора
ООО «ИТ Энигма»

_____/ М.М. Неверов

/

_____ 2018 г.

ТЕХНИЧЕСКИЙ ПАСПОРТ

информационной системы персональных данных

«МБОУ СОШ. СГО»

Листов: 8

1 Общие сведения об ИСПДн

Оператор ИСПДн: муниципальное бюджетное общеобразовательное учреждение «Средняя общеобразовательная школа» Челябинской области.

Наименование ИСПДн: «МБОУ СОШ. СГО».

Расположение ИСПДн: Адрес.

Уровень защищенности ПДн в ИСПДн: 3-й уровень защищенности.

2 Состав оборудования ИСПДн

Перечень основных технических средств и систем (далее – ОТСС), входящих в состав информационной системы персональных данных (далее – ИСПДн), представлен в таблице 1.

Таблица 1 – Перечень ОТСС, входящих в состав ИСПДн

№ п/п	Вид оборудования	Тип (модель)	Учетный (заводской) номер
Имя компьютера, этаж, кабинет			
1	Системный блок	-	-
2	Монитор	-	-
3	Клавиатура	-	-
4	Манипулятор (мышь)	-	-

Расположение ОТСС и сетей электропитания указано в приложении А.

Перечень вспомогательных технических средств и сетей (далее – ВТСС), входящих в состав ИСПДн, представлен в таблице 2.

Таблица 2 – Перечень ВТСС, входящих в состав ИСПДн

№ п/п	Вид оборудования	Тип	Учетный (заводской) номер
Имя компьютера, этаж, кабинет			
1	ВТСС в комплекте		
2	МФУ	-	-
3	Телефонный аппарат	-	-
4	Извещатель пожарный	-	-
5	Извещатель пожарный	-	-

Расположение ВТСС и сетей электропитания указано в приложении А.

Схема расположения границы контролируемой зоны указана в приложении А.

Состав средств защиты информации, установленных на объекте, представлен в таблице 3.

Таблица 3 – Состав средств защиты информации, установленных на объекте

№ п/п	Наименование СЗИ	Заводской номер (серийный)	Примечание
	Имя компьютера, этаж, кабинет		
1	СЗИ от НСД	-	-
2	ПК ViPNet Client 4	-	-
3	Средство антивирусной защиты	-	-

Состав используемых в ИСПДн программных средств представлен в таблице 4.

Таблица 4 – Состав используемых в ИСПДн программных средств

№ п/п	Наименование программного средства	Версия	Серийный номер (номер лицензии)
Имя компьютера, этаж, кабинет			
1	Общесистемное ПО:		
1.1	Microsoft Windows (версия)	-	-
2	Прикладное ПО:		
2.1	Microsoft Office / OpenOffice	-	-
2.2	Браузер	-	-

3 Сведения о соответствии ОТСС объекта ВТ требованиям по безопасности информации

3.1 Сведения о сертификатах на ОТСС объекта

№ п/п	Наименование установленных СЗИ	№ сертификата и кем выдан	Дата выдачи	Срок окончания действия сертификата
1	ViPNet Client 4	Сертификат соответствия ФСБ России № СФ/515-2907	17.06.2016 г	29.04.2019 г.
		Сертификат соответствия ФСБ России № СФ/124-2876	30.03.2016 г.	31.12.2018 г.
2	СЗИ от НСД	Сертификат соответствия СЗИ		
3	Средство антивирусной защиты (САВЗ)	Сертификат соответствия САВЗ		

3.2 Сведения об аттестации объекта ВТ на соответствие требованиям по безопасности информации

Кем выдан аттестат	Дата выдачи	Срок действия аттестата

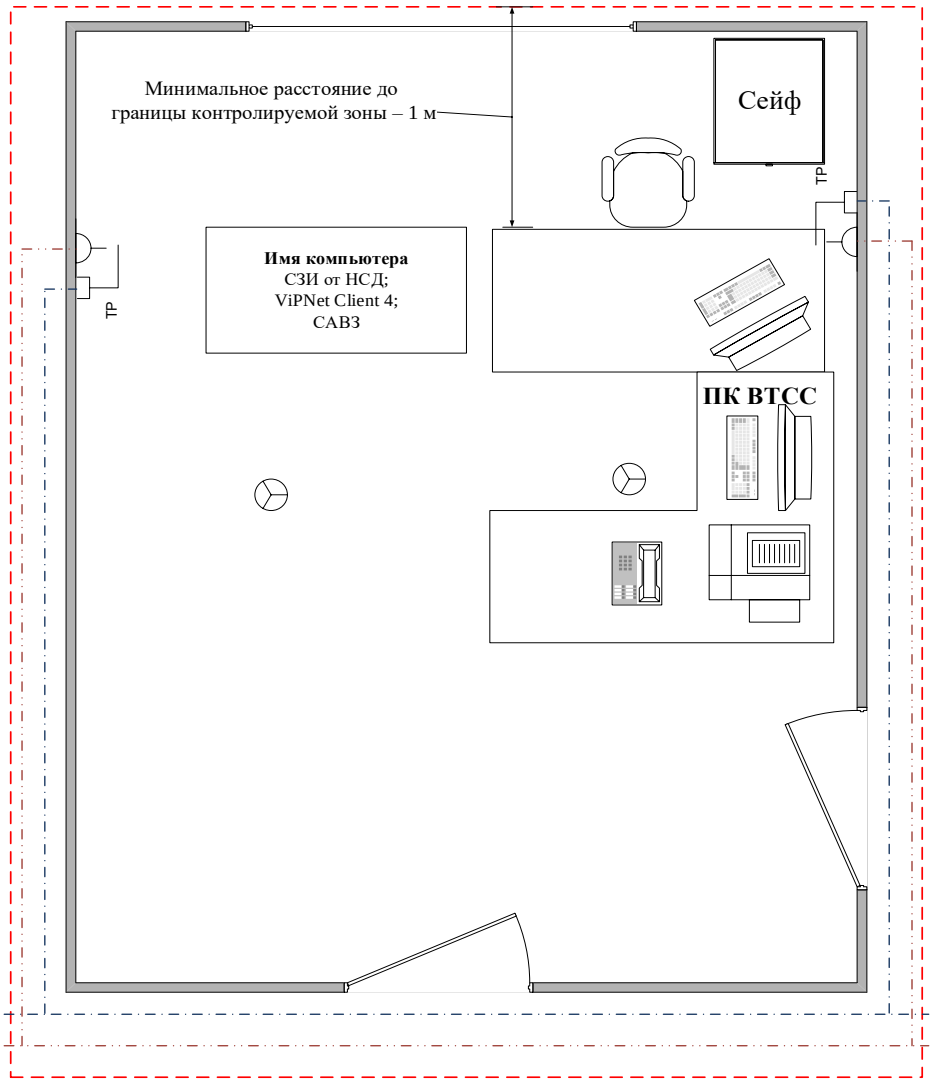
4 Учет проведения регламентных проверок

№ п/п	Наименование организации, проводившей проверку	Дата проведения проверки	Номер Протокола	Примечание

5 Лист регистрации изменений

Порядковый № и дата введения изменений	Наименование документа, фиксирующего изменения	№ замененных (исправленных) листов	ФИО и подпись лица, внесшего изменения

Приложение А. Схема размещения и расположения ОТСС и ВТСС в кабинете



Условные обозначения:

ПЭВМ

Телефонный аппарат

Принтер, МФУ

Розетка электрической сети

Телефонная розетка, розетка локальной сети

Датчик пожарной сигнализации

Сеть электропитания

Телефонная/Локальная сеть

Граница контролируемой зоны

СОСТАВИЛИ

Наименование организации	Должность	Фамилия, Имя, Отчество	Подпись	Дата
ООО «ИТ Энигма»	Ведущий специалист по защите информации			

СОГЛАСОВАНО

Наименование организации	Должность	Фамилия, Имя, Отчество	Подпись	Дата
ООО «ИТ Энигма»	Заместитель директора по информационной безопасности			

ПРИЛОЖЕНИЕ Е

Диаграмма Ганта

Для построения диаграммы Ганта определим перечень поставленных задач и их сроки (с учетом выходных дней).

Таблица 1 – Перечень работ и сроков

№ п/п	Мероприятие	Длительность. дни	Дата начала
1	Назначение ответственного за организацию обработки ПДн	1	26.04.2017
2	Назначение администратора безопасности ИСПДн	1	27.04.2017
3	Создание комиссии по вопросам обеспечения безопасности ПДн	1	28.04.2017
4	Определение перечня ИСПДн	1	01.05.2017
5	Определение перечня, обрабатываемых ПДн	1	02.05.2017
6	Определение ответственности лиц, участвующих в обработке	2	04.05.2017
7	Разработка организационно-распорядительных документов по защите персональных данных	3	08.05.2017
8	Разработка форм согласий субъектов ПДн на обработку ПДн	1	11.05.2017
9	Определить места хранения материальных носителей персональных данных	1	12.05.2017
10	Определение круга лиц, участвующих в обработке ПДн	1	15.05.2017
11	Определение прав разграничения доступа пользователей ИСПДн, необходимых для выполнения должностных обязанностей	2	16.05.2017
12	Организация информирования и обучения сотрудников о порядке обработки и обеспечения безопасности ПДн	4	18.05.2017
13	Проведение оценки возможного вреда субъектам, чьи персональные данные обрабатываются в ИСПДн	1	24.05.2017
14	Определение класса защищенности ГИС и уровня защищенности ПДн, обрабатываемых в ИСПДн (ГИС)	1	25.05.2017

№ п/п	Мероприятие	Длительность. дни	Дата начала
15	Анализ актуальности угроз безопасности персональных данных	3	26.05.2017
16	Определение методов, средств и способов защиты ПДн, выбор помещений для установки аппаратных средств ИСПДн в помещениях, с целью исключения НСД лиц, не допущенных к обработке ПДн	3	31.05.2017
17	Закупка, установка и настройка средств защиты информации	2	05.06.2017
18	Контроль защищенности	1	07.06.2017
19	Обучение пользователей	1	08.06.2017

На основе этих данных мы можем построить диаграмму Ганта, представленную на Рисунке 1.

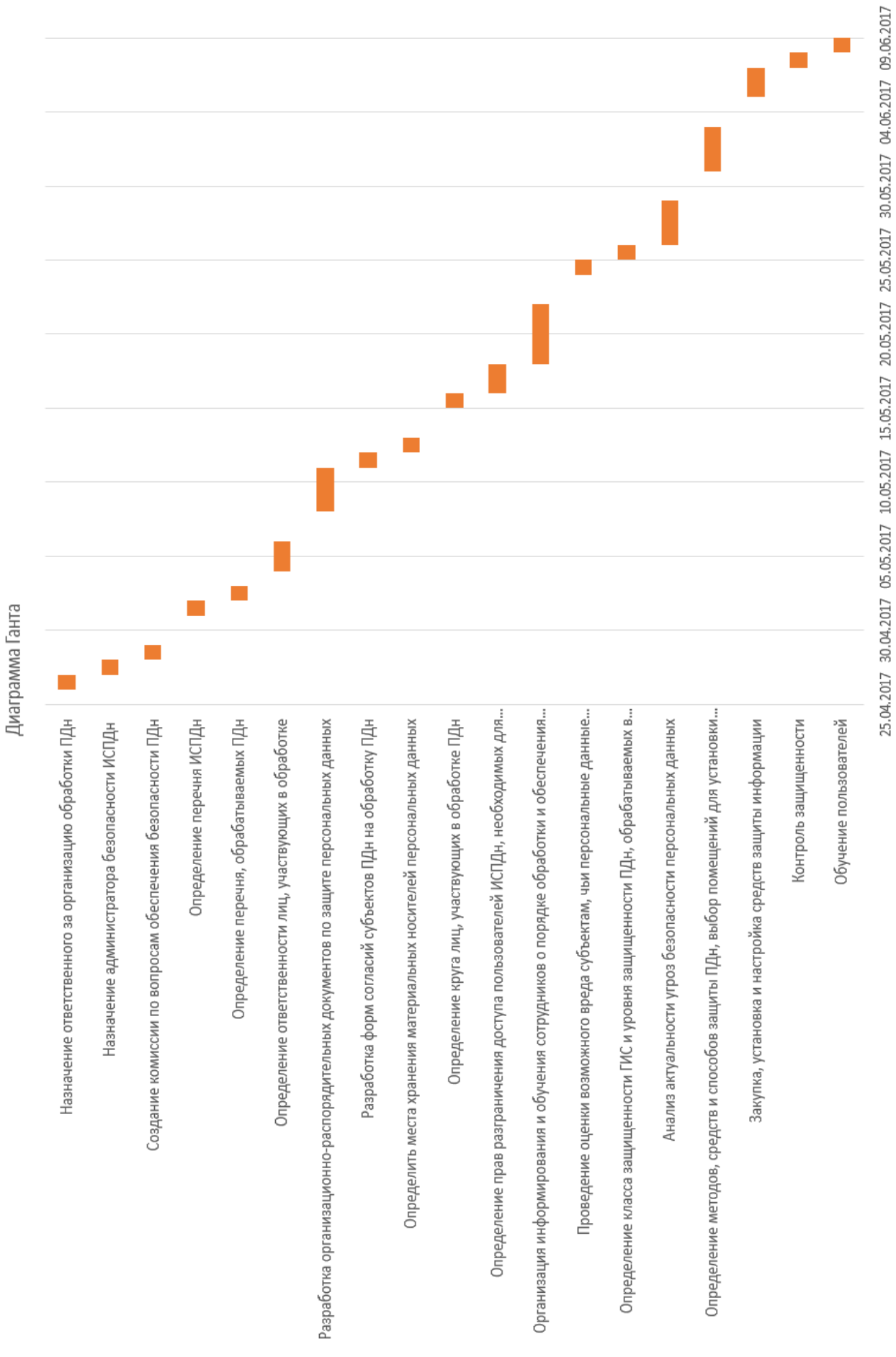


Диаграмма Ганта
Назначение ответственного за организацию обработки ПДн
Назначение администратора безопасности ИСПДн
Создание комиссии по вопросам обеспечения безопасности ПДн
Определение перечня ИСПДн
Определение перечня, обрабатываемых ПДн
Определение ответственности лиц, участвующих в обработке
Разработка организационно-распорядительных документов по защите персональных данных
Разработка форм согласий субъектов ПДн на обработку ПДн
Определить места хранения материальных носителей персональных данных
Определение круга лиц, участвующих в обработке ПДн
Определение прав разграничения доступа пользователей ИСПДн, необходимых для...
Организация информирования и обучения сотрудников о порядке обработки и обеспечения...
Проведение оценки возможного вреда субъектам, чьи персональные данные...
Определение класса защищенности ГИС и уровня защищенности ПДн, обрабатываемых в...
Анализ актуальности угроз безопасности персональных данных
Определение методов, средств и способов защиты ПДн, выбор помещений для установки...
Закупка, установка и настройка средств защиты информации
Контроль защищенности
Обучение пользователей
25.04.2017
30.04.2017
05.05.2017
10.05.2017
15.05.2017
20.05.2017
25.05.2017
30.05.2017
04.06.2017
09.06.2017

ПРИЛОЖЕНИЕ Ж

Сетевой график

Для своевременного выполнения работ, а также соответствия плану работ необходимо определить сроки выполнения работ (Таблица 1).

i-j – код работы

T – длительность работы, дней

$T_{рн}$ – ранний срок начала работы

$T_{пн}$ – поздний срок начала работы

$T_{ро}$ – ранний срок окончания работы

$T_{по}$ – поздний срок окончания работы

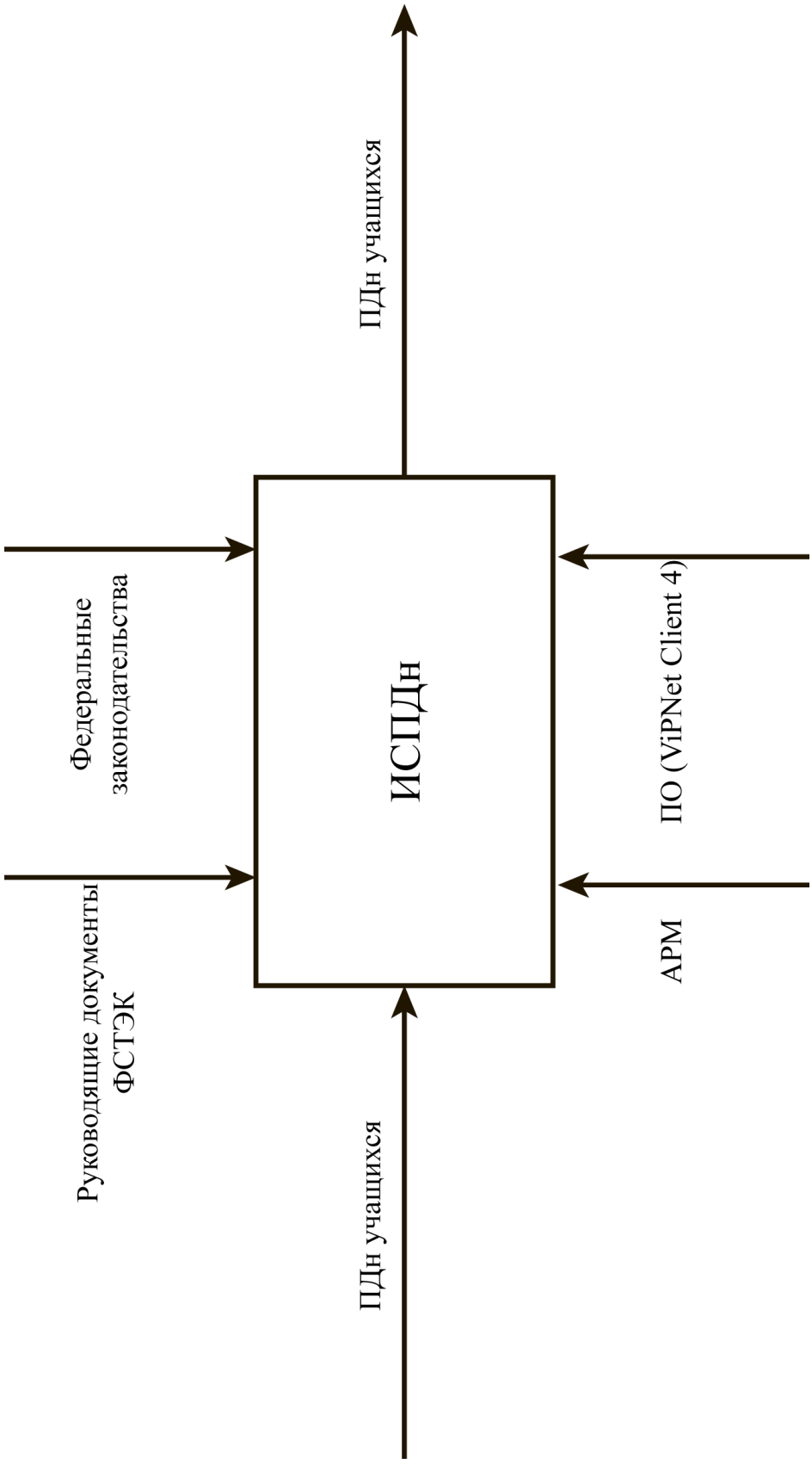
Таблица 1– Расписание выполнения работ

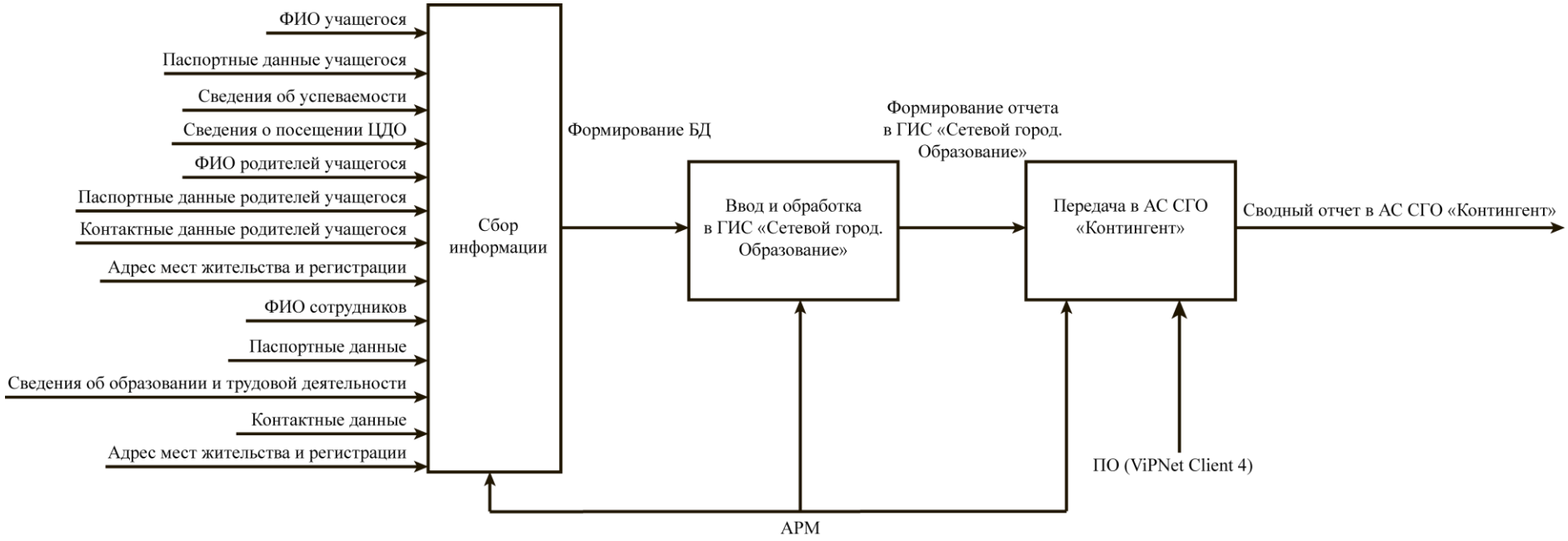
i – j	Название работ	T	$T_{рн}$	$T_{пн}$	$T_{ро}$	$T_{по}$
1 – 2	Назначение ответственного за организацию обработки ПДн	1	0	0	1	1
2 – 3	Назначение администратора безопасности ИСПДн	1	1	1	2	2
3 – 4	Создание комиссии по вопросам обеспечения безопасности ПДн	1	2	2	3	3
4 – 5	Определение перечня ИСПДн	1	3	3	4	4
5 – 6	Определение перечня, обрабатываемых ПДн	1	4	4	5	5
6 – 7	Определение ответственности лиц, участвующих в обработке	2	5	5	7	7
7 – 8	Разработка организационно-распорядительных документов по защите персональных данных	3	7	7	10	10
8 – 9	Разработка форм согласий субъектов ПДн на обработку ПДн	1	10	10	11	11
9 – 10	Определить места хранения материальных носителей персональных данных	1	11	11	12	12
10 – 11	Определение круга лиц, участвующих в обработке ПДн	1	12	13	13	13
11 – 12	Определение прав разграничения доступа пользователей ИСПДн, необходимых для выполнения должностных обязанностей	2	13	13	15	15

i – j	Название работ	T	$T_{рн}$	$T_{пн}$	$T_{ро}$	$T_{по}$
12 – 13	Организация информирования и обучения сотрудников о порядке обработки и обеспечения безопасности ПДн	4	15	15	19	19
13 – 14	Проведение оценки возможного вреда субъектам, чьи персональные данные обрабатываются в 21ИСПДн	1	19	19	20	20
14 – 15	Определение класса защищенности ГИС и уровня защищенности ПДн, обрабатываемых в ИСПДн (ГИС)	1	20	20	21	21
15 – 16	Анализ актуальности угроз безопасности персональных данных	3	21	21	24	24
16 – 17	Определение методов, средств и способов защиты ПДн, выбор помещений для установки аппаратных средств ИСПДн в помещениях, с целью исключения НСД лиц, не допущенных к обработке ПДн	3	24	24	27	27
17 – 18	Закупка, установка и настройка средств защиты информации	2	27	27	29	29
18 – 19	Контроль защищенности	1	29	29	30	30
19 – 20	Обучение пользователей	1	30	30	31	31

ПРИЛОЖЕНИЕ З

Модель деятельности общеобразовательного учреждения




ФИО учащегося
Паспортные данные учащегося
Сведения об успеваемости
Сведения о посещении ЦДО
ФИО родителей учащегося
Паспортные данные родителей учащегося
Контактные данные родителей учащегося
Адрес мест жительства и регистрации
ФИО сотрудников
Паспортные данные
Сведения об образовании и трудовой деятельности
Контактные данные
Адрес мест жительства и регистрации
Сбор информации
Формирование БД
Ввод и обработка в ГИС «Сетевой город. Образование»
Формирование отчета в ГИС «Сетевой город. Образование»
Передача в АС СГО «Контингент»
Сводный отчет в АС СГО «Контингент»
ПО (ViPNet Client 4)
АРМ