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»

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

Модернизация защиты информационной системы персональных данных ООО «РСС Челябинск»

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ – 10.03.01.2018.184.ПЗ ВКР

Руководитель проекта,
ген. директор ООО «Диджитер»
_____С.А.Сабельников
_____ 2018 г.

Автор проекта,
студент группы КЭ-471
_____ А.С.Зуев
_____ 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 10.03.01 «Информационная безопасность»

УТВЕРЖДАЮ

Заведующий кафедрой

_____ А.Н. Соколов

_____ 2018 г.

З А Д А Н И Е

на выпускную квалификационную работу студента

Зуева Артёма Сергеевича

Группа *КЭ-471*

1 Тема работы

Модернизация защиты информационной системы персональных данных в ООО «РСС Челябинск»

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

2 Срок сдачи студентом законченной работы *27.05.2018*

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)

1. ПРОВЕДЕНИЕ ПРЕДПРОЕКТНОГО ОБСЛЕДОВАНИЯ ООО "Организация"

1.1.Разработка технического паспорта

1.2.Разработка модели деятельности

1.3.Выявление защищаемой информации

1.4.Описание информационной системы

1.5.Выявление объектов защиты

1.6.Разработка модели угроз и уязвимостей для важных объектов защиты

1.7.Расчет рисков важных объектов защиты

1.8.Разработка технического задания на создание системы защиты персональных данных на предприятии ООО «РСС Челябинск»

2.ТЕОРЕТИЧЕСКОЕ ОБОСНОВАНИЕ СРЕДСТВ ЗАЩИТЫ

2.1.Обзор возможных методов устранения уязвимостей

2.2.Угрозы несанкционированного доступа к информации

2.3.Угроза воздействия вредоносных программ(вирусов)

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

3.РАЗРАБОТКА ПРОЕКТА СОЗДАНИЯ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫЗ ДАННЫХ НА ПРЕДПРИЯТИИ ООО «РСС Челябинск»

3.1.Описание объекта

3.2.Резюме проекта

3.3.Цели и задачи проекта

3.4.Объекты поставки проекта

3.5.Риски проекта

3.6.Структурное разбиение работ

3.7.Структурная схема организации проекта

3.8.Матрица ответственности

3.9.Диаграмма Гранта и сетевой график

3.10.Расчёт бюджета проекта и эго эффективности

5 Перечень графического материала (с точным указанием обязательных чертежей, плакатов в листах формата А1)
Презентация, 14 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)

7 Дата выдачи задания *25 января 2018*

Руководитель,
ген. директор ООО «Диджитер» _____С.А. Сабельников

Задание принял к исполнению _____А.С. Зуев

КАЛЕНДАРНЫЙ ПЛАН

Наименование этапов выпускной квалификационной работы (проекта)	**Срок выполнения этапов работы**	**Отметки о выполнении руководителя**
Введение	*24.03.2018*	
1.ПРОВЕДЕНИЕ ПРЕДПРОЕКТНОГО ОБСЛЕДОВАНИЯ ООО "РСС Челябинск"	*24.03.2018*	
1.1.Разработка технического паспорта	*24.03.2018*	
1.2.Разработка модели деятельности	*24.03.2018*	
1.3.Выявление защищаемой информации	*24.03.2018*	
1.4.Описание информационной системы	*24.03.2018*	
1.5.Выявление объектов защиты	*24.03.2018*	
1.6.Разработка модели угроз и уязвимостей для важных объектов защиты	*24.03.2018*	
1.7.Расчет рисков важных объектов защиты	*24.03.2018*	
1.8.Разработка технического задания на создание системы защиты персональных данных на предприятии ООО «РСС Челябинск»	*24.03.2018*	
Вывод по первой главе	*24.03.2018*	
2.Теоретическое обоснование выбора средств защиты	*30.04.2018*	
2.1.Обзор возможных методов устранения уязвимостей	*30.04.2018*	
2.2.Угрозы несанкционированного доступа к информации	*30.04.2018*	
2.3.Угроза воздействия вредоносных программ(вирусов)	*30.04.2018*	
2.4.Угроза сканирования, направленная на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций, топологии сети, открытых портов и служб, открытых соединений и др.	*30.04.2018*	
Вывод по второй главе	*30.04.2018*	
3.РАЗРАБОТКА ПРОЕКТА СОЗДАНИЯ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫЗ ДАННЫХ НА ПРЕДПРИЯТИИ ООО «РСС Челябинск»	*30.04.2018*	
3.1.Описание объекта	*30.04.2018*	
3.2.Резюме проекта	*30.04.2018*	
3.3.Цели и задачи проекта	*30.04.2018*	
3.4.Объекты поставки проекта	*30.04.2018*	

3.5.Риски проекта	*30.04.2018*	
3.6.Структурное разбиение работ	*30.04.2018*	
3.7.Структурная схема организации проекта	*30.04.2018*	
3.8.Матрица ответственности	*30.04.2018*	
3.9.Диаграмма Гранта и сетевой график	*30.04.2018*	
3.10.Расчёт бюджета проекта и эго эффективности	*30.04.2018*	
Вывод по третьей главе	*30.04.2018*	
Заключение	*30.04.2018*	
Библиографический список	*30.04.2018*	
Предзащита ВКР	*4.06.2018*	
Защита ВКР	*11.06.2018*	

Заведующий кафедрой _____ А.Н. Соколов

Руководитель работы _____ С.А. Сабельников

Студент _____ А.С. Зуев

АННОТАЦИЯ

Зуев А.С. Модернизация защиты информационной системы персональных данных в ООО «РСС Челябинск» – Челябинск: ЮУрГУ, КЭ-471, 79 с.,2 ил., 16 табл., библиогр. список – 15 наим., 8 прил.

Так как информация, приведённая в данной выпускной квалификационной работе является информацией ограниченного доступа, то некоторые данные могут быть искажены.

В рамках данной выпускной квалификационной работы была выполнена модернизация системы защиты информационной системы обработки персональных данных в ООО «РСС Челябинск». В данной организации имеется две системы для обработки ПДн: АС ПД «Клиенты» и АС ПДн «Сотрудники». В рамках данной квалификационной работы будет рассматриваться АС ПДн «Клиенты».

В выпускной квалификационной работе было проведено исследование информационной системы персональных данных предприятия и мер её защиты, выявлены слабые места и сделаны предложения по устранению данных недоработок в системе защиты.

Работа состоит из трёх глав. В первой главе было проведено пред проектное обследование организации и описана информационная система персональных данных организации.

Во второй главе было приведено сравнение средств защиты и выбраны оптимальные средства, предотвращающие актуальные угрозы организации, обоснован их выбор с точки зрения экономической целесообразности и эффективности.

В третьей главе была проведена разработка проекта модернизации системы защиты организации, проведён расчёт рисков и бюджета, составлена диаграмма Гранта.

ОГЛАВЛЕНИЕ

СОКРАЩЕНИЯ И ОПРЕДЕЛЕНИЯ

АРМ – автоматизированное рабочие место;
АС – автоматизированная система;
ВТСС – вспомогательные технические средства и системы;
ЗИ – защита информации;
ИБ – информационная безопасность;
ИС – информационная система;
ИСПДн – информационная система персональных данных;
НСД – несанкционированный доступ;
ООО – Общество с ограниченной ответственностью;
ОТСС – основные технические средства и системы;
ПДн – персональные данные;
ПО – программное обеспечение;
РД – руководящие документы;
РФ – Российская Федерация;
ФЗ – Федеральный закон;
ФСТЭК – Федеральная служба по техническому и экспортному контролю;

Базовые угрозы информационной безопасности – нарушение конфиденциальности, нарушение целостности и отказ в обслуживании;

Ресурс – любой контейнер, предназначенный для хранения информации, подверженный угрозам информационной безопасности (сервер, рабочая станция, переносной компьютер). Свойствами ресурса являются: перечень угроз, воздействующих на него, и критичность ресурса;

Угроза – действие, которое потенциально может привести к нарушению безопасности. Свойством угрозы является перечень уязвимостей, при помощи которых может быть реализована угроза;

Уязвимость – это слабое место в информационной системе, которое может привести к нарушению безопасности путем реализации некоторой угрозы. Свойствами уязвимости являются: вероятность (простота) реализации угрозы через данную уязвимость и критичность реализации угрозы через данную уязвимость;

Критичность ресурса – степень значимости ресурса для информационной системы, т.е. как сильно реализация угроз информационной безопасности на ресурс повлияет на работу информационной системы. Задается в деньгах;

Критичность реализации угрозы – степень влияния реализации угрозы на ресурс, т.е. как сильно реализация угрозы повлияет на работу ресурса. Задается в процентах;

Вероятность реализации угрозы через данную уязвимость в течение года – степень возможности реализации угрозы через данную уязвимость в тех или иных условиях. Указывается в процентах.

ВВЕДЕНИЕ

В современном обществе практически в каждой организации имеется информационная система, на которой обрабатывается большое количество информации. Часть из этой информации — это персональные данные сотрудников и клиентов организации, которая ограниченна к распространению и не должна попасть за пределы организации. Подобная утечка данных может обернуться значительным ущербом для компании. Именно поэтому очень актуальным является вопрос защиты информационной системы предприятия и находящихся в ней данных. Защиту персональных данных, согласно законам РФ, осуществляет оператор или лицо, осуществляющее обработку персональных данных по поручению оператора на основании заключаемого с этим лицом договора [1].

В ООО «РСС Челябинск» уже реализована система защиты ПДн. Причиной модернизации послужил тот факт, что действующая система не обеспечивает достаточный уровень защищённости персональных данных.

Таким образом, актуальность данной работы обусловлена необходимостью модернизации защиты автоматизированной систем обработки персональных данных в ООО «РСС Челябинск».

Объектом выпускной квалификационной работы является ООО «РСС Челябинск».

Предметом выпускной квалификационной работы является автоматизированная система обработки персональных данных «Клиенты» в данной организации.

Целью дипломной работы является модернизация защиты автоматизированной системы обработки персональных данных «Клиенты».

В соответствии с поставленной целью необходимо решить следующие задачи:

1. Проанализировать информационную систему ООО «РСС Челябинск», с целью определения уязвимостей в защите автоматизированной системы обработки персональных данных «Клиенты»;
2. Провести анализ и теоретическое обоснование выбора средств модернизации защиты информации;
3. Разработать проект по модернизации системы защиты автоматизированной системы обработки персональных данных в ООО «РСС Челябинск» «Клиенты».

1. АНАЛИЗ СОСТОЯНИЯ ЗАЩИТЫ ИНФОРМАЦИИ В ООО «РСС Челябинск» И СУЩЕСТВУЮЩИЕ ПРОБЛЕМЫ

1.1. Разработка технического паспорта

Для модернизации системы защиты информационной системы обработки ПД было проведено предпроектное обследование предприятия и составлен технический паспорт (Приложение А).

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

В качестве объекта защиты была выбрана АС «Клиенты» ООО «РСС Челябинск».

1.2. Разработка модели деятельности

После обследования АС «Клиенты» предприятия была составлена модель деятельности (Приложение В). В данной схеме показаны ключевые этапы обработки информации ограниченного доступа.

Данная модель необходима для выявления потоков информации ограниченного доступа.

1.3. Выявление защищаемой информации

В результате проведенного предпроектного обследования, ознакомления с информацией ограниченного доступа и организационно-распорядительной документацией была выявлена следующая защищаемая информация: Перечень персональных данных, подлежащих защите в автоматизированной системе обработки персональных данных «Клиенты».

В рамках данной ВКР был разработан перечень персональных данных (Приложение Г).

1.4. Описание информационной системы

Система защиты информации в АС «Клиенты» ООО «РСС Челябинск» основана на использовании организационных, правовых и программно-аппаратных мер.

Организационные меры включают в себя инструкции администратора, инструкции пользователей, инструкцию по эксплуатации СЗИ, инструкцию по парольной защите, инструкцию по резервированию, журнал учета лиц, журнал учета машинных носителей.

Правовые меры включают в себя нормативно-правовые документы, регулирующие деятельность организации в области обеспечения защиты информации:

– Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка) [6];

– Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных [8];

– Федеральный закон «О персональных данных» [1];

– Постановление Правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [16];

– Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» [4];

Программно-аппаратные меры включают в себя комплекс программно-аппаратных средств, обеспечивающих работу автоматизированной системы и ее защиту. В рамках ВКР была проведена инвентаризация автоматизированной системы, результаты которой представлены в Таблицах 1 и 2.

Таблица 1 – Аппаратное обеспечение

Наименование устройства	Фирма производитель, модель	Заводской / инвентаризационный номер
1	2	3
ОТСС		
Системный блок	InWin BM677	1ABMAGE000030
НЖМД	WD WD5000AAKS-22A7B0	WCASY2495047
Монитор	Benq ET-0034-N	ETT9902134026
Клавиатура	MITSUMI KFK-EB9HY	KFKEB9HY518B0011
Мышь	Genius NetScroll EYE	136703402193
Принтер	Samsung SCX-4600	Z2VJBFFSC00519K
ИБП	DNS SMART PRO LCD 1000VA	1108210223
Системный блок	InWin BM677	1ABMAGE000183
НЖМД	WD WD5000AAKS-22A7B0	WCASY2495089
Монитор	Benq ET-0034-N	ETT9902134041
Клавиатура	MITSUMI KFK-EB9HY	KFKEB9HY518B0273
Мышь	Genius NetScroll EYE	136703402462
ИБП	DNS SMART PRO LCD 1000VA	1108210248
ВТСС		
Коммутатор	TP-LINK Archer C7	135A2400354
Датчик пожарной сигнализации	ИП 212-45	61506053432
Телефон	Panasonic KX-T 7630RU	T7630RUV4-N1A
Датчик охранной сигнализации	н/а	н/а

Таблица 2 – Программное обеспечение

Наименование	Версия
Microsoft Windows 7 Professional SP1	6.1
MS Office	16.0.4266.1001
360 Total Security	8.2.0.1034
1C	2.1.11.5
Chrome	48.0.2564.109
Bitrix24	3.1.88.23

1.5. Выявление объектов защиты

Опираясь на вышеизложенную информацию был определён перечень объектов, подлежащих защите:

- 2 АРМ, на которых происходит обработка ПДн.
- линии питания и связи;
- носители информации;
- сотрудники.

Подробный перечень объектов приведён в Приложении А.

1.6. Разработка модели угроз и уязвимостей для важных объектов защиты

Модель угроз – это перечень возможных угроз. Модель угроз безопасности персональных данных необходима для определения требований к системе защиты. Без модели угроз невозможно построить адекватную (с точки зрения денежных затрат) систему защиты информации, обеспечивающую безопасность персональных данных.

На основании модели деятельности организации был сформулирован перечень важных объектов защиты:

- персонал;
- автоматизированное рабочее место, на котором обрабатывается защищаемая информация;

Далее, были выделены наиболее существенные угрозы информационной безопасности и разработана модель угроз на основании документа «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка)» ФСТЭК.

Подробное описание модели угроз приведено в пунктах 1.6.1-1.6.5.

1.6.1 Угрозы утечки информации по техническим каналам

1.6.1.1 Угрозы утечки акустической(речевой) информации

Возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя ИСПДн, при обработке ПДн в ИСПДн, возможно при наличии функции голосового ввода ПДн в ИСПДн или функций воспроизведения ПДн акустическими средствами ИСПДн.

В данной АС функции голосового ввода ПДн или функции воспоизведения ПДн акустическими средствами отсутствуют.

Вероятность реализации угрозы – маловероятна.

1.6.1.2 Угрозы утечки видовой информации

Реализация угрозы утечки видовой информации возможна за счет просмотра информации с помощью оптических (оптико-электронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео и буквенно-цифровой информации, входящих в состав ИСПДн.

В здании ООО «РСС Челябинск» введен контроль доступа в контролируемую зону, двери закрываются на замки, монитор развёрнут в сторону от окна.

Вероятность реализации угрозы – маловероятна.

1.6.1.3 Угрозы утечки информации по каналам ПЭМИН

Угрозы утечки информации по каналу ПЭМИН, возможны из-за наличия паразитных электромагнитных излучений у элементов ИСПДн.

Размер КЗ достаточно большой, паразитные излучения ИСПДн экранируются стенами, а также маскируются множеством паразитных сигналов других устройств.

Вероятность реализации угрозы – маловероятна.

1.6.2 Угрозы несанкционированного доступа к информации

1.6.2.1 Кража ПЭВМ

Угроза осуществляется путём НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн.

В здании ООО «РСС Челябинск» введен контроль доступа в контролируемую зону, двери закрываются на замок, вынос техники за пределы здания возможен только с разрешения руководства.

Вероятность реализации угрозы – маловероятна.

1.6.2.2 Кража носителей информации

Угроза осуществляется путем НСД внешними и внутренними нарушителями к помещениям, где расположены носители информации.

В здании ООО «РСС Челябинск» введен контроль доступа в контролируемую зону, двери закрываются на замок.

Вероятность реализации угрозы – маловероятна.

1.6.2.3 Кража ключей и атрибутов доступа

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где происходит работа сотрудников.

В здании ООО «РСС Челябинск» введен контроль доступа в контролируемую зону, двери закрываются на замок.

Вероятность реализации угрозы – маловероятна.

1.6.2.4 Кража, модификация, уничтожение информации

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн и средства защиты, а так же происходит работа сотрудников.

В здании ООО «РСС Челябинск» введен контроль доступа в контролируемую зону, двери закрываются на замок.

Вероятность реализации угрозы – маловероятна.

1.6.2.5 Вывод из строя узлов ПЭВМ, каналов связи

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн и проходят каналы связи.

В здании ООО «РСС Челябинск» введен контроль доступа в контролируемую зону, двери закрываются на замок.

Вероятность реализации угрозы – маловероятно.

1.6.2.6 Несанкционированное отключения средств защиты

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены средства защиты ИСПДн.

В здании ООО «РСС Челябинск» введен контроль доступа в контролируемую зону, двери закрываются на замок.

Вероятность реализации угрозы – маловероятно

1.6.2.7 Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ

В Учреждении техническое обслуживание ПЭВМ осуществляется сотрудниками, подписавшими соглашение о неразглашении.

Вероятность реализации угрозы – маловероятна

1.6.3 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).

1.6.3.1 Действие вредоносных программ (вирусов)

Программно-математическое воздействие - это воздействие с помощью вредоносных программ. Программой с потенциально опасными последствиями или вредоносной программой (вирусом) называют некоторую самостоятельную программу (набор инструкций), которая способна выполнять любое непустое подмножество следующих функций:

– скрывать признаки своего присутствия в программной среде компьютера;

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

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

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

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

– 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.

В учреждении на всех элементах ИСПДн установлена бесплатная антивирусная защита, функционал которой ограничен, пользователи проинструктированы о мерах предотвращения вирусного заражения.

Вероятность реализации угрозы – высокая.

1.6.3.2 Недекларированные возможности системного ПО и ПО для обработки персональных данных

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Разработку и сопровождение программного обеспечения ИСПДн осуществляет доверенная организация.

Вероятность реализации угрозы – маловероятна.

1.6.3.2 Установка ПО, не связанного с исполнением служебных обязанностей

Угроза осуществляется путем несанкционированной установки ПО внутренними нарушителями, что может привести к нарушению конфиденциальности, целостности и доступности всей ИСПДн или ее элементов.

Все пользователи проинструктированы о политике установки ПО и осуществляется контроль.

Вероятность реализации угрозы – маловероятна.

1.6.4 Угрозы непреднамеренных 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

1.6.4.1 Утрата ключей и атрибутов доступа

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения парольной политике в части их создания (создают легкие или пустые пароли, не меняют пароли по истечении срока их жизни или компрометации и т.п.) и хранения (записывают пароли на бумажные носители, передают ключи доступа третьим лицам и т.п.) или не осведомлены о них.

В учреждении введена парольная политика, предусматривающая требуемую сложность пароля, пользователи проинструктированы о парольной политике и о действиях в случаях утраты или компрометации паролей.

Вероятность реализации угрозы – средняя.

1.6.4.2 Непреднамеренная модификация (уничтожение) информации сотрудниками

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения принятых правил работы с ИСПДн или не осведомлены о них.

В учреждении резервное копирование обрабатываемых ПДн не осуществляется.

Вероятность реализации угрозы – высокая.

1.6.4.3 Непреднамеренное отключение средств защиты

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения принятых правил работы с ИСПДн и средствами защиты или не осведомлены о них.

В учреждении введен контроль доступа в контролируемую зону, двери закрываются на замок, осуществляется разграничение доступа к настройкам режимов средств защиты, пользователи проинструктированы о работе с ИСПДн.

Вероятность реализации угрозы – маловероятно.

1.6.4.4 Выход из строя аппаратно-программных средств

Угроза осуществляется вследствие несовершенства аппаратно-программных средств, из-за которых может происходить нарушение целостности и доступности защищаемой информации.

В учреждении осуществляется резервирование ключевых элементов ИСПДн.

Вероятность реализации угрозы – низкая.

1.6.4.5 Сбой системы электроснабжения

Угроза осуществляется вследствие несовершенства системы электроснабжения, из-за чего может происходить нарушение целостности и доступности защищаемой информации.

В учреждении ко всем ключевым элементам ИСПДн подключены источники бесперебойного питания.

Вероятность реализации угрозы – маловероятна.

1.6.4.6 Стихийное бедствие

Угроза осуществляется вследствие несоблюдения мер пожарной безопасности.

В учреждении установлена пожарная сигнализация, пользователи проинструктированы о действиях в случае возникновения внештатных ситуаций.

Вероятность реализации угрозы – маловероятна.

1.6.5 Угрозы преднамеренных действий внутренних нарушителей

1.6.5.1 Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке

Угроза осуществляется путем НСД внешних нарушителей в помещения, где расположены элементы ИСПДн и средства защиты, а также происходит работа пользователей.

В здании ООО «РСС Челябинск» введен контроль доступа в контролируемую зону, двери закрываются на замок.

Вероятность реализации угрозы – маловероятна.

1.6.5.2 Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения о неразглашении обрабатываемой информации или не осведомлены о них.

В учреждении пользователи осведомлены о порядке работы с персональными данными, а также подписали Соглашение о неразглашении.

Требуется резервное копирование обрабатываемой информации.

Вероятность реализации угрозы – средняя.

1.6.5.3 Угрозы несанкционированного доступа по каналам связи

В соответствии с «Типовой моделью угроз безопасности персональных данных, обрабатываемых в распределенных ИСПДн, имеющих подключение к сетям общего пользования и (или) международного информационного обмена» (п. 6.6. Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 15 февраля 2008 г.), для ИСПДн рассматриваются следующие угрозы, реализуемые с использованием протоколов межсетевого взаимодействия:

- угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации;
- 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.;
- угрозы выявления паролей по сети;
- угрозы навязывания ложного маршрута сети;
- угрозы подмены доверенного объекта в сети;
- угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях;
- угрозы типа «Отказ в обслуживании»;
- угрозы удаленного запуска приложений;
- угрозы внедрения по сети вредоносных программ.

1.6.5.4 Угроза «Анализ сетевого траффика»

Эта угроза реализуется с помощью специальной программы-анализатора пакетов (sniffer), перехватывающей все пакеты, передаваемые по сегменту сети, и выделяющей среди них те, в которых передаются идентификатор пользователя и его пароль. В ходе реализации угрозы нарушитель:

– изучает логику работы ИСПДн - то есть стремится получить однозначное соответствие событий, происходящих в системе, и команд, пересылаемых при этом хостами, в момент появления данных событий. В дальнейшем это позволяет злоумышленнику на основе задания соответствующих команд получить, например, привилегированные права на действия в системе или расширить свои полномочия в ней;

– перехватывает поток передаваемых данных, которыми обмениваются компоненты сетевой операционной системы, для извлечения конфиденциальной или идентификационной информации (например, статических паролей пользователей для доступа к удаленным хостам по протоколам FTP и TELNET, не предусматривающих шифрование), ее подмены, модификации и т.п.

Требуется установка программного или аппаратного межсетевого экрана.

Вероятность реализации угрозы – средняя.

1.6.5.5 Угроза «сканирование сети»

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.

Требуется установка программного или аппаратного межсетевого экрана.

Вероятность реализации угрозы – высокая.

1.6.5.6 Угроза выявления паролей

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, подмена доверенного объекта сети (IP-spoofing) 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.

В учреждении применяются стойкие пароли.

Вероятность реализации угрозы – маловероятна.

1.6.5.7 Угрозы навязывания ложного маршрута сети

Данная угроза реализуется одним из двух способов: путем внутрисегментного или межсегментного навязывания. Возможность навязывания ложного маршрута обусловлена недостатками, присущими алгоритмам маршрутизации (в частности из-за проблемы идентификации сетевых управляющих устройств), в результате чего можно попасть, например, на хост или в сеть злоумышленника, где можно войти в операционную среду технического средства в составе ИСПДн. Реализации угрозы основывается на несанкционированном использовании протоколов марш-

рутизации (RIP, OSPF, LSP) и управления сетью (ICMP, SNMP) для внесения изменений в маршрутно-адресные таблицы. При этом нарушителю необходимо послать от имени сетевого управляющего устройства (например, маршрутизатора) управляющее сообщение.

В ИСПДн межсетевое взаимодействие не осуществляется.

Вероятность реализации угрозы – маловероятна.

1.6.5.8 Угрозы подмены доверенного объекта

Такая угроза эффективно реализуется в системах, в которых применяются нестойкие алгоритмы идентификации и аутентификации хостов, пользователей и т.д. Под доверенным объектом понимается объект сети (компьютер, межсетевой экран, маршрутизатор и т.п.), легально подключенный к серверу.

Могут быть выделены две разновидности процесса реализации указанной угрозы: с установлением и без установления виртуального соединения.

Процесс реализации с установлением виртуального соединения состоит в присвоении прав доверенного субъекта взаимодействия, что позволяет нарушителю вести сеанс работы с объектом сети от имени доверенного субъекта. Реализация угрозы данного типа требует преодоления системы идентификации и аутентификации сообщений (например, атака rsh-службы UNIX-хоста).

Процесс реализации угрозы без установления виртуального соединения может иметь место в сетях, осуществляющих идентификацию передаваемых сообщений только по сетевому адресу отправителя. Сущность заключается в передаче служебных сообщений от имени сетевых управляющих устройств (например, от имени маршрутизаторов) об изменении маршрутно-адресных данных.

В результате реализации угрозы нарушитель получает права доступа к техническому средству ИСПДн - цели угроз.

В ИСПДн межсетевое взаимодействие не осуществляется.

Вероятность реализации угрозы – маловероятна.

1.6.5.9 Внедрение ложного объекта сети

Эта угроза основана на использовании недостатков алгоритмов удаленного поиска. В случае если объекты сети изначально не имеют адресной информации друг о друге, используются различные протоколы удаленного поиска (например, SAP в сетях Novell NetWare; ARP, DNS, WINS в сетях со стеком протоколов TCP/IP), заключающиеся в передаче по сети специальных запросов и получении на них ответов с искомой информацией. При этом существует возможность перехвата нарушителем поискового запроса и выдачи на него ложного ответа, использование которого приведет к требуемому изменению маршрутно-адресных данных. В дальнейшем весь поток информации, ассоциированный с объектом-жертвой, будет проходить через ложный объект сети.

В ИСПДн межсетевое взаимодействие не осуществляется.

Вероятность реализации угрозы – маловероятна.

1.6.5.10 Угрозы 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:

– 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. Примерами реализации угроз подобного рода могут служить: направленный шторм эхо-запросов по протоколу ICMP (Ping flooding), шторм запросов на установление TCP-соединений (SYN-flooding), шторм запросов к FTP-серверу;

– 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. Примерами угроз данного типа могут служить шторм широковещательных ICMP-эхо-запросов (Smurf), направленный шторм (SYN-flooding), шторм сообщений почтовому серверу (Spam);

– 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 (например, ICMP Redirect Host, DNS-flooding) или идентификационной и аутентификационной информации;

– явный отказ в обслуживании, вызванный передачей злоумышленником пакетов с нестандартными атрибутами (угрозы типа «Land», «TearDrop», «Bonk», «Nuke», «UDP-bomb») или имеющих длину, превышающую максимально допустимый размер (угроза типа «Ping Death»), 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 соответствующей службы предоставления удаленного доступа к 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.

На всех компьютерах локальной сети установлены бесплатные антивирусные средства, функционал которых ограничен.

Вероятность реализации угрозы – средняя.

1.6.5.11 Угрозы 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:

– распространение файлов, содержащих несанкционированный исполняемый код;

– удаленный запуск приложения путем переполнения буфера приложений-серверов;

– 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 типа Back. Orifice, Net Bus), либо штатными средствами управления и администрирования компьютерных сетей (Landesk Management Suite, Managewise, Back Orifice и т. п.). В результате их использования удается добиться удаленного контроля над станцией в сети.

На всех компьютерах локальной сети установлены бесплатные антивирусные средства, функционал которых ограничен.

Вероятность реализации угрозы – средняя.

1.6.5.12 Угрозы 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 ра-

бочую 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:

– программы подбора и вскрытия паролей;
– программы, реализующие угрозы;
– программы, демонстрирующие использование недекларированных возможностей программного и программно-аппаратного обеспечения ИСПДн;
– программы-генераторы компьютерных вирусов;
– программы, демонстрирующие уязвимости средств защиты информации и др.

На всех компьютерах локальной сети установлены бесплатные антивирусные средства, функционал которых ограничен.

Вероятность реализации угрозы – средняя.

1.7 Расчет рисков важных объектов защиты

Расчет рисков важных объектов защиты предприятия ООО «РСС Челябинск» был выполнен на основе документа «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» ФСТЭК.

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

Для оценки возможности реализации угрозы применяются два показателя: уровень исходной защищенности ИСПДн(Y1) и частота (вероятность) реализации рассматриваемой угрозы(Y2).

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

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	Средний
По уровню (обезличивания) ПДн	Низкий

Продолжение таблицы 3

1	2
По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки	Высокая

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	0,25	низкая
Кража носителей информации	0,25	низкая
Кража ключей и атрибутов доступа	0,25	низкая
Кражи, модификации, уничтожения информации	0,25	низкая
Вывод из строя узлов ПЭВМ, каналов связи	0,25	низкая
Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	0,25	низкая
Несанкционированное отключение средств защиты	0,25	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)	0,75	высокая

Продолжение таблицы 4

1	2	3
Недекларированные возможности системного ПО и ПО для обработки персональных данных	0,25	низкая
Установка ПО не связанного с исполнением служебных обязанностей	0,25	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	0,5	средняя
Непреднамеренная модификация (уничтожение) информации сотрудниками	0,75	высокая
Непреднамеренное отключение средств защиты	0.25	низкая
Выход из строя аппаратно-программных средств	0,35	средняя
Сбой системы электроснабжения	0,25	низкая
Стихийное бедствие	0,25	низкая
Угрозы преднамеренных действий внутренних нарушителей		
Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке	0,25	низкая
Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	0,5	средняя
Угрозы несанкционированного доступа по каналам связи		
Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации	0,5	средняя
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.	0,75	высокая
Угрозы выявления паролей по сети	0,25	низкая
Угрозы навязывание ложного маршрута сети	0,25	низкая

Продолжение таблицы 4

1	2	3
Угрозы подмены доверенного объекта в сети	0,25	низкая
Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	0,25	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

1.7.1 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

Продолжение таблицы 5

1	2
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)	Низкая
Недекларированные возможности системного ПО и ПО для обработки персональных данных	Низкая
Установка ПО не связанного с исполнением служебных обязанностей	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	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	Низкая
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.	Низкая
Угрозы выявления паролей по сети	Низкая
Угрозы навязывание ложного маршрута сети	Низкая
Угрозы подмены доверенного объекта в сети	Низкая
Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	Низкая
Угрозы типа «Отказ в обслуживании»	Низкая
Угрозы удаленного запуска приложений	Низкая
Угрозы внедрения по сети вредоносных программ	Низкая

1.7.2 Определение актуальности угроз

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

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
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
Недекларированные возможности системного ПО и ПО для обработки персональных данных	Не актуальная
Установка ПО не связанного с исполнением служебных обязанностей	Не актуальная

Продолжение таблицы 7

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	Не актуальная
Непреднамеренная модификация (уничтожение) информации сотрудниками	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	Не актуальная
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	Не 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»	Не актуальная
Угрозы удаленного запуска приложений	Не актуальная
Угрозы внедрения по сети вредоносных программ	Не актуальная

1.8 Разработка технического задания на создание системы защиты персональных данных на предприятии ООО «РСС Челябинск»

По результатам предпроектного обследования было разработано техническое задание на создание системы защиты персональных данных на предприятии ООО «РСС Челябинск» (Приложение Б).

В качестве основы был взят ГОСТ 34.602-1989 «Техническое задание на создание автоматизированной системы». Техническое задание имеет следующие разделы:

1) общие сведения.

2) назначение и цели совершенствования системы;
3) характеристика объектов защиты;
4) требования к ИСПДн;
5) состав и содержание работ по совершенствованию системы;
6) порядок контроля и приемки системы;
7) требования к документированию.

ВЫВОДЫ ПО ПЕРВОЙ ГЛАВЕ

В результате проведенного предпроектного обследования СЗИ ООО «РСС Челябинск», была проделана следующая работа:

– Составлен технический паспорт на автоматизированную систему обработки персональных данных;

– Разработана модель деятельности, отражающая процесс обработки информации ограниченного доступа;

– Разработан перечень персональных данных, подлежащих защите в автоматизированной системе обработки персональных данных;

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

– Разработано техническое задание на модернизацию системы защиты персональных данных на предприятии ООО «РСС Челябинск»

– Определена контролируемая зона (Приложение А);

– Определены типы актуальных угроз (Таблица 7);

– Определён уровень защищённости (Таблица 3);

– Определена категория обрабатываемых персональных данных – 3 категория;

– Определён уровень защищённости системы (Приложение Ж).

2. ТЕОРЕТИЧЕСКОЕ ОБОСНОВАНИЕ ВЫБОРА СРЕДСТ ЗАЩИТЫ

2.1 Обзор возможных методов устранения уязвимостей

На основании разработанной нами модели угроз и уязвимостей ООО «РСС Челябинск» приведём обзор методов и средств их устранения. Проанализировав данные средства выберем наиболее оптимальные с соотношения стоимости/эффективности.

2.2 Угрозы несанкционированного доступа к информации

По результатам предпроектного обследования ООО «РСС Челябинск» очевидным стал факт высокого риска возникновения угроз, связанных с несанкционированным доступом к информации. Для устранения данной угрозы используются программно-аппаратные средства защиты, позволяющие управлять доступом к АРМ, выполнять регистрацию и учет пользователей и обеспечивать целостность и неизменность программной среды.

Из множества продуктов, имеющих сертификаты СЗИ от НСД и предоставленных на рынке в данный момент можно выделить следующие:

- SecretNet 7;
- Dallas Lock 8.0-K;
- Аккорд-X.

Сравнительный анализ предоставлен в таблице 8

Таблица 8- Сравнительный анализ СЗИ от НСД

Характеристика	Secret Net 7	Dallas Lock 8.0-K	Аккорд-X
1	2	3	5
Наличие сертификата	№2707, выдан 07.09.2012г, действителен до 07.09.2018г.	№2720, выдан 25.09.2012г, действителен до 25.09.2018г.	№3079, выдан 30.01.2014г, действителен до 30.01.2020г.
Идентификация и аутентификация пользователей до загрузки ОС	Да	Да	Да
Возможность аппаратной идентификации	Да	Да	Нет
Защита от обхода загрузки СЗИ	Да	Да	Да
Кодирование данных	Да	Да	Нет

Продолжение таблицы 8

Зачистка дискового пространства при удалении произвольных файлов	Да	Нет	Да
Автоматическая очистка дискового пространства при удалении информации	Да	Да	Нет
Разграничение доступа к внешним носителям, устройствам	Да	Да	Да
Контроль аппаратной конфигурации	Да	Частично	Да
Интеграция с доменом в режиме рабочей станции домена	Да	Да	Да
Регистрация событий безопасности	Да	Да	Нет
Совместимость с Windows 7	Да	Да	Нет
Средняя стоимость, руб.	7700	7500	9089

СЗИ от НСД Secret Net 7 имеет среднюю стоимость среди предоставленных средств. Так же данная СЗИ достаточно распространена, не очень сложна в настройке и имеет хорошее соотношение функциональность/цена. Поэтому выберем Secret Net 7.

2.3 Угроза воздействия вредоносных программ(вирусов)

Антивирусное ПО - специализированная программа, предназначенная для обнаружения компьютерных вирусов и вредоносных программ. Проведя анализ рынка, нами было выявлено три наиболее популярных антивируса, используемых пользователями, а также имеющих сертификаты ФСТЭК.

Для выбора наиболее оптимального продукта проведём их сравнение:

Таблица 9- Сравнение антивирусного ПО

Антивирус	Найдено угроз	% определения	Время на поиск	Загрузка ЦП, %	Средняя цена за одну АРМ на год, руб.	Сертификат
Kaspersky Endpoint Security 10	3695	96,3	23 мин	80-95	1633	№3025, выдан 25.11.2013г, действителен до 25.11.2019г.
Dr.Web Desktop Security Suite 10	2968	77,3	1 мин 10 сек	50-60	1210	№3509, выдан 25.01.2016г, действителен до 27.01.2019г.
ESET NOD32 Small Business Pack	2679	74,2	1 мин 12 сек	40-50	1465	№ 3243 от 13 октября 2014г, действителен до 13 октября 2020г.

Исходя из таблицы наиболее лучшим антивирусом по количеству найденных угроз является Kaspersky Endpoint Security 10 при минимальной разнице в цене с другими антивирусами. Поэтому целесообразным выбором антивирусного ПО из соотношения цена/качество будет являться Kaspersky Endpoint Security 10.

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

В ходе анализа результатов предпроектного обследования было выявлено, что для ООО «РСС Челябинск» актуальны 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.

Для защиты от этих угроз необходимо применение межсетевых экранов. Межсетевой экран (МСЭ) – это устройство обеспечения безопасности сети, которое осуществляет мониторинг входящего и исходящего сетевого трафика и на основании установленного набора правил безопасности принимает решения, пропустить или блокировать конкретный трафик. Межсетевой экран может быть аппаратным, про-

граммным или смешанного типа. В рамках ВКР был проведен сравнительный анализ программных межсетевых экранов, результаты которого приведены в Таблице 10.

Таблица 10- сравнение межсетевых экранов

Характеристика	TrustAccess	VipNet Office Firewall	Киберсейф: Межсетевой экран
Класс МЭ	2	3	4
Наличие сертификата	№ 2146, выдан 30.07.2010г, действителен до 30.07.2019г	№ СФ/515-3137, выдан 30.06.2017г, действителен до 9.05.2019г.	№ 3417, выдан 04.06.2015г, действителен до 04.06.2018г
Цена	От 1975	От 15710	От 900

По соотношению цена/функциональность и совместимости с СЗИ от НСД «Secret Net 7» для защиты выберем межсетевой экран «TrustAccess».

ВЫВОД ПО ВТОРОЙ ГЛАВЕ

В рамках второй главы были рассмотрены возможные методы устранения актуальных угроз, выявленных в ходе предпроектного обследования организации и выбраны средства защиты. Остальные, выявленные угрозы безопасности ИСПДн, на основе «Базовой модели угроз безопасности информации при их обработке в ИСПДн» ФСТЭК России от 15 февраля 2008 г. были признаны неактуальными и не рассмотрены в рамках данной работы.

Были применены следующие средства защиты:

1. Для защиты от несанкционированного доступа к информации:
   - Установлено СЗИ от НСД «Secret Net 7», по причине наилучшего соотношения функционал/цена (сравнение продуктов по СЗИ от НСД приведено в таблице 8).
2. Для защиты от воздействия вредоносных программ(вирусов):
   - Установлено антивирусное ПО «Kaspersky Endpoint Security 10 для Windows», так как его соотношение функционал/цена, гораздо лучше, чем у конкурирующего антивирусного ПО.
3. Для защиты от угроз сканирования, направленная на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций, топологии сети, открытых портов и служб, открытых соединений и др.:
   - Установлен межсетевой экран «TrustAccess1.3», так как он полностью совместим с продуктом «Secret Net 7» и обладает хорошим соотношением функционал/цена.

4. Для защиты от угрозы непреднамеренной модификации (уничтожение) информации сотрудниками введено резервное копирование информации, обрабатываемой на АРМ.

5. Для эффективной эксплуатации системы защиты от вирусов была создана инструкция по антивирусной защите (Приложение З).

3. РАЗРАБОТКА ПРОЕКТА СОЗДАНИЯ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫЗ ДАННЫХ НА ПРЕДПРИЯТИИ ООО «РСС Челябинск»

3.1 Описание объекта

Основным видом деятельности ООО «РСС Челябинск» является ремонт компьютеров, ноутбуков и другой орг. техники. В связи с этим возникает необходимость защищать персональные данные клиентов. В таблице 11 предоставлен поток защищаемой информации.

Таблица 11-поток защищаемой информации

Входящая информация	Исходящая информация
ПДн клиентов	База данных клиентов

3.2 Резюме проекта

Проект разработан согласно утвержденному техническому заданию по модернизации системы защиты ИСПДн на предприятии ООО «РСС Челябинск» (Приложение Б).

Для достижения поставленной цели, необходимо разработать ряд организационных, инженерно-технических и программно-аппаратных мер. На каждый отдельный этап работы, с помощью матрицы ответственности назначается ответственное лицо.

Результатом проекта является модернизированная ИСПДн, включающая внедрение программного средства, обеспечивающего защиту от НСД, соответствующая требованиям нормативно-правовых актов в этой области и целям внедрения.

3.3 Цели и задачи проекта

Целями модернизации системы защиты персональных данных ООО «РСС Челябинск» являются:

- предотвращение хищения, утери, искажения информации;
- обеспечение защищенности ИСПДн в процессе обработки и хранения ПДн;
- снижение вероятности реализации актуальных угроз несанкционированного доступа (НСД) к ПДн;
- осуществление защиты персональных данных в соответствии с нормативно-правовыми актами.

3.4 Объекты поставки проекта

3.4.1 Организационно-распорядительная документация

Организационно-распорядительная документация на предприятии ООО «РСС Челябинск»:

– Технический паспорт на автоматизированную систему обработки персональных данных (Приложение А);
– Техническое задание на создание системы защиты персональных данных (Приложение Б);
– Модель деятельности (Приложение В);
– Перечень персональных данных, подлежащих защите в автоматизированной системе обработки персональных данных (Приложение Г)
– Инструкции администратору;
– Инструкция по парольной защите;
– Инструкция по антивирусной защите (Приложение З);

3.4.2 Программно-аппаратные и инженерно-технические меры

При модернизации существующей системы защиты персональных данных необходимо закупить и установить следующие средства защиты:

– СЗИ от НСД «Secret Net 7»;
– антивирусное ПО «Kaspersky Endpoint Security 10»;
– межсетевой экран «TrustAccess 1.3».

3.4.3 Обучение персонала

Обучение сотрудников новым требованиям защиты информации с обоснованием их необходимости и значимости для организации по результатам внедрения новых организационно-распорядительных документов, предусмотренных проектом, а также программно-аппаратных решений.

3.5 Риски проекта

Вероятность реализации угрозы через данную уязвимость в течение года: P(V), (%).

Критичность реализации угрозы через уязвимость: ER, (%).

Уровень угрозы Th (%), рассчитывается по Формуле (1):

$$Th = \frac{ER \cdot P(V)}{10000} \quad (1)$$

Уровень угрозы по всем уязвимостям, через которые реализуется данная угроза CTh (%), рассчитывается по Формуле (2):

$$CTh = 1 - \prod_{i=1}^{n}(1 - Th) \quad (2)$$

Таблица 12 – Риски проекта

Риски / пути их реализации	Критичность ER	Вероятность P(V)	Th	CTh
1. Риски изменений в стране, обществе				
1.1. Ухудшение политических и экономических характеристик и факторов				0,647
– реформы в экономике и политике	10	5	0,0005	
– изменение законодательства	30	20	0,006	
1.2. Изменение характеристик общества				0,506
– здравоохранение и медицина	25	5	0,012	
– возникновение негативного отношения сотрудников	80	50	0,4	
1.3. Влияние форс-мажорных обстоятельств				0,0025
– стихийные бедствия и природные катаклизмы	5	5	0,0025	
2. Риски окружения проекта в составе организации				
2.1. Изменение или недостаток бюджета проекта				0,8328
– задержки финансирования	80	15	0,12	
– отсутствие денежного резерва для реагирования на события рисков (в т.ч. для ликвидации отставания от графика)	90	90	0,81	
2.2. Недостаточная организованность работ				0,031
– срыв графиков работ, невыполнение сроков	10	10	0,01	
– нехватка рабочей силы	30	5	0,015	
– недооценка стоимости работ и использование финансов для других целей	30	2	0,006	
2.3. Риски персонала				0,044
– влияние личностных факторов (неумеренные амбиции участников проекта, переоценка собственных возможностей, преувеличение роли технологической стороны в ущерб менеджменту)	25	10	0,025	
– риск недоступности персонала, которому сложно подобрать замену (болезнь, увольнение и другие непредвиденные обстоятельства)	20	10	0,02	

Таком образом, проведя расчеты рисков проекта и проанализировав их можно сказать, насколько критичным является воздействие конкретной угрозы на ресурс с учетом вероятности ее реализации.

Максимальным уровнем угрозы обладает риск изменения или недостатка бюджета – 0,8328. Минимальный уровень угрозы – 0,0025, соответствует риску влияния стихийных бедствий и природных катастроф.

3.6 Структурное разбиение работ

Структура разбиения работ представляет собой описание деятельности, необходимой для осуществления процесса модернизации системы защиты информации. Она является эффективным инструментом для четкого определения работ и сопоставления плана проекта с потребностями заказчика, необходимых для реализации проекта.

ИСПДн 1. Проектирование;

ИСПДн 1.1. Определение ключевых показателей существующих бизнес-процессов с точки зрения ИБ;

ИСПДн 1.2. Анализ проблем и слабых мест существующих бизнес процессов;

ИСПДн 1.3. Разработка значений ключевых показателей новых бизнес-процессов;

ИСПДн 1.4. Анализ и выбор наилучших способов и методов улучшения значений ключевых показателей бизнес-процессов;

ИСПДн 1.5. Разработка и согласование структуры новых бизнес-процессов.

ИСПДн 2. Совершенствование организационно-распорядительной документации;

ИСПДн 2.1. Технический паспорт;

ИСПДн 2.2. Инструкция по антивирусной защите;

ИСПДн 2.3. Согласование и утверждение ОРД.

ИСПДн 3. Подготовка реализации проекта создания системы защиты персональных данных;

ИСПДн 3.1. Определение ответственных лиц и исполнителей проекта;

ИСПДн 3.2. Приобретение СЗИ от НСД;

ИСПДн 3.3. Приобретение файрвола;

ИСПДн 3.4. Приобретение антивирусного ПО.

ИСПДн 4. Внедрение;

ИСПДн 4.1. Установка и настройка СЗИ от НСД;

ИСПДн 4.2. Установка и настройка антивирусного ПО;

ИСПДн 4.3. Установка и настройка файрвола;

ИСПДн 4.4. Обучение пользователей;

ИСПДн 4.5. Контроль защищенности.

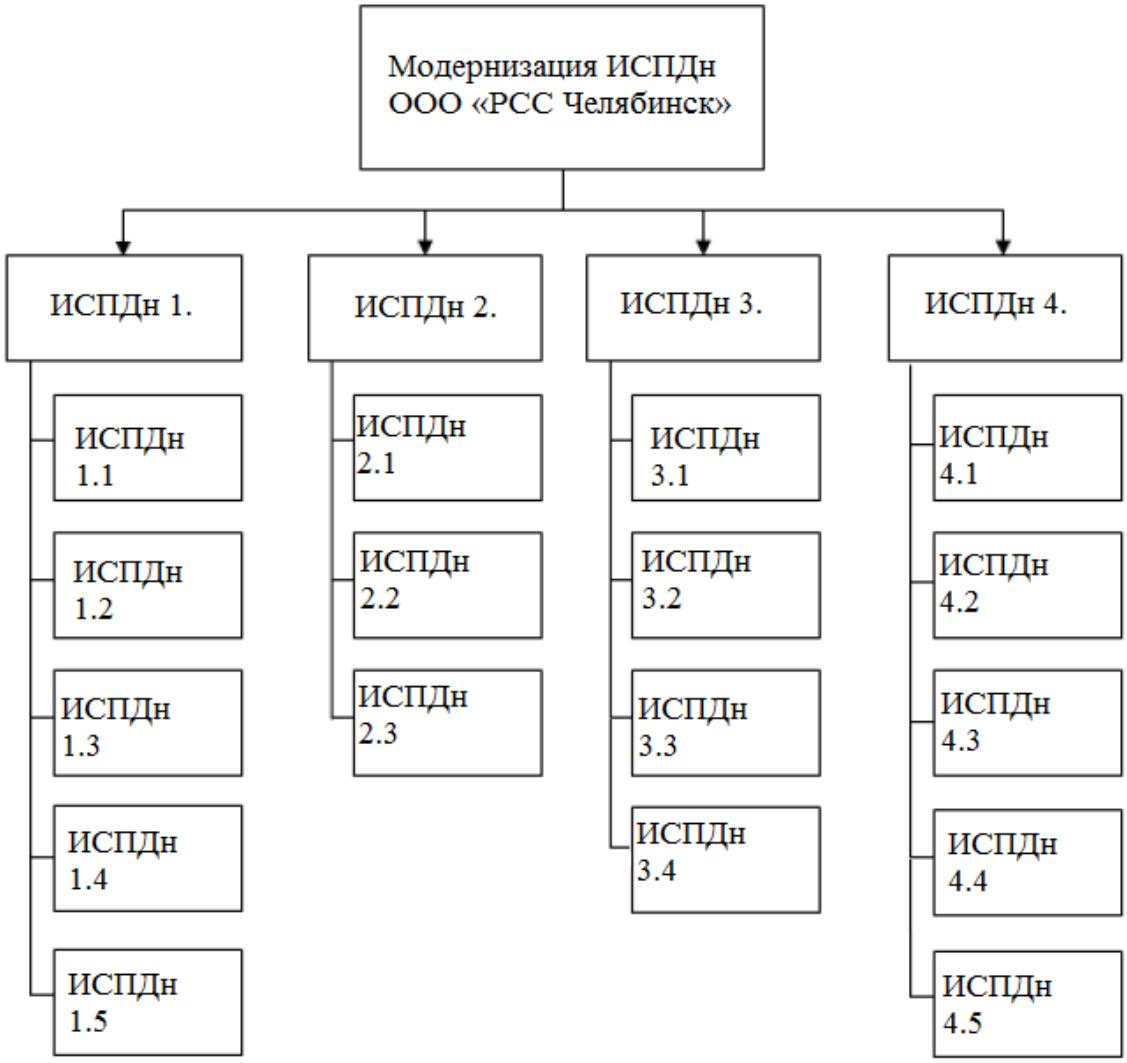


Рисунок 1 – Структура разбиения работ

3.7 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 2.

Рисунок 2 – Структурная схема организации проекта

3.8 Матрица ответственности

Матрица ответственности позволит установить степень ответственности каждого из сотрудников организации, участвующих в проекте. Для каждого из возможных действий установим обозначения:

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

В соответствии со структурой разбиения работ и структурной схемой организации проекта составим матрицу. Матрица ответственности представлена в таблице 13.

Таблица 13- Матрица ответственности

Исполнитель/Работа	1	2	3	4
ИСПДн 1.	К/У			
ИСПДн 1.1.	К		И	
ИСПДн 1.2.	К		И/К	
ИСПДн 1.3	К		И/К	
ИСПДн 1.4.	К		И	
ИСПДн 1.5.	К		И/К	
ИСПДн 2.	К		У/И	
ИСПДн 2.1.	К		У/И	
ИСПДн 2.2.	К		У/И	
ИСПДн 2.3.	К		У/И	
ИСПДн 3.	К			
ИСПДн 3.1.	К			
ИСПДн 3.2.	К		И	
ИСПДн 3.3.	К		И	
ИСПДн 3.4.	К		И	
ИСПДн 4.	К			
ИСПДн 4.1.	К	И		
ИСПДн 4.2.	К	И		
ИСПДн 4.3.	К	И		
ИСПДн 4.4.	К			И
ИСПДн 4.5.	К		И	

3.9 Диаграмма Гранта и сетевой график

Диаграмма Ганта используется для иллюстрации плана, графика работ по выбранному проекту. Для проекта усовершенствования СЗИ ООО «РСС Челябинск» была построена диаграмма Ганта, представленная в Приложении Д.

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 проекта создания системы защиты персональных данных на предприятии ООО «РСС Челябинск» представлен в Приложении Е.

3.10 Расчёт бюджета проекта и эго эффективности

В результате предпроектного обследования были выявлены уязвимости в системе, в связи с чем необходимо модернизацию системы защиты информации. Был проведен расчёт затрат на реализацию предложенных мер защиты. В таблице 14 представлена стоимость оборудования и программного обеспечения.

Таблица 14 – Стоимость оборудования и программного обеспечения

Наименование	Количество	Цена за шт. (руб.)	Сумма (руб.)
СЗИ от НСД «Secret Net 7»	2	7 700	15 400
Межсетевой экран «TrustAccess1.3»	2	1 975	3 950
Антивирусное ПО « Kaspersky Endpoint Security 10 для Windows»	2	1 633	3 266
		Итог	22 616

Стоимость реализации проекта приведена в таблице 15.

Таблица 15 – Стоимость реализации проекта

Наименование	Стоимость (руб.)
Анализ существующей СЗИ	12 000
Разработка организационно-распорядительной документации	8 000
Установка и настройка СЗИ от НСД «Secret Net 7»	6 000
Установка и настройка ПАК доверенной загрузки «Dallas Lock»	5 500
Установка и настройка антивирусного ПО «Kaspersky Endpoint Security 10 для Windows»	3 500
Установка и настройка межсетевого экрана «TrustAccess1.3»	4 500
Итог	39 500

Итого, общая стоимость по модернизации системы защиты информации информационной системы ООО «РСС Челябинск» составляет 61661.

Чтобы определить, будет успешным тот или иной проект финансовыми специалистами используется определенный метод оценки проектов – NPV.

Таблица 16 – Чистая приведенная стоимость проекта

Периоды	0	1	2	3	4
Первоначальные инвестиции	-61 661				
Выгоды		3 912 418	3 912 418	3 912 418	3 912 418
Стоимость годовой поддержки			-10 000	-10 000	-10 000
Затраты на поддержание инфраструктуры			-12 000	-12 000	-12 000
Итого	-61 661	3 912 418	3 890 418	3 890 418	3 890 418

NPV — это сокращение по первым буквам фразы «Net Present Value» и расшифровывается это как чистая приведенная (к сегодняшнему дню) стоимость. Это метод оценки инвестиционных проектов, основанный на методологии дисконтирования денежных потоков. Рассчитывается NPV по Формуле (3):

$$NPV = \sum_{t=0}^{n} \frac{CF_t}{(1+R)^t}, \quad (3)$$

где CF – денежный поток;
R – стоимость капитала (ставка дисконтирования);
n, t – количество временных периодов.

Ставку дисконтирования примем эквивалентной ключевой ставке центрального банка – 7,25 %.

NPV = -61440 + 3912418⁄1,0725 + 3890418⁄1,0725^2 + 3890418⁄1,0725^3 = -61661 + 3647942,2 + 3382218,5 + 3153583,7 = 10122083,4

Так как NPV больше нуля, значит данный проект создания системы защиты персональных на предприятии ООО «РСС Челябинск» выгоден.

ВЫВОД ПО ТРЕТЬЕЙ ГЛАВЕ

В результате выполненных работ была модернизирована система защиты персональных данных ООО «РСС Челябинск». Причиной модернизации послужила необходимость обновления и улучшения средств защиты, используемых в АС «Клиенты» ООО «РСС Челябинск». В ходе работ по модернизации были установлены средства защиты от НСД, средства антивирусной защиты и файрвол. Также была разработана инструкция по антивирусной защите для пользователей АС «Клиенты». Все работы были упорядочены и структурированы. Для каждого этапа разработан график, который позволяет контролировать сроки выполнения и объемы работ.

Итогом работ является введение в эксплуатацию модернизированной системы защиты, которая удовлетворяет всем требованиям законодательства в сфере защиты информации и способна адекватно реагировать на все виды угроз данной информационной системе.

Так же были рассчитаны риски проекта, проведено разбиение работ и составлена матрица ответственности.

Расчёт бюджета проекта и его эффективности показал, что на реализацию данного проекта потребуется 61661 рубль. Срок реализации проекта занял чуть больше двух месяцев. Учитывая стоимость информационных ресурсов предприятия, модернизация будет целесообразна. Все это подтверждает, что проект по модернизации системы защиты эффективен.

ЗАКЛЮЧЕНИЕ

В результате проведения выпускной квалификационной работы был проведен анализ состояния защиты информации на предприятии ООО «РСС Челябинск». В ходе предпроектного обследования были выявлены уязвимости в существующей системе защиты информации и отсутствие части организационно-распорядительной документации в области защиты информации. По этой причине были разработаны необходимые организационно-распорядительные документы и установлены программно-аппаратные средства защиты информации.

Результатами выпускной квалификационной работы стали:

- разработан технический паспорт на автоматизированную систему – был проведен осмотр помещений и технических средств, составлены их перечни и схемы расположения;
- разработана модель деятельности предприятия – построены диаграммы, позволяющие выявить потоки защищаемой информации;
- разработана модель угроз и уязвимостей для автоматизированной системы и рассчитаны риски на основе базовой модели угроз безопасности ФСТЭК и методики определения актуальных угроз ФСТЭК;
- разработано техническое задание на модернизацию системы защиты информации на предприятии ООО «РСС Челябинск»;
- проведена оценка экономической эффективности проекта, по ее результатам внедрение системы защиты экономически целесообразно;
- установлены программно-аппаратные средства защиты информации:
  - межсетевой экран «TrustAccess1.3»;
  - антивирусное ПО « Kaspersky Endpoint Security 10 для Windows »;
  - СЗИ от НСД «Secret Net 7».

Итогом проведённой работы является модернизированная система защиты ПДн, отвечающая всем требованиям законодательства.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. «О персональных данных»: федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ : (ред. от 24.11.2014) // КонсультантПлюс. Технология 3000 : Интернет-версия [Электрон-ный ресурс] / ЗАО «КонсультантПлюс». – Электрон. дан. и прогр. – М., 2017.

2. Нормативно-методический документ. «Специальные требования и рекомендации по технической защите конфиденциальной информации». Утвержден приказом Гостехкомиссии России от 30 августа 2002 г. № 282: (ред. от 30.08. 2002) — М., 27с.

3. Указ Президента РФ "Об утверждении перечня сведений конфиденциального характера" от 6 марта 1997 г. N 188: (ред. от 13.07.2015)// Гарант: Интернет-версия [электронный ресурс] / ЗАО «Гарант». – Электрон. дан. и прогр. – М., 2017

4. Руководящий документ. Автоматизированные системы. «Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. — М., 29с.

5. Приказ «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», ФСТЭК от 11.02.2013: (ред. от 15.02.2017)// ФСТЭК: Интернет-версия [электронный ресурс]. – Электрон. дан. и прогр. – М., 2017

6. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», ФСТЭК от 15.02.2008: (ред. от 09.01.2008)// ФСТЭК: Интернет-версия [электронный ресурс]. – Электрон. дан. и прогр. – М., 2017

7. Методический документ: «Методика определения угроз безопасности информации в информационных системах», ФСТЭК от 2015: (ред. от 11.05.2015)// ФСТЭК: Интернет-версия [электронный ресурс]. – Электрон. дан. и прогр. – М., 2017

8. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», ФСТЭК от 14.02.2008: (ред. от 14.02.2008)// ФСТЭК: Интернет-версия [электронный ресурс]. – Электрон. дан. и прогр. – М., 2017

9. ГОСТ 34.602–1989 «Техническое задание на создание автоматизированной системы». — М.: Изд-во стандартов, 1989. — 48 с.

10. ГОСТ Р 50922-2006.Защита информации. Основные термины и определения. – Введ. 2008–02–01. – М.: Госстандарт России, 2001.– 12 с.

11. СанПиН 2.2.2/2.4.1340-03 «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы». – М.: Минздрав России, 2003.– 42 с.

12. СанПиН 2.2.4.3359-16 «Санитарно-эпидемиологические требования к физическим факторам на рабочих местах». – М.: Минздрав России, 2016.– 64 с.

13. Справочная информация: «Правила устройства электроустановок (ПУЭ)». – М.: 2001.– 12 с.

14. Постановление Правительства РФ «О противопожарном режиме» от 25.04.2012 N 390: (ред. от 21.03.2017))// Гарант: Интернет-версия [электронный ресурс] / ЗАО «Гарант». – Электрон. дан. и прогр. – М., 2017

15. Федеральный закон "Технический регламент о требованиях пожарной безопасности" от 22.07.2008 N 123-ФЗ: (ред. от 21.03.2017))// Гарант: Интернет-версия [электронный ресурс] / ЗАО «Гарант». – Электрон. дан. и прогр. – М., 2017

16. Постановление правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»: постановление правительства Российской Федерации от 01.11.2012 № 1119 // КонсультантПлюс. Технология 3000: Интернет-версия [Электронный ресурс] / ЗАО «КонсультантПлюс». – Электрон. дан. и прогр. – М., 2016.

ПРИЛОЖЕНИЕ А

УТВЕРЖДАЮ
Генеральный директор Общества с ограниченной ответственностью «РСС Челябинск»

_____
«____» _____ 2018 г.

ТЕХНИЧЕСКИЙ ПАСПОРТ
на объект информатизации
АС «Клиенты»

Общества с ограниченной ответственностью «РСС Челябниск»

СОСТАВИЛ

_____ А.С. Зуев

«____» _____ 2018 г.

2018 г.

1 ОБЩИЕ СВЕДЕНИЯ ОБ ОБЪЕКТЕ

1.1 Наименование объекта: АС «Клиенты» Общества с ограниченной ответственностью «РСС Челябинск».

1.2 Расположение объекта: Челябинская обл., г. Челябинск, ул. Керченская, д. 6, 1 этаж, кабинет №4.

2 СОСТАВ ОБОРУДОВАНИЯ ОБЪЕКТА

2.1 Состав основных технических средств и систем (ОТСС) объекта информатизации отражен в таблице 2.1.

Таблица 2.1 – Перечень ОТСС, входящих в состав АС «Клиенты»

Наименование устройства	**Фирма производитель, модель**	**Заводской / инвентаризационный номер**	**Расположение**
ПЭВМ1			
Системный блок	InWin BM677	1ABMAGE000030	Рисунок 2.1
НЖМД	WD WD5000AAKS-22A7B0	WCASY2495047	Рисунок 2.1
Монитор	Benq ET-0034-N	ETT9902134026	Рисунок 2.1
Клавиатура	MITSUMI KFK-EB9HY	KFKEB9HY518B0011	Рисунок 2.1
Мышь	Genius NetScroll EYE	136703402193	Рисунок 2.1
ИБП	DNS SMART PRO LCD 1000VA	1108210223	Рисунок 2.1
ПЭВМ2			
Системный блок	InWin BM677	1ABMAGE000183	Рисунок 2.1
НЖМД	WD WD5000AAKS-22A7B0	WCASY2495089	Рисунок 2.1
Монитор	Benq ET-0034-N	ETT9902134041	Рисунок 2.1
Клавиатура	MITSUMI KFK-EB9HY	KFKEB9HY518B0273	Рисунок 2.1
Мышь	Genius NetScroll EYE	136703402462	Рисунок 2.1
ИБП	DNS SMART PRO LCD 1000VA	1108210248	Рисунок 2.1
Средство печати			
Принтер	Samsung SCX-4600	Z2VJBFFSC00519K	Рисунок 2.1

2.2 Состав вспомогательных технических средств и систем (ВТСС) объекта, установленных в помещении объекта информатизации отражен в таблице 2.2.

Таблица 2.2 – Перечень ВТСС АС «Клиенты»

№	Наименование устройства	Фирма производитель, модель	Заводской / инвентаризационный номер	Расположение
1	Телефонный аппарат	Panasonic KX-T 7630RU	T7630RUV4-N1A	Рисунок 2.2
2	Телефонный аппарат	Panasonic KX-T 7630RU	T7630RUV4-N3A	Рисунок 2.2
3	Датчик пожарной сигнализации	ИП 212-45	61506053432	Рисунок 2.2
4	Коммутатор	TP-LINK Archer C7	135A2400354	Рисунок 2.2
5	Датчик охранной сигнализации	н/а	н/а	Рисунок 2.2

2.3 Схема размещения и расположения ОТСС на объекте с привязкой к границам контролируемой зоны.

Структура, топология и размещение ОТСС и ВТСС объекта относительно границ контролируемой зоны объекта приведены на рисунках 2.1 – 2.3.

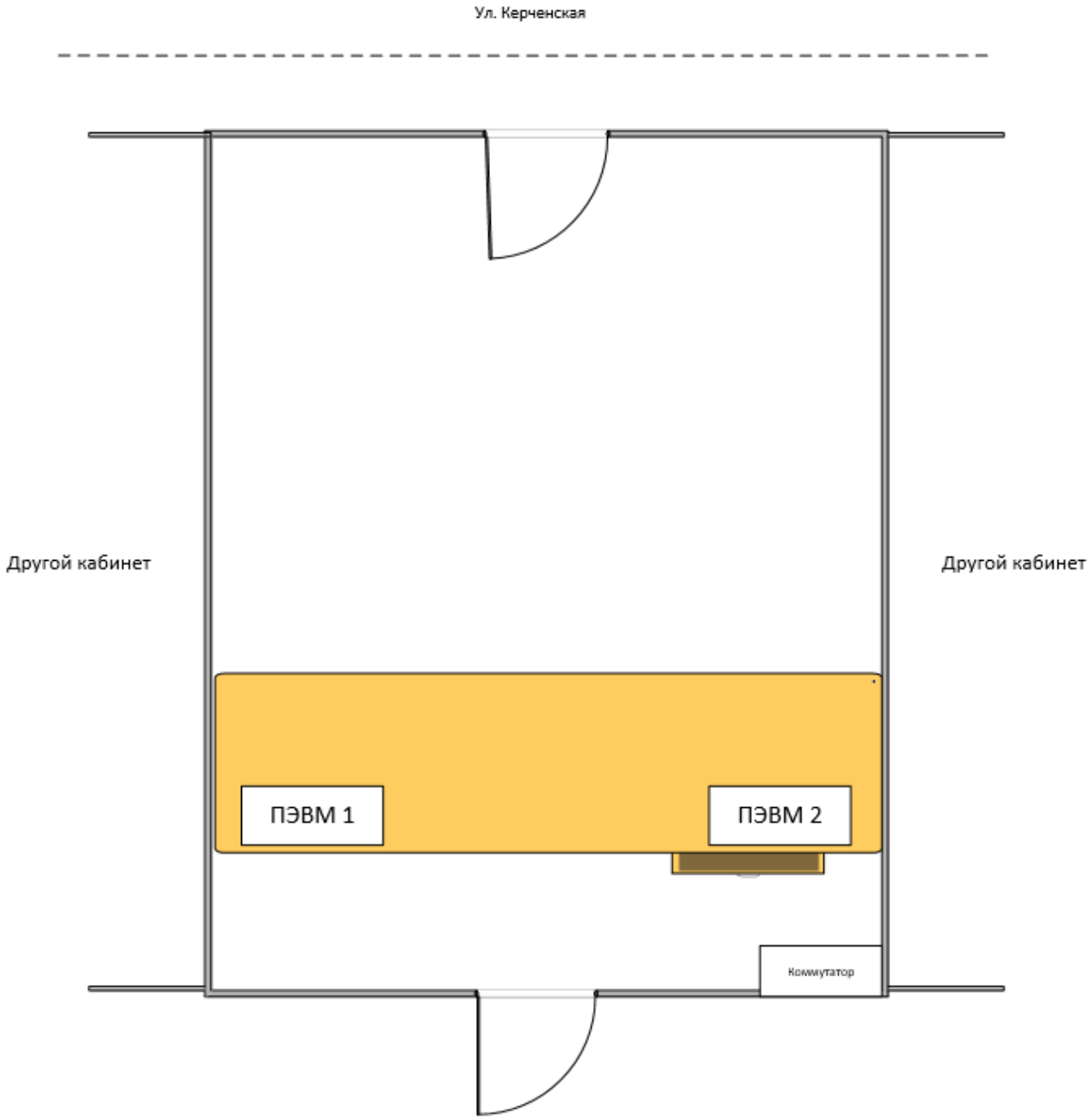


Рисунок 2.1 – Размещение ОТСС АС «Клиенты»

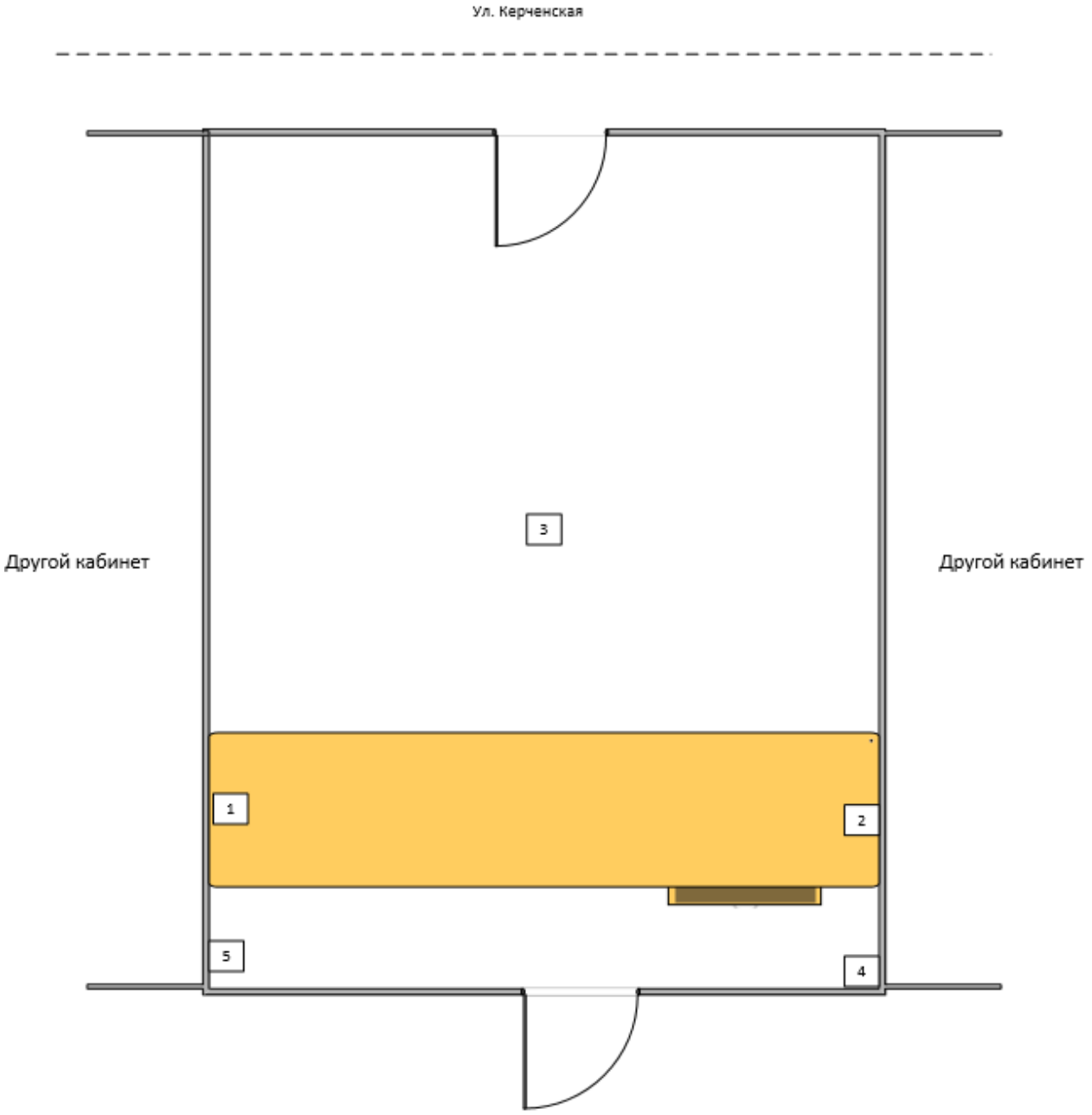


Рисунок 2.2 – Размещение ВТСС АС «Клиенты»
*Примечание: Обозначения 1-5 приведены в Таблице 2.2 основной части технического паспорта.

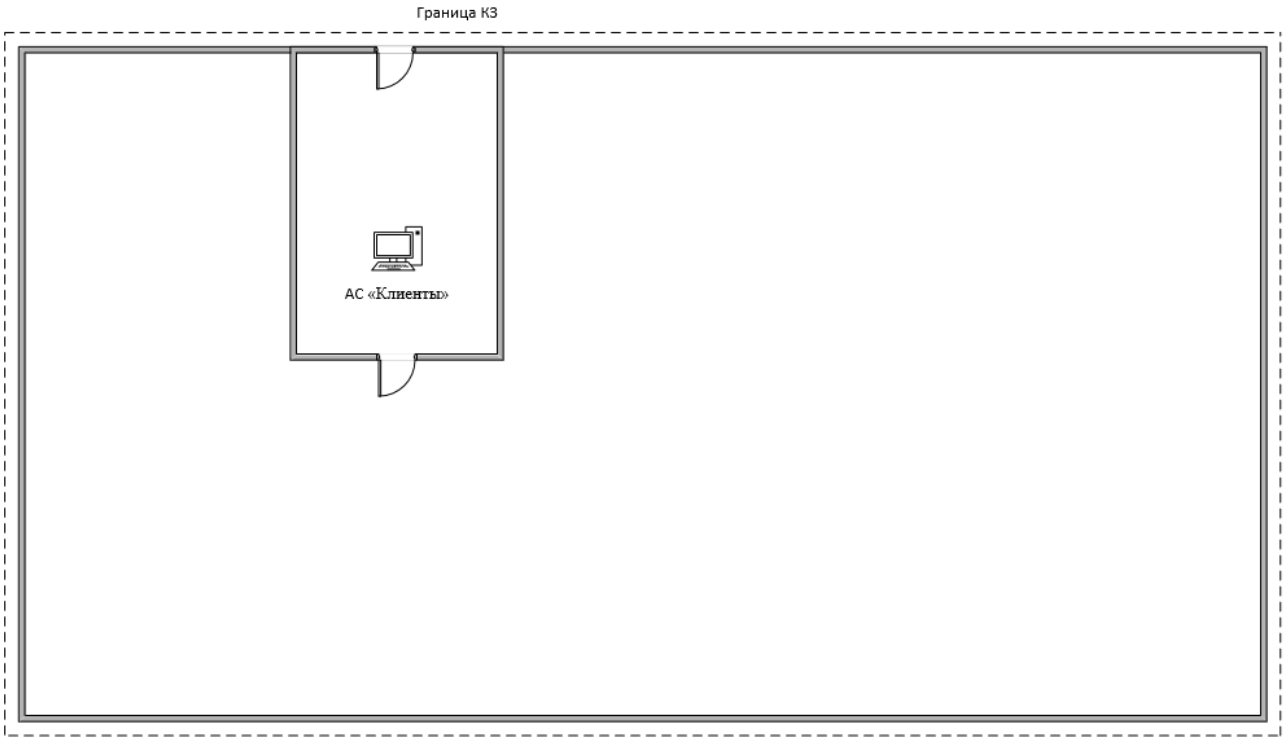


Рисунок 2.3 – Размещение ОТСС относительно границ контролируемой зоны

Границей контролируемой зоной являются ограждающие конструкции здания, в котором находится офис Общества с ограниченной ответственностью «РСС Челябинск» Челябинская обл., г. Челябинск, ул. Керченская, д. 6.

Кабинет располагается на первом этаже. Окно выходит на ул. Керченская, завешано жалюзи. Минимальное расстояние от ОТСС до КЗ составляет 2,2 метра.

2.4 Размещение ВТСС, линий приведено на рисунке 2.4.

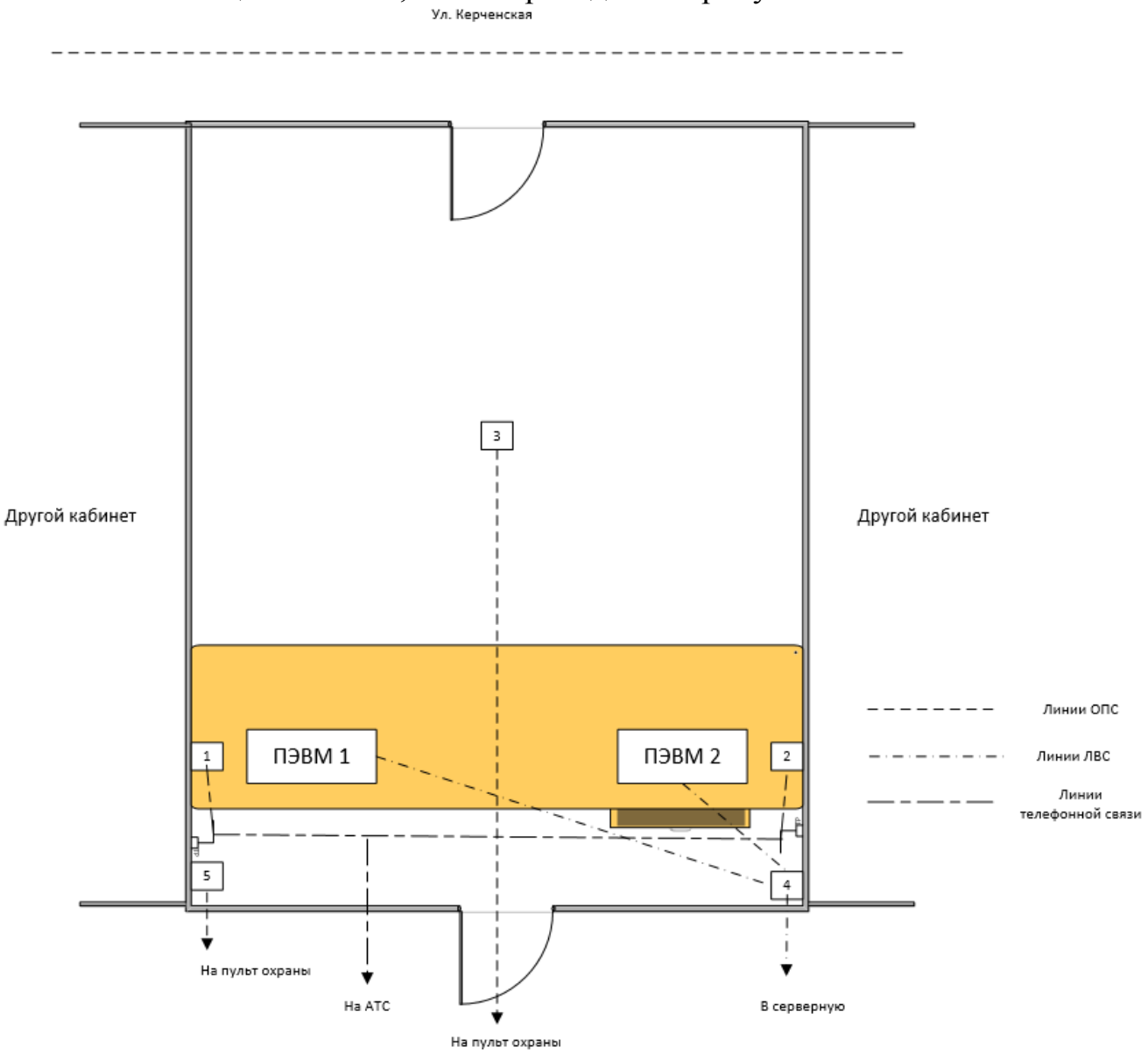


Рисунок 2.4 – Размещение ВТСС, расположение линий

*Примечание: Обозначения 1-5приведены в Таблице 2.2 основной части технического паспорта

2.5 Размещение системы электропитания, заземления и инженерных коммуникаций приведено на рисунке 2.5.

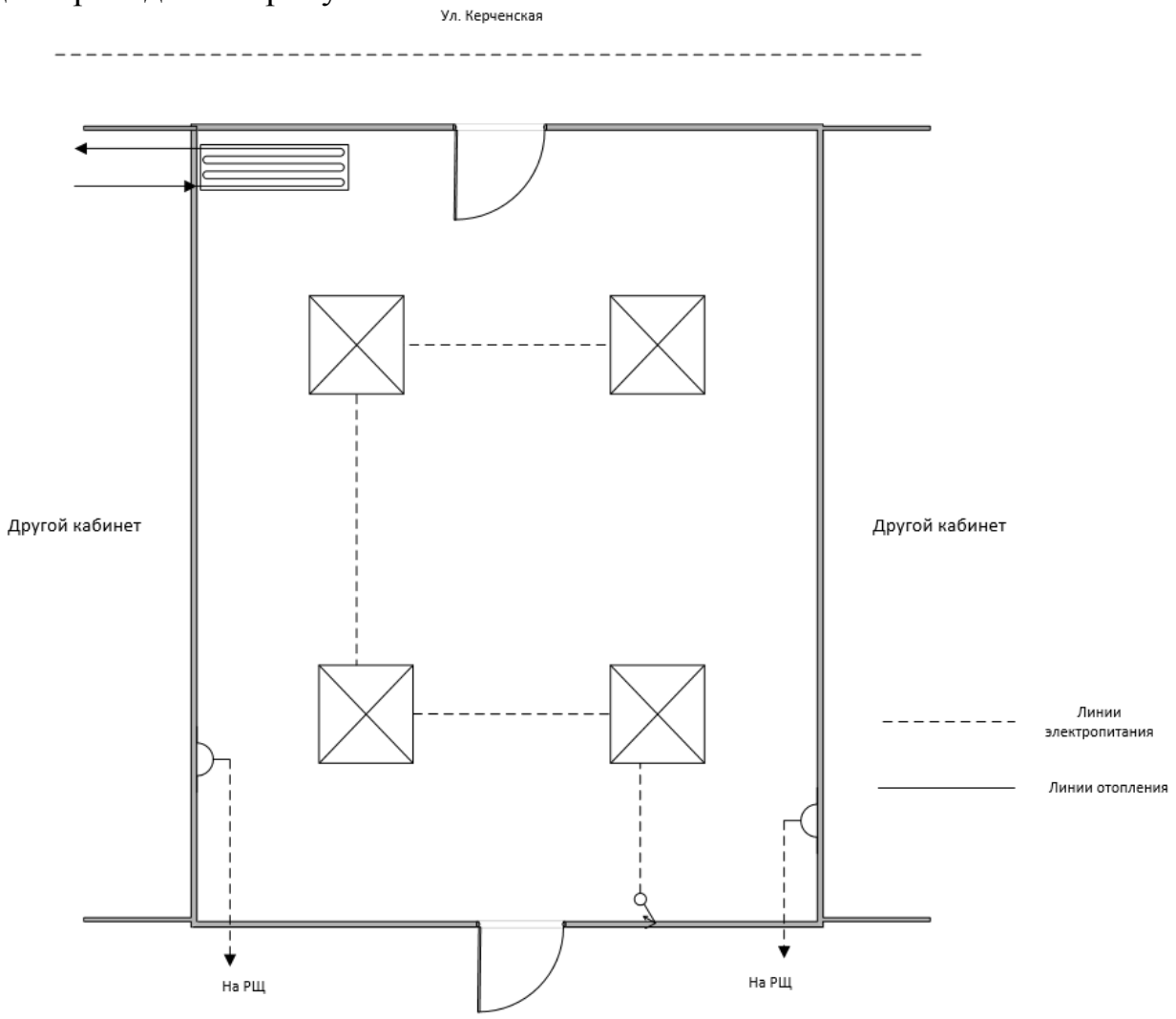


Рисунок 2.5 – Размещение системы электропитания, заземления и инженерных коммуникаций

Наименование линии	**Выходит за пределы КЗ (выходит/не выходит)**
Линия электропитания	не выходит
Линия заземления	не выходит
Линия охранной сигнализации	не выходит
Линия пожарной сигнализации	не выходит
Линия телефонной связи	выходит
Линия ЛВС	выходит
Линия отопления	выходит
Линия вентиляции	не выходит

2.6 Перечень средств защиты информации, установленных на объекте информатизации АС «Клиенты» приведен в Таблице 2.3.

Таблица 2.3 – Перечень средств защиты, установленных на АС «Клиенты»

Наименование и тип технического средства	**Заводской номер/СЗЗ**	**Сведения о сертификате**	**Расположение**
Антивирусное ПО «360 Total Security »		-	В ПЭВМ

2.7 Перечень программных средств, установленных на объекте информатизации АС «Клиенты» приведен в Таблице 2.4.

Таблица 2.4 – Перечень ПО установленного на АС «Клиенты»

Наименование ПО	**Версия**
Microsoft Windows 7 Professional SP1	6.1
MS Office	16.0.4266.1001
360 Total Security	8.2.0.1034
1C	2.1.11.5
Chrome	48.0.2564.109
Bitrix24	3.1.88.23

3 СВЕДЕНИЯ ОБ АТТЕСТАЦИИ ОБЪЕКТА ИНФОРМАТИЗАЦИ НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ ПО БЕЗОПАСНОСТИ ИНФОРМАЦИИ

3.1 Протоколы испытаний и даты их регистрации

3.2 Сведения об аттестации объекта информатизации на соответствие требованиям по безопасности информации:

Заключение по результатам аттестационных испытаний объекта информатизации №

Аттестат соответствия №

4 УЧЕТ ПРОВЕДЕНИЯ РЕГЛАМЕНТНЫХ ПРОВЕРОК

Таблица 4.1 – Учет проведения регламентных проверок

Наименование организации, проводившей проверку	Дата проведения проверки	Номер протокола	Примечание

5 ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Таблица 5.1 – Лист регистрации изменения состава и размещения ОТСС, ВТСС и средств защиты объекта информатизации

Дата внесения изменений	Наименование документа, фиксирующего изменения	Номера заменённых (исправленных) листов формуляра	Подпись лица, внесшего изменения

ПРИЛОЖЕНИЕ Б

«УТВЕРЖДАЮ»
Генеральный директор
ООО «РСС Челябинск»
Д.А.Балохин
«___» _____2017 г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ
на модернизацию системы защиты персональных данных на предприятии ООО «РСС Челябинск»

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Полное наименование работы и ее условное обозначение

Полное наименование системы: Система защиты автоматизированной системы обработки персональных данных, в обществе с ограниченной ответственностью «РСС Челябинск».

Полное наименование работы: выполнение работ по модернизации системы защиты автоматизированной системы обработки персональных данных в обществе с ограниченной ответственностью «РСС Челябинск».

Условное обозначение работы: выполнение работ по модернизации системы защиты персональных данных.

1.2. Наименование заказчика и исполнителя

Предприятие разработчик системы: ООО «РСС Челябинск», в лице главного специалиста по защите информации.

Предприятие заказчик системы: ООО «РСС Челябинск», в лице генерального директора.

1.3. Перечень документов, на основании которых модернизируется система:

– Федеральный закон от 27 июля 2007 года N 152-ФЗ «О персональных данных»

– Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

– Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

– Трудовой кодекс РФ от 30.12.2001 N 197-ФЗ;

1.4. Порядок оформления и предъявления заказчику результатов работ по созданию системы (ее частей), по изготовлению и наладке отдельных средств (технических, программных, информационных) и программно-технических (программно-методических) комплексов системы

Результаты работы оформляются и предъявляются заказчику по мере исполнения в виде минимальных независимых частей проекта и/или предварительных проектов. Окончательный вариант проекта предоставляется на рассмотрение заказчику после главного специалиста по защите информации ООО «РСС Челябинск».

2. НАЗНАЧЕНИЕ И ЦЕЛИ МОДЕРНИЗАЦИИ СИСТЕМЫ

2.1. Назначение модернизации системы

В связи с постоянным ростом информационных потоков, соответственно растет и количество возможных угроз информационной безопасности. Для эффективного противодействия этим угрозам необходима современная и надёжная система защиты персональных данных.

2.2. Цели модернизации системы

Основной целью проведения работ является приведение всех этапов работы с информации в автоматизированной системе обработки персональных данных ООО

«РСС Челябинск» в соответствие требованиям перечисленных в данном Техническом задании.

3. ХАРАКТЕРИСТИКА ОБЪЕКТОВ ЗАЩИТЫ

3.1. Краткие сведения об объектах защиты

Объектом защиты является автоматизированная система обработки персональных данных, представляющая из себя два автоматизированных рабочих места, носителей информации ограниченного доступа, помещение, в котором расположена автоматизированная система:

1. Автоматизированные рабочие места:
   – АРМ АС «Клиенты».
2. Помещения для хранения и работы с важной защищаемой информацией:
   – Кабинет отдела персонала.
3. Линии и средства связи, системы обеспечения функционирования СВТ и деятельности организации:
   – Линии проводной городской телефонной связи;
   – Система электропитания;
   – Линии охранной и пожарной сигнализации;
   – Линии локальной компьютерной сети.
4. Средства ввода-вывода и отображения информации:
   – Мониторы сотрудников отдела;
   – Принтер Samsung SCX-4600;
5. Система бесперебойного питания АРМ:
   – Источники бесперебойного питания АРМ сотрудников.
6. Носители информации:
   – Бумажные носители информации ограниченного доступа;
   – Электронные (флэш-накопители с документами, содержащими информацию ограниченного доступа);
   – Персонал.
7. Персонал:
   – Сотрудники отдела.

3.2. Сведения об условиях эксплуатации объекта защиты и характеристиках окружающей информационной среды

3.2.1. Объекты защиты подвержены воздействию следующих угроз:

3.2.1.1. АРМ:

– Уничтожение информации в случае повреждения носителей информаци;

– Несанкционированный доступ к информации в системе, хранящейся на АРМ.

3.2.2. Присутствуют следующие уязвимости:

3.2.2.1. АРМ:

- Отсутствие межсетевого экрана;
- Отсутствие надёжной антивирусной защиты;
- Отсутствие документации по эксплуатации СЗИ.

4. СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО МОДЕРНИЗАЦИИ СИСТЕМЫ

Работы должны проводиться в соответствии с положениями, перечисленными в данном Техническом задании.

Работы должны проводиться в два этапа: Приведение в соответствие с нормативно-правовыми актами порядка обработки персональных данных, проверка технических средств обработки информации.

4.1. Приведение в соответствие с нормативно-правовыми актами порядка обработки персональных данных

Список необходимых к проведению работ относительно автоматизированной системы обработки персональных данных:

– Разработка нормативно-правовой документации: Акта обследования АС, акта классификации АС, инструкции по эксплуатации СЗИ, технического паспорта;

– Изучение существующих организационных мер обеспечения безопасности информации ограниченного доступа;

– Разработка актуализированной модели угроз;

– Разработка перечня требований по защите информации ограниченного доступа;

– Выявление имеющихся средств технической защиты информации и мер, которые применяются для обеспечения безопасности персональных данных;

– Анализ соответствия применяющихся мер и средств технической защиты предъявляемым требованиям нормативно-правовой базы Российской Федерации в области защиты персональных данных.

4.2. Проверка технических средств обработки информации

Список необходимых к проведению работ относительно автоматизированной системы обработки персональных данных:

– Определение условий расположения технических средств обработки информации ограниченного доступа относительно границ контролируемой зоны;

– Определение линий и коммуникаций, расположенных в месте размещения технических средств обработки информации ограниченного доступа;

– Изучение существующих организационных мер обеспечения безопасности работоспособности и функционирования информационных систем;

– Покупка необходимых программных и технических средств, для обеспечения повышения защищенности автоматизированной системы;

– Обновление программных продуктов информационной системы до актуального состояния;

4.3. Порядок проведения работ:

4.3.1. Для выполнения работ Исполнитель привлекает специалистов Заказчика имеющих необходимую компетенцию.

4.3.2. Специалисты Заказчика временно переходят под руководство Исполнителя.

4.3.3. В ходе проведения работ Исполнитель собирает исходные данные путем:

– опроса персонала Заказчика, в том числе руководителей и сотрудников структурных подразделений;

– обследования АРМ и места его расположения;

– анализа документов и записей результатов деятельности Заказчика в части обеспечения безопасности информационных систем персональных данных (нормативных документов, проектной и эксплуатационной документации, актов, журналов и пр.).

5. ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ ГОТОВОЙ СИСТЕМЫ

5.1. Критериями для приемки работ является настоящее техническое задание и соответствующие частные Технические задания, разрабатываемые в процессе выполнения работ.

5.2. Приемка работ осуществляется единовременно.

5.3. Заказчик направляет замечания в письменном виде.

6. ТРЕБОВАНИЯ К СОСТАВУ И СОДЕРЖАНИЮ ПРОЕКТА РАБОТ ПО ПОДГОТОВКЕ ОБЪЕКТА ЗАЩИТЫ К ВВОДУ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ДЕЙСТВИЕ

При подготовке к проведению Исполнителем работ со стороны Заказчика необходимо обеспечить следующее:

– назначить ответственное лицо от Заказчика, наделенное соответствующими полномочиями, для обеспечения выполнения работ Исполнителем;

– определить лицо для организации и проведения опроса;

– обеспечить промежутки времени доступности лиц, АРМ и выделенного помещения.

7. ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

7.1. При разработке системы Исполнителем должны быть подготовлены следующие документы:

– Акт обследования автоматизированной системы;

– Акт классификации автоматизированной системы;

– Технический паспорт.

7.2. Отчетные документы предоставляются Заказчику в электронном виде в формате документов Microsoft Office и на бумажных носителях.

8. ДОПОЛНИТЕЛЬНЫЕ УСЛОВИЯ И ОГРАНИЧЕНИЯ

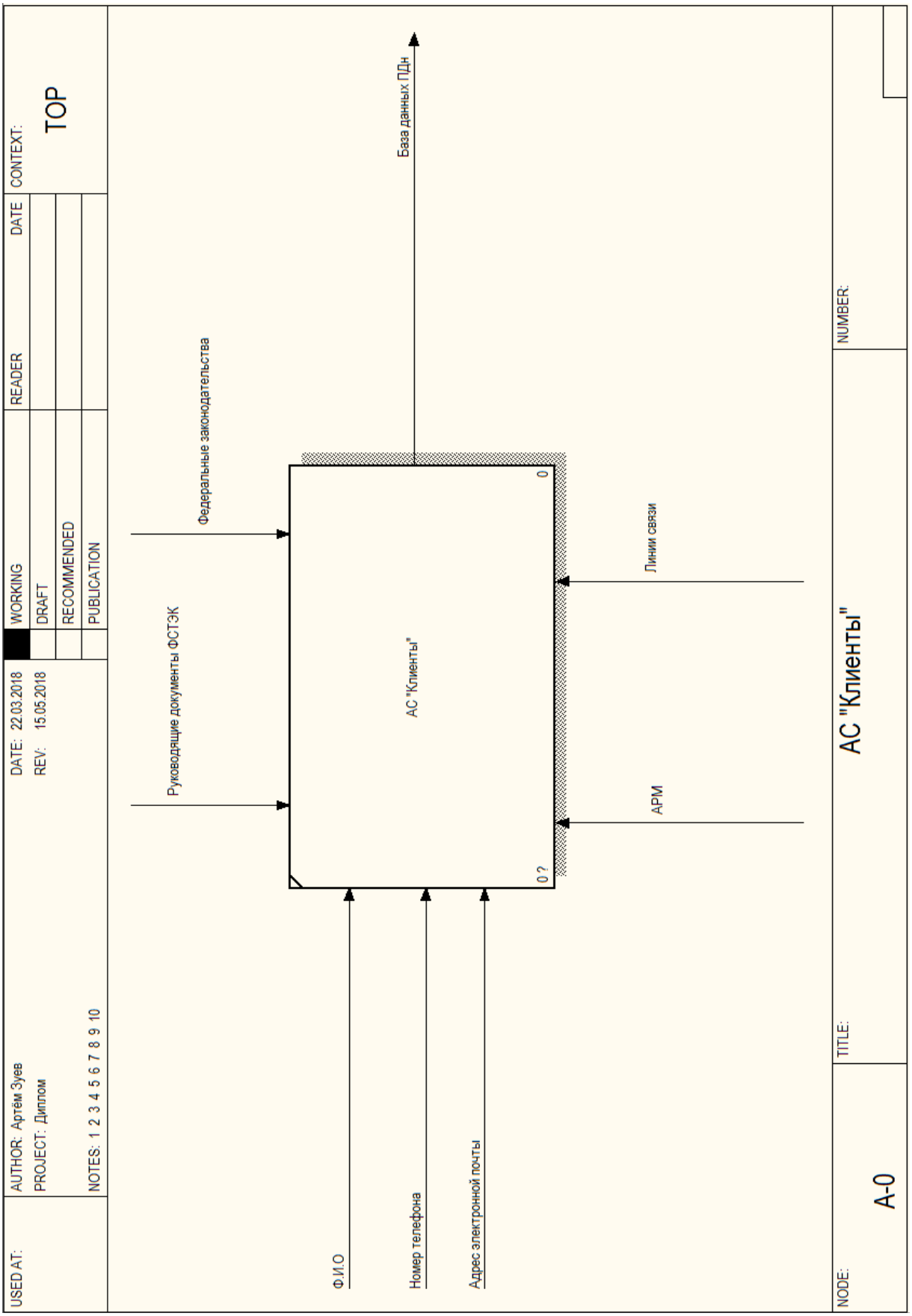
8.1. В случае поставки и внедрения технических средств защиты третьей стороной до начала работ по аттестации, Заказчик согласует с Исполнителем следующее:

– состав и спецификацию технических средств;
– состав сопроводительной документации к техническим средствам и сертификатов;
– схемы установки и подключения;
– настройки аппаратно-программных средств;
– рабочую документацию этапа внедрения.

8.2. Срок поставки и внедрения технических средств защиты не входит в расчет сроков этапов работ.

В случае задержки по срокам предоставления исходных данных при проведении работ, или неполного предоставления информации со стороны Заказчика, по согласованию сторон возможен перенос сроков выполнения работ по договору в сторону увеличения.

ПРИЛОЖЕНИЕ В



ПРИЛОЖЕНИЕ Г

УТВЕРЖДАЮ
Генеральный директор ООО «РСС Челябинск»

_____Д.А. Балохин
«____»_____ 2017 г.

ПЕРЕЧЕНЬ ПЕРСОНАЛЬНЫХ ДАННЫХ,
подлежащих защите в автоматизированной системе обработки персональных данных
АС «Клиенты»

№	Тип персональных данных, подлежащих защите
1.	Фамилия, Имя, Отчество
2.	Номер телефона
3.	Адрес электронной почты

Генеральный директор ООО «РСС Челябинск» _____ Д.А. Балохин

ПРИЛОЖЕНИЕ Д

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

Таблица 1 – Перечень работ и сроков

Название работы	Длительность	Начало	Окончание
1. Проектирование	17	16.02.2018	28.02.2018
1.1. Определение ключевых показателей бизнес-процессов с точки зрения ИБ	3	16.02.2018	19.02.2018
1.2. Анализ проблем и слабых мест существующих бизнес-процессов	2	20.02.2018	22.02.2018
1.3. Разработка значений ключевых показателей новых бизнес-процессов	3	24.02.2018	27.02.2018
1.4. Анализ и выбор наилучших способов и методов улучшения значений ключевых показателей бизнес-процессов	3	28.02.2018	2.03.2018
1.5. Разработка и согласование структуры новых бизнес-процессов	3	5.03.2018	7.03.2018
2. Совершенствование организационно-распорядительной документации	7	11.03.2018	18.03.2018
2.1. Технический паспорт	3	11.03.2018	13.03.2018
2.2. Инструкция по антивирусной защите	2	14.03.2018	15.03.2018
2.3. Согласование и утверждение ОРД	3	16.03.2018	18.03.2018
3. Подготовка реализации проекта создания системы защиты персональных данных	8	19.03.2018	26.03.2018
3.1. Определение ответственных лиц и исполнителей проекта	4	19.03.2018	22.03.2018
3.2. Приобретение СЗИ от НСД	1	23.03.2018	24.03.2018
3.3. Приобретение межсетевого экрана	1	24.03.2018	25.03.2018
3.4. Приобретение антивирусного ПО	1	25.03.2018	26.03.2018
4. Внедрение	18	2.04.2018	20.04.2018
4.1. Установка и настройка СЗИ от НСД	2	2.03.2018	4.04.2018
4.2. Установка и настройка межсетевого экрана	2	4.04.2018	6.04.2018
4.3. Установка и настройка антивирусного ПО	2	6.04.2018	10.04.2018
4.4. Контроль защищенности	3	10.04.2018	13.04.2018
4.5. Обучение пользователей	5	13.04.2018	20.04.2018

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

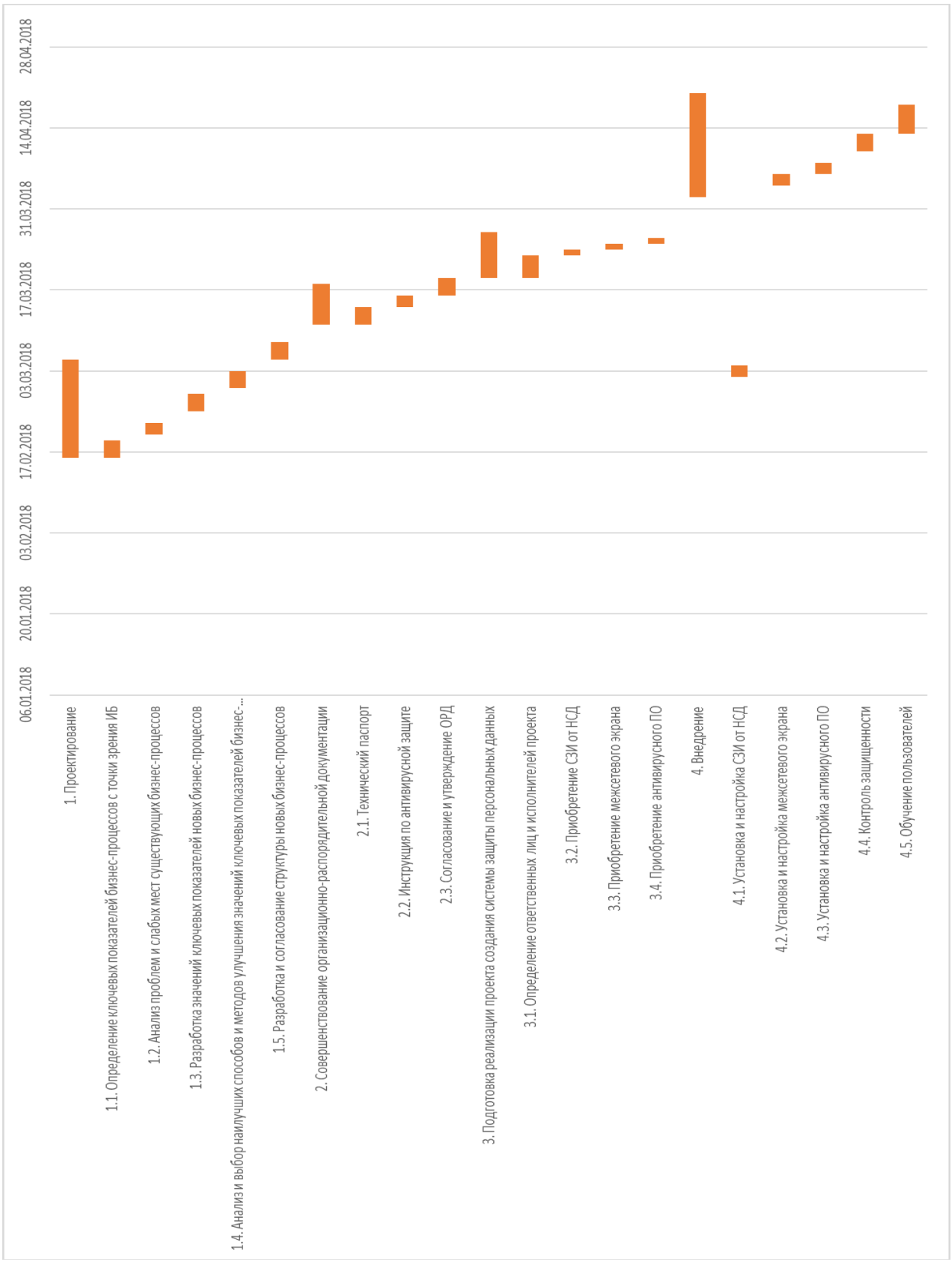


Рисунок 1 – Диаграмма Ганта

ПРИЛОЖЕНИЕ Е

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 работы	T	$T_{рн}$	$T_{пн}$	$T_{ро}$	$T_{по}$
	Проектирование	17	0	0	17	17
1-2	Определение ключевых показателей существующих бизнес-процессов с точки зрения ИБ	3	0	0	3	3
2-3	Анализ проблем и слабых мест существующих бизнес-процессов	2	3	3	5	5
3-4	Разработка значений ключевых показателей новых бизнес-процессов	3	5	5	8	8
4-5	Анализ и выбор наилучших способов и методов улучшения значений ключевых показателей бизнес-процессов	3	8	8	11	11
5-6	Разработка и согласование структуры новых бизнес-процессов	3	11	11	14	14
	Совершенствование ОРД	7	14	14	21	21
6-7	Технический паспорт	3	14	14	17	17
7-8	Инструкция по антивирусной защите	2	17	17	19	19
8-9	Согласование и утверждение ОРД	3	19	19	22	22
	Подготовка реализации проекта создания системы защиты персональных данных	8	22	22	30	30
9-10	Определение ответственных лиц и исполнителей проекта	4	22	22	26	26
10-11	Приобретение СЗИ от НСД	1	26	26	27	27
11-12	Приобретение межсетевого экрана	1	27	27	28	28
12-13	Приобретение антивирусного ПО	1	28	28	29	29
	Внедрение	18	29	29	47	47
13-14	Установка и настройка СЗИ от НСД	2	29	29	31	31
14-15	Установка и настройка межсетевого экрана	2	31	31	33	33
15-16	Установка и настройка антивирусного ПО	2	33	33	35	35
16-17	Контроль защищённости	3	35	35	38	38
17-18	Обучение пользоваталей	7	38	38	45	45

ПРИЛОЖЕНИЕ Ж

УТВЕРЖДАЮ

Генеральный директор ООО «РСС Челябинск»

_____Д.А. Балохин

«____»_____ 2018 г.

АКТ

классификации автоматизированной системы на базе АРМ
АС «Клиенты» ООО «РСС Челябинск»

Комиссия в составе:

- Д.А.Балохин. – директор ООО «РСС Челябинск», председатель комиссии;
- _____. – инженер по сопровождению электронного документооборота, член комиссии;
- _____. – инженер по сопровождению электронного документооборота, член комиссии;

рассмотрев исходные данные на АС «Клиенты» на базе автоматизированного рабочего места, расположенной по адресу: г. Челябинск, ул. Керченская, д. №6, условия её эксплуатации, режимы обработки информации **установила:**

1. Высший гриф конфиденциальности обрабатываемой информации в АС – «**для служебного пользования**».

2. В АС работает несколько пользователей, имеющих одинаковые права доступа к ресурсам.

3. Информация находится на носителях одного грифа конфиденциальности.

Классификация проводилась на соответствие требованиям Руководящего документа Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

Вывод: Исходя из вышеизложенных определяющих признаков, установлен класс защиты от несанкционированного доступа **2Б.**

Председатель комиссии: _____

Члены комиссии: _____

_____

ПРИЛОЖЕНИЕ З

УТВЕРЖДАЮ

Генеральный директор ООО «РСС Челябинск»

_____ И.О. Фамилия

«____» _____ 2017 г.

ИНСТРУКЦИЯ
ПО ОРГАНИЗАЦИИ АНТИВИРУСНОЙ ЗАЩИТЫ
в автоматизированной системе обработки персональных данных
АС «КЛИЕНТЫ»

2018 г.

ИНСТРУКЦИЯ

по антивирусной защите в информационных системах ООО «РСС Челябинск»

1 Общие положения

1.1 Настоящая Инструкция предназначена для всех сотрудников ООО «РСС Челябинск», имеющих доступ к информационным системам (ИС) «РСС Челябинск».

1.2 Инструкция устанавливает требования и ответственность при организации защиты информации от воздействия вредоносных компьютерных вирусов.

1.3 Инструкция регулирует вопросы организации антивирусной защиты и требования к порядку проведения антивирусного контроля при работе в ИС «РСС Челябинск».

2 Обеспечение антивирусной защиты

2.1 Порядок организации антивирусной защиты.

2.1.1 Для организации антивирусной защиты ИС «РСС Челябинск» допускаются к использованию только сертифицированные ФСТЭК России лицензионные антивирусные средства общего применения.

2.1.2 Антивирусное средство защиты должно быть установлено на все средства вычислительной техники (СВТ) (при наличии технической возможности), входящие в ИС «РСС Челябинск».

2.1.3 В ИС «РСС Челябинск» права по управлению (администрированию) средствами антивирусной защиты предоставлены только администратору информационной безопасности.

2.1.4 Разработка и осуществление мероприятий по проведению антивирусного контроля осуществляется ответственным за защиту информации с привлечением (при необходимости) администратора информационной безопасности и /или специалистов лицензированной организации.

2.1.5 Должностные лица не должны допускать использования в ИС «РСС Челябинск» программного обеспечения и данных, не связанных с выполнением должностных обязанностей.

В ИС «РСС Челябинск» обеспечивается централизованное управление (установка, удаление, обновление, конфигурирование и контроль актуальности версий программного обеспечения средств антивирусной защиты) средствами антивирусной защиты, установленными на компонентах информационной системы (автоматизированных рабочих местах).

2.1.6 В ИС «РСС Челябинск» обеспечивается централизованное управление обновлением базы данных признаков вредоносных компьютерных программ (вирусов).

2.1.7 Расширенный антивирусный контроль проводится администратором информационной безопасности не реже одного раза в месяц и при необходимости, в случае подозрений в заражении вирусной программой.

2.1.8 При загрузке, открытии или исполнении объектов (файлов) из внешних источников средствами антивирусной защиты проводится автоматическая проверка объектов (файлов).

2.1.9 В виртуальной инфраструктуре обеспечивается реализация и управление антивирусной защитой:

2.1.9.1 проверка наличия вредоносных программ (вирусов) в хостовой операционной системе, включая контроль файловой системы, памяти, запущенных приложений и процессов;

2.1.9.2 проверка наличия вредоносных программ в гостевой операционной системе, в процессе ее функционирования, включая контроль файловой системы, памяти, запущенных приложений и процессов.

2.2 Порядок проведения антивирусного контроля.

2.2.1 Устанавливаемое (изменяемое) программное обеспечение предварительно проверяется администратором информационной безопасности на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера, должна быть выполнена антивирусная проверка администратором информационной безопасности.

2.2.2 При загрузке компьютера средствами антивирусной защиты проводится антивирусный контроль в автоматическом режиме.

2.2.3 При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь ИС «РСС Челябинск» самостоятельно или вместе с администратором информационной безопасности проводит внеочередной антивирусный контроль своей рабочей станции для определения факта наличия или отсутствия компьютерного вируса.

2.2.4 В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователи ИС «РСС Челябинск» обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя и администратора информационной безопасности, владельца зараженных файлов, а также смежные подразделения, использующие

эти файлы в работе;

- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов;
- в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, направить зараженный вирусом файл на съемном носителе информации администратору информационной безопасности для дальнейшей передачи его в организацию, с которой заключен договор на антивирусную поддержку (при наличии);
- по факту обнаружения зараженных вирусом файлов составить служебную записку администратору информационной безопасности, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

2.3 Обновление базы данных признаков вредоносных компьютерных программ (вирусов).

2.3.1 Администратор информационной безопасности обеспечивает получение из доверенных источников и установку обновлений базы данных признаков вредоносных компьютерных программ (вирусов).

2.3.2 Контроль целостности обновлений базы данных признаков вредоносных компьютерных программ (вирусов) обеспечивается путем автоматического получения или предварительно скачиваемых обновлений из официальных источников, например, с сервера обновлений производителя антивирусного средства.

3 Ответственность при организации антивирусной защиты

3.1 Ответственность за организацию антивирусной защиты ИС «РСС Челябинск» в соответствии с требованиями настоящей Инструкции возлагается на администратора информационной безопасности.

3.2 Ответственность за соблюдение требований настоящей Инструкции возлагается на администратора информационной безопасности, администратора ИС «РСС Челябинск и пользователей, эксплуатирующих ИС «РСС Челябинск».

Продолжение приложения 3

Лист ознакомления

с инструкцией по антивирусной защите в информационных системах Полное наименование организации

№ п/п	ФИО	Должность	Дата ознакомления	Подпись
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				

18.				
19.				
20.				