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.

Создание системы защиты персональных данных на предприятии ООО «Мечелстрой»

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ – 10.03.01.2018.194.ПЗ ВКР

Руководитель проекта,
зам. директора ООО «Стратегия безопасности»
_____ Е.Ю. Мищенко
_____ 2018 г.

Автор проекта,
студент группы КЭ-471
_____ П.С.Чернышёва
_____ 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

Чернышёвой Полины Сергеевны

Группа *КЭ-471*

1 Тема работы

Создание системы защиты персональных данных

на предприятии ООО «Мечелстрой»

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)

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

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,
зам. директора ООО «Стратегия безопасности»_____ Е.Ю. Мищенко

Задание принял к исполнению _____ П.С. Чернышёва

КАЛЕНДАРНЫЙ ПЛАН

Наименование этапов выпускной квалификационной работы (проекта)	**Срок выполнения этапов работы**	**Отметки о выполнении руководителя**
Введение		
1 Наименование первой главы		
2 Наименование второй главы		
в соответствии с программой практики		
и др. пункты в соответствии со		
стандартом СТО ЮУрГУ 04-2008		
3 Наименование третьей главы		
Заключение		
Библиографический список		
Предзащита ВКР		
Защита ВКР		

Заведующий кафедрой _____ А.Н. Соколов

Руководитель работы _____ Е.Ю. Мищенко

Студент _____ П.С. Чернышёва

АННОТАЦИЯ

Чернышёва П.С. Создание системы защиты персональных данных на предприятии ООО «Мечелстрой» – Челябинск: ЮУрГУ, КЭ-471, 72с., 4 ил., 17 табл., библиогр. список 12 наим., 6 прил.

Выпускная квалификационная работа выполнена с целью создания системы защиты информации на предприятии ООО “Мечелстрой”. Работа состоит из трёх глав.

В первой главе проведен анализ текущего состояния защиты информации, в ходе которого был разработан паспорт предприятия, выявлены объекты защиты, рассмотрены актуальные угрозы, уязвимости, рассчитаны риски для ключевых объектов защиты.

Во второй главе проведен анализ и теоретическое обоснование выбранных средств защиты информации, включающее в себя анализ выявленных угроз, уязвимостей и средств по их устранению.

В третей главе разработаны рекомендации по созданию системы защиты персональных данных. В результате были определены объекты поставки, рассчитаны риски, построена матрица ответственности, разработана диаграмма Ганта, сетевой график и рассчитан бюджет и его эффективность.

ОГЛАВЛЕНИЕ

СОКРАЩЕНИЯ И ОПРЕДЕЛЕНИЯ

ЗИ – защита информации;
ИБ – информационная безопасность;
ТЗ – техническое задание;
АРМ - автоматизированное рабочее место;
АС – автоматизированная система;
НСД – несанкционированный доступ;
ОС – операционная система;
ООО – общество с ограниченной ответственностью;
СЗИ –система защиты информации;
ПЭВМ – персональная электронная вычислительная машина;
ПК – персональный компьютер;
ПО – программное обеспечение;
ИТ – информационные технологии;
РФ – Российская Федерация;
ФЗ – Федеральный закон;
ФСБ – Федеральная служба безопасности;
ФСТЭК - Федеральная служба по техническому и экспортному контролю;
ПО – программное обеспечение;
ОТСС – основные техническое средства вычислительной техники;
ВТСС – вспомогательные технические средства и системы;
ПДн – персональные данные;
ИСПДн – информационная система персональных данных;
ИС – информационная система.

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;

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

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

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 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 наше время информационные технологии развиваются стремительными темпами, увеличивается количество и важность обрабатываемых данных. Множество предприятий каждый день обрабатывает данные различных видов, которые несут огромную значимость для компании, но где есть что-то ценное всегда будут те, кто хочет это украсть. Именно поэтому уделяется огромное внимание защите персональных данных: издаются новые указы, постановления, стандарты, направленные на усиление ИБ.

Организация комплексной системы защиты информации и ее совершенствование позволяет избежать затрат, связанных с утечкой информации и ее распространением, обеспечить безопасность данных и их сохранность.

Объектом выпускной квалификационной работы является управляющая компания ООО «Мечелстрой».

Предметом дипломной работы является система защиты персональных данных.

Целью выпускной квалификационной работы является разработка системы защиты информации.

Для достижения поставленной цели необходимо:

1. Провести анализ информационной среды на предприятии ООО «Мечелстрой».
2. Провести анализ и теоретическое обоснование выбора средств защиты информации.
3. Организовать систему защиты информациина предприятии ООО «Мечелстрой».

В рамках моей работы внимание будет уделено персональным данным, так как именно они обрабатываются и хранятся на предприятии и имеют наибольшую ценность и необходимость в защите.

1. АНАЛИЗ СОСТОЯНИЯ ЗАЩИТЫ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ ООО «МЕЧЕЛСТРОЙ» И СУЩЕСТВУЮЩИЕ ПРОБЛЕМЫ

1.1. Разработка паспорта

Для определения необходимых мер по ЗИ необходимо получить общее представление о защищаемом объекте, поэтому был составлен паспорт предприятия(Приложение А).

В нем перечислены виды деятельности предприятия, реквизиты, организационная структура, состав ОТСС и ВТСС, их размещение.

В качестве объектов защиты были выбраныИСПДн«Клиенты» и ИСПДн«Городской центр начисления коммунальных платежей» на предприятии ООО «Мечелстрой».

Информация для составления паспорта предприятия была получена устным опросом начальника и сотрудников предприятия.

1.2. Разработка модели деятельности

В ходе анализа работыпредприятия ООО “Мечелстрой” была построена модель его деятельности (Приложение Г). Эта модельпозволяет ознакомиться с основными бизнес-процессамипредприятия, вспомогательными процессами, процессами управления, входной и выходной информацией.

Построение модели в случае необходимости поможет провести обучение персонала, создать матрицу ролей пользователей и модернизации основных и вспомогательных бизнес-процессов.

1.3. Выявление защищаемой информации в ООО «Мечелстрой»

В ходе анализа информации, обрабатываемой в ООО «Мечелстрой» и организационно-распорядительной документации организации, была выявлена информация, подлежащая защите:

-Сведения, составляющие персональные данные (на основании Федерального закона«О персональных данных»).

- Общедоступная информация, располагаемая в общедоступныхисточниках и сети интернет (на основании Федерального закона«Об информации, информационных технологиях и о защите информации»).

Информация, составляющая персональные данные, содержится в перечне сведений, составляющих персональные данные в ООО «Мечелстрой» (Приложение Г).

1.4. Описание информационной среды

Информационную среду предприятия ООО«Мечелтрой» составляет организационные, правовые и программно-аппаратные аспекты.

К организационным аспектам относятся документы:

- должностные инструкции персонала;
- инструкции по эксплуатации технических средств;
- инструкции по эксплуатации программного обеспечения;
- положения об особых режимах и системных взаимодействиях с персоналом.

К правовым аспектам относятся нормативно правовые документы, обеспечивающие регулирование деятельности организации и информационных процессов по защите информации. К таким документам относятся:

- Конституция РФ;
- Федеральный закон «О персональных данных»;
- Трудовой кодекс РФ;
- Гражданский кодекс РФ;
- Жилищный кодекс РФ;
- Федеральный закон «Об информации, информационных технологиях и о защите информации»;
- Указ президента«Об утверждении перечня сведений конфиденциального характера»;
- Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ Министерства строительства и жилищно-коммунального хозяйства№882 от 22.12.2014 «Об утверждении форм раскрытия информации организациями, осуществляющими деятельность в сфере управления многоквартирными домами»;
- Постановление Правительства РФ от 06.05.2011 г. N 354 «О предоставлении коммунальных услуг собственникам и пользователям помещений в многоквартирных домах и жилых домов»;
- Постановление Правительства РФ от 23.05.2006 г. № 306 «Об утверждении правил установления и определения нормативов потребления коммунальных услуг»;
- Постановление Правительства РФ от 13.08.2006 г. № 491 «Об утверждении Правил содержания общего имущества в многоквартирном доме и Правил изменения размера платы за содержание и ремонт жилого помещения в случае оказания услуг и выполнения работ по управлению, содержанию и ремонту общего имущества в многоквартирном доме ненадлежащего качества и (или) с перерывами, превышающими установленную продолжительность»;
- Постановление Госстроя РФ от 27.09.2003г. № 170 «Об утверждении правил и норм технической эксплуатации жилищного фонда»;
- Постановление Правительства РФ от 3 апреля 2013 г. N 290 «О минималь-

ном перечне услуг и работ, необходимых для обеспечения надлежащего содержания общего имущества в многоквартирном доме, и порядке их оказания и выполнения»;

- Постановление Правительства РФ от 15.05.2013 г. N 416 «О порядке осуществления деятельности по управлению многоквартирными домами»;

- Постановление Правительства РФ от 21.01.2006 г. № 25 «Об утверждении правил пользования жилыми помещениями».

К программно-аппаратным аспектам относятся программно-аппаратные средства, которые обеспечивают работу предприятия. Аппаратные средства представлены в Таблице 1, Программные в Таблице 2.

Таблица 1 – Аппаратные средства

№	Наименование устройства	Фирма производитель	Кол-во	Год выпуска
1	2	3	4	5
АРМ				
1.1	Системный блок	Acer Extensa EM2710	3	2014
1.2	Монитор	BenQ GW2760HS	3	2014
1.3	Клавиатура	Logitech Keyboard K120 Black USB	3	2014
1.4	Мышь	Logitech Mouse M90 Black USB	3	2012
1.5	Источник бесперебойного питания	APC APCBack-UPS BE400-RS	3	2012
1.6	МФУ	Kyocera ECOSYSM2040dn	2	2012
1.7	Телефон	Gigaset C530A IP	2	2013

Таблица 2 – Программные средства

№	Наименование	Описание	Версия
1	2	3	4
АРМ			
1.1	Windows 7	Операционная система	
1.2	Пакет Microsoft Office 2015	Офисный пакет для работы с договорами, приказами, отчетами и т.д.	
1.3	ESET NOD32 Antivirus	Антивирусное ПО	11.0
1.4	Adobe Reader DC	Программа для чтения, печати и рецензирования файлов PDF	
1.5	WinRAR	Программа для сжатия файлов	
1.6	Google Chrome	Интернет браузер	

1.5. Выявление объектов защиты

В результате анализа средств, методов обработки информации и перечня защищаемой информации можно выделить следующий перечень объектов защиты информации:

- АРМ сотрудников;
- информационная инфраструктура:
  - ОС на АРМ;
  -ПО на АРМ;
  - программные средства и модули, осуществляющие функции по защите информации от несанкционированного доступа на ПК;
  - протоколы сетевого и межсетевого взаимодействия;
- системы бесперебойного питания АРМ;
- персонал;
- средства ввода-вывода и отображения информации:
  - мониторы;
  - периферийные устройства;
- линии и средства связи, системы обеспечения функционирования СВТ и деятельности организации:
  - линии электропитания;
  - телефонные линии связи;
  - линии охранной и пожарной сигнализации;
  - линии локальной компьютерной сети;
- носители информации:
  - бумажные носители;
  -флеш-накопители.

1.6. Разработка модели угроз и уязвимостей для объектов защиты

На основе «Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утверждена ФСТЭК 14 февраля 2008) и «Специальных требований и рекомендаций по технической защите конфиденциальной информации» (Утверждены приказом Гостехкомиссии России от 02.03.2001 № 282), на основании документа «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка)» ФСТЭК была составлена модель угроз и уязвимостей, представленная в таблицах 7 и 8. Но сперва, для выявления наиболее значимых угроз ИБ организации нужно определить уровень исходной защищенности, представленный в таблицах 3 и 4 и выделить объекты защиты информации относительно персональных данных, ими являются:

- персонал;
- АРМ сотрудников, на которых обрабатываются персональные данные.

Также было выявлено наличие двух ИСПДн:

- ИСПДн «Клиенты», отвечающее за сбор, хранение и изменения паспортных данных жильцов домов, обслуживаемых организацией;
- ИСПДн «Городской центр начисления коммунальных платежей», отвечающее за принятие показаний приборов учета расхода воды и начисляющее платежи за общедомовые коммунальные услуги.

Таблица 3 - Уровень исходной защищенностиИСПДн «Клиенты»

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
1	2	3	4
1. По территориальному размещению:			
Локальная ИСПДн, развернутая в пределах одного здания;	+		
2. По наличию соединения с сетями общего пользования:			
ИСПДн, физически отделенная от сети общего пользования;	+		
3. По встроенным (легальным) операциям с записями баз персональных данных:			
модификация, передача;			+
4. По разграничению доступа к персональным данным:			
ИСПДн, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИСПДн, либо субъект ПДн;		+	
5. По наличию соединений с другими базами ПДн иных ИСПДн:			
ИСПДн, в которой используется одна база ПДн, принадлежащая организации-владельцу данной ИСПДн;	+		
6. По уровню (обезличивания) ПДн:			
ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;		+	
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки:			
ИСПДн, не предоставляющие никакой информации.	+		

ИСПДн«Клиенты» имеет средний уровень исходной защищенности, так как более 70% характеристик соответствуют уровню не ниже "средний", но менее 70% характеристик соответствуют уровню высокий (Y_1= 5).

Таблица 4 – Уровень исходной защищенности ИСПДн «Городской центр начисления коммунальных платежей»

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
1	2	3	4
1. По территориальному размещению:			
локальнаяИСПДн, развернутая в пределах одного здания;	+		
2. По наличию соединения с сетями общего пользования:			
ИСПДн, имеющая одноточечный выход в сеть общего пользования;		+	
3. По встроенным (легальным) операциям с записями баз персональных данных:			
модификация, передача;			+
4. По разграничению доступа к персональным данным:			
ИСПДн, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИСПДн, либо субъект ПДн;		+	
5. По наличию соединений с другими базами ПДн иных ИСПДн:			
интегрированная ИСПДн (организация использует несколько баз ПДнИСПДн, при этом организация не является владельцем всех используемых баз ПДн);			+
6. По уровню (обезличивания) ПДн:			
ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;		+	
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки:			
ИСПДн, не предоставляющие никакой информации.	+		

ИСПДн«Городской центр начисления коммунальных платежей» имеет средний уровень исходной защищенности, так как более 70% характеристик соответствуют уровню не ниже "средний", но менее 70% характеристик соответствуют уровню высокий (Y_1= 5).

На основе выделенных объектов защиты информации выявим наиболее значимые угрозы.

Оценка вероятности и опасности угроз, а также их актуальности для ИСПДнприведены в таблицах 5 и 6.

Таблица 4 –Угрозы дляИСПДн«Клиенты»

Тип угроз безопасности ПДн	Коэффициент реализуемости угрозы (Y)	Возможность реализации	Опасность	Актуальность
1	2	3	4	5
1. Угрозы от утечки по техническим каналам.				
1.1. Угрозы утечки акустической информации	0,25	низкая	средняя	неактуальная
1.2. Угрозы утечки видовой информации	0,25	низкая	низкая	неактуальная
1.3. Угрозы утечки информации по каналам ПЭМИН	0,25	низкая	низкая	неактуальная
2. Угрозы несанкционированного доступа к информации.				
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн				
2.1.1. Кража ПЭВМ	0,25	низкая	средняя	неактуальная
2.1.2. Кража носителей информации	0,25	низкая	средняя	неактуальна
2.1.3. Кража ключей и атрибутов доступа	0,25	низкая	средняя	неактуальная
2.1.4. Кражи, модификации, уничтожения информации	0,25	низкая	высокая	актуальная
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	0,25	низкая	низкая	неактуальная
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	0,25	низкая	высокая	актуальная
2.1.7. Несанкционированное отключение средств защиты	0,25	низкая	высокая	актуальная
2.2. 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).				

Продолжение Таблицы 4

1	2	3	4	5
2.2.1. Действия вредоносных программ (вирусов)	0,25	низкая	высокая	актуальная
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	0,25	низкая	низкая	неактуальная
2.2.3. Установка ПО не связанного с исполнением служебных обязанностей	0,25	низкая	низкая	неактуальная
2.3. 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.				
2.3.1. Утрата ключей и атрибутов доступа	0,25	низкая	средняя	неактуальная
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	0,25	низкая	высокая	актуальная
2.3.3. Непреднамеренное отключение средств защиты	0,25	низкая	средняя	неактуальная
2.3.4. Выход из строя аппаратно-программных средств	0,25	низкая	низкая	неактуальная
2.3.5. Сбой системы электроснабжения	0,25	низкая	низкая	неактуальная
2.3.6. Стихийное бедствие	0,25	низкая	низкая	неактуальная
2.4. Угрозы преднамеренных действий внутренних нарушителей				
2.4.1. Доступ к информации, модификация, уничтожение лицами не допущенными к ее обработке	0,25	низкая	высокая	актуальная

Продолжение Таблицы 4

1	2	3	4	5
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	0,25	низкая	высокая	актуальная
2.5.Угрозы несанкционированного доступа по каналам связи.				
2.5.1.1. Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации	0,25	низкая	средняя	неактуальная
2.5.1.2. Перехват за переделами с контролируемой зоны	0,25	низкая	средняя	неактуальная
2.5.1.3. Перехват в пределах контролируемой зоны внешними нарушителями	0,25	низкая	средняя	неактуальная
2.5.1.4.Перехват в пределах контролируемой зоны внутренними нарушителями.	0,25	низкая	средняя	неактуальная
2.5.2.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.	0,25	низкая	средняя	неактуальная
2.5.3.Угрозы выявления паролей по сети	0,25	низкая	низкая	неактуальная
2.5.4.Угрозы навязывание ложного маршрута сети	0,25	низкая	низкая	неактуальная

Продолжение Таблицы 4

1	2	3	4	5
2.5.5.Угрозы подмены доверенного объекта в сети	0,25	низкая	низкая	неактуальная
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	0,25	низкая	низкая	неактуальная
2.5.7.Угрозы типа «Отказ в обслуживании»	0,25	низкая	низкая	неактуальная
2.5.8.Угрозы удаленного запуска приложений	0,25	низкая	низкая	неактуальная
2.5.9.Угрозы внедрения по сети вредоносных программ	0,25	низкая	низкая	неактуальная

Таблица 5 – Угрозы для ИСПДн «Городской центр начисления коммунальных платежей»

Тип угроз безопасности ПДн	Коэффициент реализуемости угрозы (Y)	Возможность реализации	Опасность	Актуальность
1	2	3	4	5
1. Угрозы от утечки по техническим каналам.				
1.1. Угрозы утечки акустической информации	0,25	низкая	средняя	неактуальная
1.2. Угрозы утечки видовой информации	0,25	низкая	низкая	неактуальная
1.3. Угрозы утечки информации по каналам ПЭМИН	0,25	низкая	низкая	неактуальная
2. Угрозы несанкционированного доступа к информации.				
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн				
2.1.1. Кража ПЭВМ	0,25	низкая	средняя	неактуальная
2.1.2. Кража носителей информации	0,25	низкая	средняя	неактуальная

Продолжение Таблицы 5

1	2	3	4	5
2.1.3. Кража ключей и атрибутов доступа	0,25	низкая	средняя	неактуальная
2.1.4. Кражи, модификации, уничтожения	0,25	низкая	высокая	актуальная
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	0,25	низкая	низкая	неактуальная
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	0,25	низкая	высокая	актуальная
2.1.7. Несанкционированное отключение средств защиты	0,25	низкая	высокая	актуальная
2.2. 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).				
2.2.1. Действия вредоносных программ (вирусов)	0,25	низкая	высокая	актуальная
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	0,25	низкая	низкая	неактуальная
2.2.3. Установка ПО не связанного с исполнением служебных обязанностей	0,25	низкая	низкая	неактуальная
2.3. 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.				
2.3.1. Утрата ключей и атрибутов доступа	0,35	низкая	высокая	актуальная

Продолжение Таблицы 5

1	2	3	4	5
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	0,25	низкая	высокая	актуальная
2.3.3. Непреднамеренное отключение средств защиты	0,25	низкая	средняя	неактуальная
2.3.4. Выход из строя аппаратно-программных средств	0,25	низкая	низкая	неактуальная
2.3.5. Сбой системы электроснабжения	0,25	низкая	низкая	неактуальная
2.3.6. Стихийное бедствие	0,25	низкая	низкая	неактуальная
2.4. Угрозы преднамеренных действий внутренних нарушителей				
2.4.1. Доступ к информации, модификация, уничтожение лицами не допущенными к ее обработке	0,25	низкая	высокая	актуальная
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	0,25	низкая	высокая	актуальная
2.5.Угрозы несанкционированного доступа по каналам связи.				
2.5.1.1. Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации	0,35	средняя	средняя	актуальная
2.5.1.2. Перехват за переделами КЗ	0,35	средняя	средняя	актуальная
2.5.1.3. Перехват в пределах КЗвнешними нарушителями	0,25	низкая	средняя	актуальная

Продолжение Таблицы 5

1	2	3	4	5
2.5.1.4.Перехват в пределах КЗ внутренними нарушителями.	0,25	низкая	средняя	актуальная
2.5.2.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.	0,35	средняя	средняя	актуальная
2.5.3.Угрозы выявления паролей по сети	0,35	средняя	средняя	актуальная
2.5.4.Угрозы навязывание ложного маршрута сети	0,35	средняя	средняя	актуальная
2.5.5.Угрозы подмены доверенного объекта в сети	0,35	средняя	средняя	актуальная
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	0,35	средняя	средняя	актуальная
2.5.7.Угрозы типа «Отказ в обслуживании»	0,35	средняя	средняя	актуальная
2.5.8.Угрозы удаленного запуска приложений	0,35	средняя	средняя	актуальная
2.5.9.Угрозы внедрения по сети вредоносных программ	0,35	средняя	средняя	актуальная

Анализируя актуальность угроз, составим таблицу актуальных угроз и уязвимостей для каждой ИСПДн.

Актуальные угрозы безопасности ПДн в ИСПДн «Клиенты», представлены в таблице 6.

Актуальные угрозы безопасности ПДн в ИСПДн «Городской центр начисления коммунальных платежей», представлены в таблице 7.

Таблица 6 – Актуальные угрозы и уязвимости для ИСПДн «Клиенты»

Объект	Угроза	Уязвимость
1	2	3
Персонал	Непреднамеренная модификация (уничтожение) информации сотрудниками	Не соблюдение соглашения о неразглашении информации, составляющей ПДн
	Утрата ключей и атрибутов доступа	Нарушение пропускного режима
	Разглашение информации, составляющей ПДн	Преднамеренные действия пользователей системы
	Доступ к информации, модификация, уничтожение лицами не допущенными к ее обработке	Преднамеренные действия внешних нарушителей
	Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	
АРМ сотрудников, на которых обрабатываются ПДн	Кражи, модификации, уничтожения информации	Нарушение пропускного режима
	Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	Наличие ПО, которое может создать условия для НСД
	Несанкционированное отключение средств защиты	Наличие вредоносного ПО в системе
	Действия вредоносных программ (вирусов)	

Таблица 7– Актуальные угрозы и уязвимости для ИСПДн «Городской центр начисления коммунальных платежей»

Объект	Угроза	Уязвимость
1	2	3
Персонал	Непреднамеренная модификация (уничтожение) информации сотрудниками	Не соблюдение соглашения о неразглашении информации, составляющей ПДн

Продолжение Таблицы 7

1	2	3
	Утрата ключей и атрибутов доступа	Нарушение пропускного режима
	Разглашение информации, составляющей ПДн	Преднамеренные действия пользователей системы
	Доступ к информации, модификация, уничтожение лицами не допущенными к ее обработке	Преднамеренные действия внешних нарушителей
	Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	
АРМ сотрудников, на которых обрабатываются ПДн	Кражи, модификации, уничтожения информации	Наличие ПО, которое может создать условия для НСД
	Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	Нарушение пропускного режима
	Несанкционированное отключение средств защиты	Наличие вредоносного ПО в системе
	Действия вредоносных программ (вирусов)	Отсутствие сертифицированных средств межсетевого экранирования
	Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации	
	Перехват за переделами с контролируемой зоны	

Продолжение Таблицы 7

1	2	3
	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 навязывание ложного маршрута сети	
	Угрозы подмены доверенного объекта в сети	
	Угрозы типа «Отказ в обслуживании»	
	Угрозы удаленного запуска приложений	
	Угрозы внедрения по сети вредоносных программ	

Рекомендуемыми мерами по предотвращению реализации актуальных угроз, являются:

- установка антивирусной защиты;
- межсетевого экрана;
- парольная политика, устанавливающая обязательную сложность и периодичность смены пароля;
- назначить ответственного за безопасность персональных данных из числа сотрудников учреждения;
- инструкции пользователей ИСПДн, в которых отражены порядок безопасной работы с ИСПДн и в сетях общего пользования и (или) международного обмена, а так же с ключами и атрибутами доступа;
- убрать подключение элементов ИСПДн к сетям общего пользования и (или) международного обмена (сеть Интернет), если это не требуется для функционирования ИСПДн.

1.7. Расчет рисков объектов защиты

Расчет рисков необходим для выявления наиболее вероятных угроз для объекта информации и уязвимостей, через который они могут быть реализованы.

Алгоритм расчета рисков выглядит следующим образом:
1. На первом этапе рассчитывается уровень угрозы по уязвимости Th на основе критичности и вероятности реализации угрозы через данную уязвимость по формуле (1). Уровень угрозы показывает, насколько критичным является воздействие данной угрозы на ресурс с учетом вероятности ее реализации.

$$\mathrm{Th} = \frac{\mathrm{ER}}{100} \cdot \frac{\mathrm{P(V)}}{100}, \qquad (1)$$

где ER - критичность реализации угрозы (указывается в %);
P(V) - вероятность реализации угрозы через данную уязвимость (указывается в %). Полученное значение уровня угрозы по уязвимости лежит в интервале от 0 до

2. Для расчета уровня угрозы по всем уязвимостям CTh, через которые возможна реализация данной угрозы на ресурсе используется формула (2).

$$\mathrm{CTh} = 1 - \prod_{i=1}^{n} (1 - Th_i), \qquad (2)$$

где Th- уровень угрозы по уязвимости.
Значение уровня угрозы по всем уязвимостям лежит в интервале от 0 до 1.

3. Аналогично рассчитывается общий уровень угроз по ресурсу CThR (учитывая все угрозы, действующие на ресурс) по формуле (3).

$$\mathrm{CThR} = 1 - \prod_{i=1}^{n} (1 - CTh_i), \qquad (3)$$

где CTh - уровень угрозы по всем уязвимостям.
Значение общего уровня угрозы лежит в интервале от 0 до 1.

4. Риск по ресурсу R рассчитывается в соответствии с формулой (4):
$R = \mathrm{CThR} \times D, \qquad (4)$
где D - критичность ресурса (задается в деньгах);
CThR- общий уровень угроз по ресурсу.

Оценка рисков приведена в таблице 8.
Таблица 8 – Оценка рисков для ИСПДн «Клиенты»

Риски / пути их реализации	ER	P(V)	Th	CTh	CThR	R
1	2	3	4	5	6	7
Риски уничтожения, хищения аппаратных средств и носителей информации				0,791	0,919	919000
Непреднамеренная модификация (уничтожение) информации сотрудниками	70	40	0,28			
Утрата ключей и атрибутов доступа	50	30	0,15			
Разглашение информации, составляющей ПДн	60	30	0,18			

Продолжение Таблицы 8

1	2	3	4	5	6	7
Доступ к информации, модификация, уничтожение лицами не допущенными к ее обработке	80	30	0,24			
Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	80	30	0,24			
Кражи, модификации, уничтожения информации	70	40	0,28			
Риски хищения, модификации или блокирования информации				0,615		
Кражи, модификации, уничтожения информации	80	30	0,24			
Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	50	30	0,10			
Несанкционированное отключение средств защиты	50	50	0,25			
Действия вредоносных программ (вирусов)	50	50	0,25			

Таблица 9 – Оценка рисков для ИСПДн «Городской центр начисления коммунальных платежей»

Риски / пути их реализации	ER	P(V)	Th	CTh	CThR	R
1	2	3	4	5	6	7
Риски уничтожения, хищения аппаратных средств и носителей информации				0,771	0,974	974000
Непреднамеренная модификация (уничтожение) информации сотрудниками	70	30	0,21			
Утрата ключей и атрибутов доступа	50	30	0,15			
Разглашение информации, составляющей ПДн	60	30	0,18			
Доступ к информации, модификация, уничтожение лицами не допущенными к ее обработке	80	30	0,24			
Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	80	30	0.24			
Кражи, модификации, уничтожения информации	70	40	0,28			

Продолжение Таблицы 9

1	2	3	4	5	6	7
Риски хищения, модификации или блокирования информации				0,887		
Кражи, модификации, уничтожения информации	80	30	0,24			
Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	50	30	0,10			
Несанкционированное отключение средств защиты	50	50	0,25			
Действия вредоносных программ (вирусов)	50	50	0,25			
Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации	50	80	0,40			
Перехват за переделами КЗ	50	50	0,25			
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	50	70	0,35			
Угрозы выявления паролей по сети	80	70	0,56			
Угрозы навязывание ложного маршрута сети	80	70	0,56			
Угрозы подмены доверенного объекта в сети	80	70	0,56			
Угрозы типа «Отказ в обслуживании»	80	70	0,56			
Угрозы удаленного запуска приложений	80	20	0,16			
Угрозы внедрения по сети вредоносных программ	80	20	0,16			

1.8. Разработка технического задания на создание системы защиты ПДн

В результате проведенной работы стало необходимо разработать техническое задание по созданию системы защиты ПДн в ООО «Мечелстрой» (Приложение Д).

Основой для написания ТЗ является ГОСТ 34.602-1989 «Техническое задание на создание автоматизированной системы», содержащий следующие разделы:

1) общие сведения;
2) назначение и цели разработки системы;
3) характеристика объектов защиты;
4) требования к ИСПДн;
5) состав и содержание работ по внедрению системы;
6) порядок контроля и приемки системы;
7) требования к составу и содержанию работ по подготовке объекта защиты к вводу ИСПДн в действие;
8) требования к документированию;
9) источники разработки.

1.9. Вывод по первой главе

В первой главе была проанализированаинформационная среда в ООО «Мечелстрой», был разработан паспорт предприятия, выявлены объекты защиты, рассмотрены актуальные угрозы, уязвимости, рассчитаны риски для ключевых объектов защиты. На основе полученных данных, результаты были проанализированы.

Был составлен паспорт предприятия, в котором были рассмотрены такие пункты, как виды осуществляемой деятельности и защищаемой информации, структура организации, программно-аппаратные средства. Была выделена группа сведений, подлежащих защите, а именно сведения, составляющие персональные данные.

Также были разработаны:

- модель деятельности, отражающая процесс обработки информации ограниченного доступа;
- модель угроз безопасности персональных данных и произведена оценка их актуальности;
- техническое задание на создание системы защиты персональных данных на предприятии ООО «Мечелстрой».

В результате проведенной работы следует, что предприятие защищено не должным образом и значение рисков велико. Необходимо принятие организационных мер и внедрение дополнительных средств защиты от несанкционированного доступа. По окончанию анализа нами было разработано техническое задание по созданию системы защиты персональных данных в ООО «Мечелстрой» (Приложение Д).

2. ТЕОРЕТИЧЕСКОЕ ОБОСНОВАНИЕ ВЫБОРАНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

2.1. Обзор возможных методов устранения уязвимостей

Определение методов и средств, необходимых для устранения угроз и уязвимостей, выявленных ранее, актуальных для комплексной системы защиты информации в рамках рассматриваемого объекта, а также их анализ – это один из важнейших этапов нашей работы по созданию системы защиты ПДн.

На этом этапе необходимо выявить наиболее эффективные по решению задачи защиты объекта.

2.2. Угрозы, связанные с НСД

В условиях стремительного развития ИТ и конкурентной среды существует некая тенденция к повышению заинтересованности предприятий к информации, составляющую персональные данные, будь то владелец или конкурент, желающий получить информацию с целью каких-либо выгод.

Так как большинство современных коммерческих предприятий занимается обработкой информации ограниченного доступа рамках внутренней ИС, то существуют то, кто пытается завладеть этой информацией различными способами и методами. Одним из таких методов для получения информации лицами, не являющимися владельцами, является несанкционированный доступ.

Несанкционированный доступ - это противоправное преднамеренное владение конфиденциальной информацией лицами, не имеющими права доступа к защищаемой информации. В соответствии с ГОСТ Р 50922-96 "Защита информации. Основные термины и определения", под защитой информации от несанкционированного воздействия понимается - деятельность по предотвращению воздействия на защищаемую информацию с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Необходимо определить актуальные угрозы для рассматриваемого объекта, которые связаны с несанкционированным доступом. На основе выявленных угроз произвести выбор наиболее эффективных средств и методов защиты информации в рамках нашего объекта.

Угрозы, связанные с НСД:

- несанкционированный доступ к АРМ сотрудников;

В таблицах 7 и 8 также были определены уязвимости для рассматриваемых угроз в рамках нашей работы.

2.2.1.Несанкционированный доступ к АРМ сотрудников

Для реализации угрозы несанкционированного доступа к АРМ сотрудников нарушителя могут быть использованы следующие уязвимости:

- отсутствие пломбирования корпуса АРМ;
- наличие ПО, которое может создать условия для НСД;
- наличие вредоносного ПО в системе;
- нарушение пропускного режима.

Для минимизации возможности возникновения первой угрозы необходимо провести опломбировку корпуса ПК сотрудников, назначить лицо, которое будет вести контроль и учет состояния пломбировки персональных компьютеров и серверов.

Уязвимостью авторизации на аппаратном уровне можно пренебречь, принять риск, так как организация не готова тратить деньги на установку средств контроля аппаратной авторизации АРМ сотрудников. Компании считает эту уязвимость маловероятной и более выгодным ликвидировать последствия реализации данной угрозы через эту уязвимость.

В рамках ВКР был проведен сравнительный анализ программных средств защиты от НСДи МЭ, результаты которого приведены в Таблице 10.

Таблица 10 – Сравнение СЗИ от НСД и МЭ

Критерии сравнения	Secret Net Studio	Dallas Lock 8.0-K	ViPNet Client 4
Класс защищенности	По 5 классу защищенности	По 5 классу защищенности	По 3 классу защищенности
Уровень контроля НДВ	По 4 уровню контроля	По 4 уровню контроля	По 3 уровню контроля
Класс автоматизированных систем	До класса 1Г включительно	До класса 1Г включительно	До класса 1В включительно
Дополнительные аппаратные требования: свободное место на жестком диске	2 Гб	0,03 Гб	0,1 Гб
Цена	8175	7 500	7 800
Цена + МЭ	9375	8900	10 800

Для исключения уязвимости отсутствие установленных средств защиты от НСД необходимо установить комплекс средств защиты информации от НСД «Secret Net», в функциональные возможности которого входит обеспечение контроля неизменной конфигурации ПК во время работы, усиленная аутентификация пользователя с помощью пароля и персонального идентификатора, создание доверенной среды, контроль утечек и каналов распространения защищаемой информации, межсетевое экранирование и другие немаловажные функции.

Так как на компьютерах организации уже было установлено средство защиты

от вирусов, которое постоянно обновляется, и руководитель не намерен менять ПО, то было решено оставить текущее средство антивирусной защиты ESETNOD32. Данное ПО, по их мнению, в должной мере осуществляет защиту от всевозможных вирусных угроз и претензий на данный момент к нему не было и этих мер будет достаточно для исключения данной угрозы. Однако, для минимизации угрозы через данную угрозы необходимо своевременно обновлять модули защиты и антивирусные базы.

Для исключения последней уязвимости необходимо ужесточить пропускной режим в контролируемое помещение, чтобы свести на нет возможность проникновения злоумышленника или иного лица, не обладающего такими правами доступа.

2.3. Разглашение информации, составляющей персональные данные

Одним из нескольких путей разглашение информации, составляющей персональные данные, является утечка информации по акустическому каналу, который реализован в подслушивании разговоров в помещениях или открытой местности, с использованием выносных микрофонов или иных средств для записи разговора.

К проявлению данной угрозы приводят ряд следующих уязвимостей:

- отсутствие или неактуальность документов, регламентов по защите персональных данных;
- несоблюдение соглашения о неразглашении информации подлежащей защите;
- нарушение пропускного режима.

Первые две уязвимости можно устранить благодаря разработки новой организационно-распорядительной документации в области защиты персональных данных предприятия, который будет включать в себя положение о персональных данных, должностные инструкции, политика допустимого использования и физической безопасности и т.д. Также необходимостью является проведение специальных тренингов и профилактических бесед с сотрудниками, подробное разъяснение и доведение до их сведения мер ответственности за разглашение защищаемой информации и подписания. Необходимо чтобы каждый сотрудник в договоре расписался, что ознакомился с положениями и понимает всю ответственность за разглашение сведений, составляющих персональные данные.

2.4. Угрозы преднамеренных действий внутренних нарушителей

Данные угрозы являются наиболее распространенными и, соответственно, наиболее важными с точки зрения защиты информации, так как больший приоритет имеет защита информации ограниченного доступа от преднамеренных действий внутренних нарушителей, а именно сотрудников, допущенных к ее обработке.

Для ООО «Мечелстрой» актуален данный вид угроз и рекомендуются следу-

ющие меры для их минимизации:

- Установка СЗИ от НСД «Secret Net Studio»;
- Обеспечение резервного копирования информации ограниченного доступа, обрабатываемой на АРМ.

2.5. Вывод по второй главе

На основе результатов работ по выявлению уязвимостей на рассматриваемом предприятии, приводящих к реализации возможных угроз, были применены следующие меры по их минимизации:

1. Для защиты от угроз несанкционированного доступа к информации:

– Установлены СЗИ от НСД «Secret Net Studio» по причине наилучшего соотношения цена/функциональность из сравниваемых СЗИ от НСД в таблице 10;

2. Для защиты от угроз преднамеренных действий внутренних нарушителей:

- Обеспечено резервное копирование информации, обрабатываемой на АРМ;
- Установлены СЗИ от НСД «Secret Net Studio»;
- Опломбированы корпуса ПК сотрудников.

3. Для защиты от угроз несанкционированного доступа по каналам связи:

– Установлен программный межсетевой экран «Secret Net Studio» По сравнению с другими, выбранный межсетевой экран обладает выгодной ценой и наличием модулей расширения, при желании, позволяющих заменить его основные интерфейсы.

3. СОЗДАНИЕ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ НА ПРЕДПРИЯТИИ ООО «МЕЧЕЛСТРОЙ»

3.1. Описание объекта

Компания ООО «Мечелстрой» занимается обслуживанием и ремонтом многоквартирных домов в Металлургическом районе города Челябинска по улицам: Жукова, Электростальская, Дегтярева, Шоссе Металлургов, Доменная.
Дома были переданы в управление строительными компаниями ООО МПК "Архимед" и ЗАО "Мечелстрой". В жилом фонде находятся панельные и каркасно-монолитные дома.
Таблица 11 – Потоки защищаемой информацииАС «Клиенты»

Входящая информация	Исходящая информация
Информация о клиентах	База данных клиентов
	Паспортный стол Металлургического района
	Почтовое отделение

Таблица 12 – Потоки защищаемой информации АС «Городской центр начисления коммунальных платежей»

Входящая информация	Исходящая информация
Информация о клиентах	База данных клиентов
	Сбербанк

3.2. Резюме проекта

Разработка проекта велась согласно утвержденному техническому заданию на создание системы защиты персональных данных на предприятии ООО «Мечелстрой» (Приложение Д).
Создание системы защиты должно осуществляться с помощью организационных, инженерно-технических и программно-аппаратных мер. На каждый конкретный этап работ должны быть назначены ответственные лица с помощью матрицы ответственности.
Результатом работ должна стать система защиты персональных данных ООО «Мечелстрой», соответствующая нормативно-правовым актам в области защиты персональных данных.

3.3. Цели и задачи проекта

Целями создания системы защиты персональных данных ООО «Мечелстрой» являются:

- Предотвращение угроз, связанных с НСД;
- Предотвращение угроз преднамеренных действий внутренних нарушителей;
- Предотвращение угроз несанкционированного доступа по каналам связи;

- 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 «Мечелстрой»:

- Технический паспорт на автоматизированную систему обработки персональных данных (Приложение А);
- Техническое задание на создание системы защиты персональных данных (Приложение Д);
- Модель деятельности (Приложение Е);
- Политика в области обработки персональных данных (Приложение Г).

3.4.2. Программно-аппаратные и инженерно-технические меры

В рамках реализации проекта по созданию системы защиты персональных данных должны быть закуплены и установлены следующие программно-аппаратные средства:

- СЗИотНСДс функцией межсетевого экранирования «SecretNetStudio»

3.4.3. Обучение персонала

В рамках реализации проекта по созданию системы защиты персональных данных должно быть проведено обучение сотрудников порядку работы с персональными данными, обучение основам работы с СЗИ от НСД и межсетевым экраном.

3.5. Описание информационных потоков

Описание информационных потоков предприятия должно отражать структуру бизнес-процессов, их взаимодействие с внешней средой и представляться в схематическом виде. Данная модель должна быть в конечном итоге понятна как самим разработчикам, так и сотрудникам. Построенная модель будет являться чрезвычайно полезной для проведения процедуры внутреннего аудита, а именно: для выявления требований законодательства относительно защищаемой информации; построить представление о структуре бизнес-процессов; разработать такие рекомендации по улучшению защищенности информации ограниченного доступа, которые не смогли бы в дальнейшем влиять на непрерывность бизнес-процессов.

Описание информационных потоков составляют формализованныеграфичные документы «Схемы информационных потоков», текстовые и табличные документы «Справочник информационных объектов и хранилищ данных», «Каталог

данных», содержащие сведения об информационных потоках, объектах и субъектах, задачах, местах хранения данных.
В рамках ВКР, описание информационных потоков АО «Мечелстрой» отражается в Приложении Е.

3.6. 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	2	3	4	5
1. Риски изменений в стране, обществе				
1.1. Ухудшение политических и экономических характеристик и факторов				0,0015
реформы в экономике и политике	10	5	0,005	
изменение законодательства	20	10	0,01	
1.2. Изменение характеристик общества				0,1162
здравоохранение и медицина	25	5	0,0125	
возникновение негативного отношения сотрудников	70	15	0,105	
1.3. Влияние форс-мажорных обстоятельств				0,25
стихийные бедствия и природные катаклизмы	25	10	0,025	
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				0,0733
срыв графиков работ, невыполне-	15	20	0,03	

ние сроков				
нехватка рабочей силы	20	5	0,01	
недооценка стоимости работ и использование финансов для других целей	35	10	0,035	
2.3. Риски персонала				
влияние личностных факторов (неумеренные амбиции участников проекта, переоценка собственных возможностей, преувеличение роли технологической стороны в ущерб менеджменту)	20	5	0,01	0,035
риск недоступности персонала, которому сложно подобрать замену (болезнь, увольнение и другие непредвиденные обстоятельства)	25	10	0,025	

Минимальную угрозу проекту составляют риски стихийных бедствий и природных катаклизмов, а максимальную – риски изменения или недостатка бюджета проекта. Максимальные риски принимаются, так как устранить их невозможно.

3.7. Структура разбиения работ

Структура разбиения работ позволяет определить, какие работы необходимо выполнить для реализации проекта, и установить единую структуру управления этими работами. Структура разбиения работ представлена на Рисунке 1.
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. Техническое задание;
ИСПДн 2.3. Акт установления уровня защищенности.
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 (и МЭ для АРМ 2);
ИСПДн 4. Внедрение;
ИСПДн 4.1. Установка и настройка СЗИ от НСД (и МЭ для АРМ 2);

ИСПДн 4.2. Обучение пользователей;
ИСПДн 4.3. Контроль защищенности.

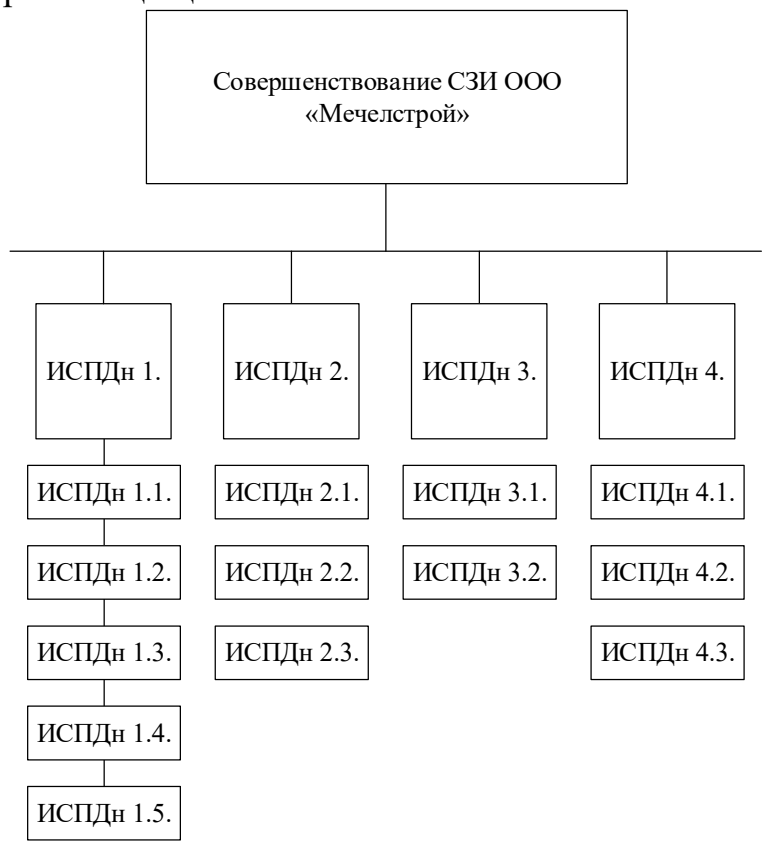

Рисунок 1 – Структура разбиения работ

3.8. Структурная схема организации проекта

Структурная схема организации проекта создания системы защиты персональных данных приведена на Рисунке 2.

Рисунок 2 – Структурная схема организации проекта

3.9. Матрица ответственности

Для наглядности обязанностей исполнителей проекта составляется матрица ответственности. Работа исполнителей разделяется на следующие группы: управление (У), исполнение (И), контроль (К).

Таблица 13 – Матрица ответственности

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

3.10. Диаграмма Ганта и сетевой график

Диаграмма Ганта – инструмент для наглядной иллюстрации календарного плана разных этапов работ в проектном менеджменте. Для проекта создания системы защиты персональных данных ООО «Мечелстрой». Диаграмма Ганта представлена на рисунке3. На основании диаграммы Гантапроект займет 28 дней.

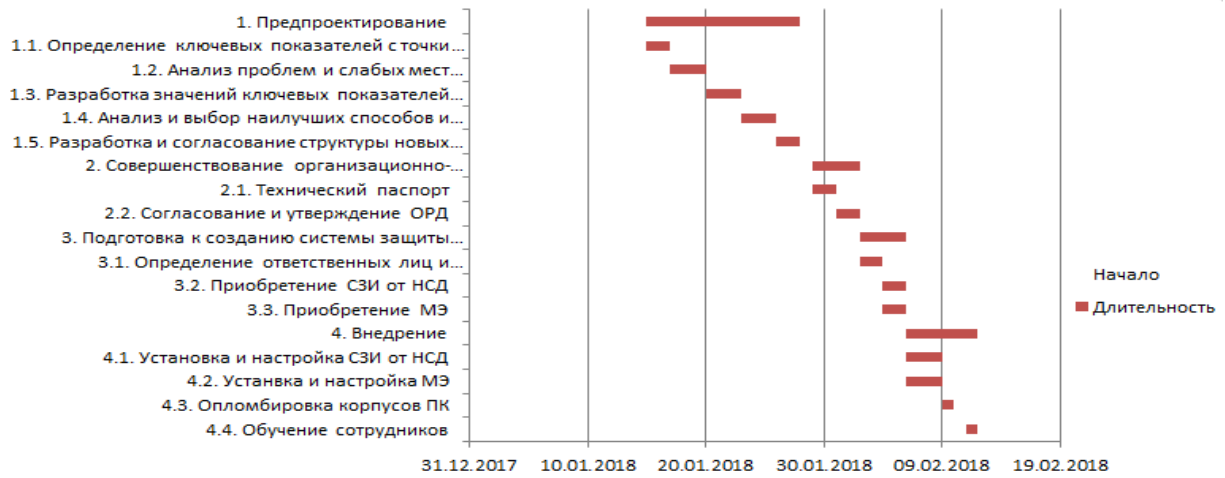

Рисунок 3 – Диаграмма Ганта

Сетевой график – это динамическая модель проекта, отражающая последовательность и зависимость работ, необходимых для завершения проекта. Сетевой график проекта создания системы защиты персональных данных на предприятии ООО «Мечелстрой» представлен в таблице 14.

Для своевременного выполнения работ, а также соответствия плану работ необходимо определить сроки выполнения работ.

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 14– Расписание выполнения работ

i-j	Название работы	T	$T_{рн}$	$T_{пн}$	$T_{ро}$	$T_{по}$
Предпроектирование		13	0	0	13	13
1-2	Определение ключевых показателей существующих бизнес-процессов с точки зрения ИБ	2	0	0	2	2
2-3	Анализ проблем и слабых мест существующих бизнес-процессов	3	2	2	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	2	11	11	13	13
Совершенствование ОРД		4	13	13	23	23
6-7	Технический паспорт	2	13	13	16	16
7-8	Согласование и утверждение ОРД	2	19	19	23	23
	Подготовка реализации проекта создания системы защиты персональных данных	4	23	23	53	53
8-9	Определение ответственных лиц и исполнителей проекта	2	23	23	26	26
9-10	Приобретение СЗИ от НСД	2	26	26	33	33
10-11	Приобретение МЭ	2	33	33	43	43
Внедрение		6	53	53	74	74
11-12	Установка и настройка СЗИ от НСД	3	53	53	57	57
12-13	Установка МЭ	3	57	57	61	61
13-14	Опломбировка корпусов ПК	1	64	64	67	67
14-15	Обучение сотрудников	1	67	67	74	74

3.11. Расчет бюджета проекта и его эффективности

Для устранения уязвимостей, выявленных в ходе предпроектного обследования, необходимо создание системы защиты обработки персональных данных ООО «Мечелстрой». Был проведен расчет затрат на реализацию предложенных мер защиты. Стоимость программного обеспечения приведена в Таблице 15. Стоимость реализации проекта приведена в Таблице 16. Чистая приведенная стоимость проекта представлена в Таблице 17.

Таблица 15 – Стоимость программного обеспечения

Наименование	Количество	Цена за шт. (руб.)	Сумма (руб.)
СЗИотНСД «SecretNet Studio»	1	8 175	7 500
СЗИотНСД+МЭ «Secret Net Studio»	1	9 375	9 375
Итог			16 875

Таблица 16 – Стоимость реализации проекта

Наименование	Стоимость (руб.)
Анализ существующей СЗИ	20 000
Разработка организационно-распорядительной документации	15 000
Установка и настройка «SecretNetStudio»	11 000
Итог	46 000

Затраты на реализацию проекта совершенствования СЗИ на предприятии ООО «Мечелстрой» составили 62875 рублей.

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

Таблица 17– Чистая приведенная стоимость проекта

Периоды	0	1	2	3	4
Первоначальные инвестиции	-55 500				
Выгоды		1 000 000	1 000 000	1 000 000	1 000 000
Стоимость годовой поддержки			-3 200	-3 200	-3 200
Затраты на поддержание инфраструктуры			-5 000	-5 000	-5 000
Итого	-55 500	1 000 000	1 000 000	1 000 000	1 000 000

NPV — это сокращение по первым буквам фразы «NetPresentValue» 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 – 9,25 %.

NPV = 1000000/1,0925+1000000/1,0925^2+1000000/1,0925^3+1000000/1,0925^4 = 915331,808+837832,318+766894,57+701962,994 = 3222021,69

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

3.12. Вывод по третьей главе

В результате выполненных работ по реализации проекта по созданию системы защиты персональных данных ООО «Мечелстрой» было сделано:

- Подготовлен комплект организационно-распорядительной документации;
- Закуплены и установлены программно-аппаратные средства защиты информации;
- Проведено обучение сотрудников порядку работы с персональными данными, обучение основам работы с СЗИ от НСД и инструктаж по антивирусной защите;
- Были рассчитаны риски проекта и определены их максимальные и минимальные значения;
- Был проведен расчет бюджета проекта и его эффективности.

ЗАКЛЮЧЕНИЕ

В результате проведения выпускной квалификационной работы был проведен анализ состояния защиты информации на предприятии ООО «Мечелстрой». В ходе предпроектного обследования были выявлены уязвимости в 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 «Мечелстрой»;
- Проведена оценка экономической эффективности проекта, по ее результатам внедрение системы защиты экономически целесообразно.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон от 27.07.2006 №152-ФЗ (ред. от 10.08.2017) «О персональных данных»;
2. Федеральный закон от 27.07.2006 №149-ФЗ (ред. от 31.12.2017) «Об информации, информационных технологиях и о защите информации»;
3. Указ Президента РФ от 06.03.1997 №188 (ред. от 13.07.2015) "Об утверждении Перечня сведений конфиденциального характера";
4. Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
5. Приказ Министерства строительства и жилищно-коммунального хозяйства №882 от 22.12.2014 «Об утверждении форм раскрытия информации организациями, осуществляющими деятельность в сфере управления многоквартирными домами»;
6. РД «Защита от несанкционированного доступа к информации. Термины и определения». – М.: ГТК РФ, 30.03.1992;
7. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения;
8. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных»: утверждена заместителем директора ФСТЭК России 14.02.2008;
9. ГОСТ 34.602-1989. Информационная технология (ИТ). Комплекс стандартов на автоматизированные системы.Техническое задание на создание автоматизированной системы. – М.: Изд-во стандартов, 1990. – 12 с.
10. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (выписка): утверждена заместителем директора ФСТЭК России 15.02.2008;
11. Куканова Н. Методика оценки риска ГРИФ 2005 из состава DigitalSecurity // BugTraq.Ru. – 2005;
12. Приказ ФСТЭК от 18.02.2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

ПРИЛОЖЕНИЕ А

ПАСПОРТ ПРЕДПРИЯТИЯ

С точки зрения обеспечения
информационной безопасности
22.02.2018 № 1

г. Челябинск

Паспорт предприятия ООО «Мечелстрой»

Содержание паспорта предприятия:

1. Организационно-правовая форма предприятия (организации, учреждения) и его реквизиты
   1.1. Название предприятия: ООО «Мечелстрой»
   2.1. Численность сотрудников: 15 человек
   3.1. Банковские реквизиты:
   ОГРН 1057423036527
   ИНН 7450039995
   КПП 746001001

2. Виды деятельности предприятия (в соответствии с Уставом), наличие лицензий ГЖИ :
   - №074000119 - Предпринимательская деятельность по управлению многоквартирными домами

3. Предполагаемые виды защищаемой информации
Персональные данные

4. Перечень предприятий клиентов и конкурентов
Клиентами ООО "Мечелстрой" являются как физические, так и юридические лица.
Конкурентами ООО "Мечелстрой" являются другие управляющие организации, тсж и кооперативы в сфере жкх.

5. Описание информационной среды предприятия.
ООО "Мечелстрой" работает как с физическими, так и с юридическими лицами. Поэтому в информационную среду предприятия входят базы данных сотрудников и клиентов. Также по специфики работы предприятия в информационную среду входят обширные локально-вычислительные и телефонные сети как между клиентами, так и внутри компании.

Программно-аппаратные средства:

- Пакет MicrosoftOffice, необходим при оформлении (дополнении и изменении) договоров, приказов, распоряжений, отчетности;
- Definity - аналоговая телефонная;
- MicrosoftSecurityEssentials, ESETNOD32 – антивирусноепрограммное обеспечение;
- AdobeReader – для чтения файлов .pdf формата;
- GoogleChrome – интернет;
- WinRAR – для архивации и разархивации документов.

6. Описание строительной инфраструктуры зданий и сооружений.

Организация располагается по адресу ул. Электростальская 23, на первом этаже жилого дома:

- 10-ти этажное здание;
- Ограждено металлической сеткой высотой 2,5 м., на въезде установлен шлагбаум;
-Установлена спринклерная система пожаротушения;
- Установлен пожарный щит с пожарным рукавом и огнетушителем;
- Система центрального водяного отопления;
- Круглосуточное видеонаблюдение, системы безопасности;
- Общая телефонная сеть.

7. Описание местоположения предприятия

Угловое здание располагается около проезжей части. Внутренний двор огорожен забором.

Сведения об организации

1. Название организации: управляющая компания ООО «Мечелстрой»;
2. Местоположение организации: ул. Электростальская 23, первый этаж;
3. Количество сотрудников, постоянно находящихся непосредственно в помещении организации: 6;
4. Описание организационной структуры отдела представлено на рисунке 4;
5. Описание информационной среды отдела представлено в таблице 12.

Таблица 13 – Программно-аппаратные средства информационной среды.

Программа	Назначение	Версия
Windows 7	Операционная система установленная на АРМ сотрудников	6.1.7601.17514
Microsoft Office 2015	Офисный пакет для ра-	15.0.4779.1002

	боты с договорами, приказами, отчетами и т.д.	
Eset NOD32 Antivirus	Программа для обнаружения компьютерных вирусов	11.0.3425.1806
Adobe Reader DC	Программа для чтения, печати и рецензирования файлов PDF	
WinRAR	Программа для сжатия файлов	
GoogleChrome	Интернет браузер	

8. Сведения об аттестации объекта информатизации на соответствие требованиям по безопасности информации

_____
_____
_____
_____
_____
_____
_____
_____
_____

9. Результаты периодического контроля

№, п/п	Дата проведения проверки	Наименование организации, проводящей проверку	Результаты проверки, номер отчетного документа

10. Лист регистрации изменений.

№, п/п	Дата внесения изменения	Описание вносимого изменения	Подпись ответственного за эксплуатацию

11.Схема помещения (относительно других помещений):

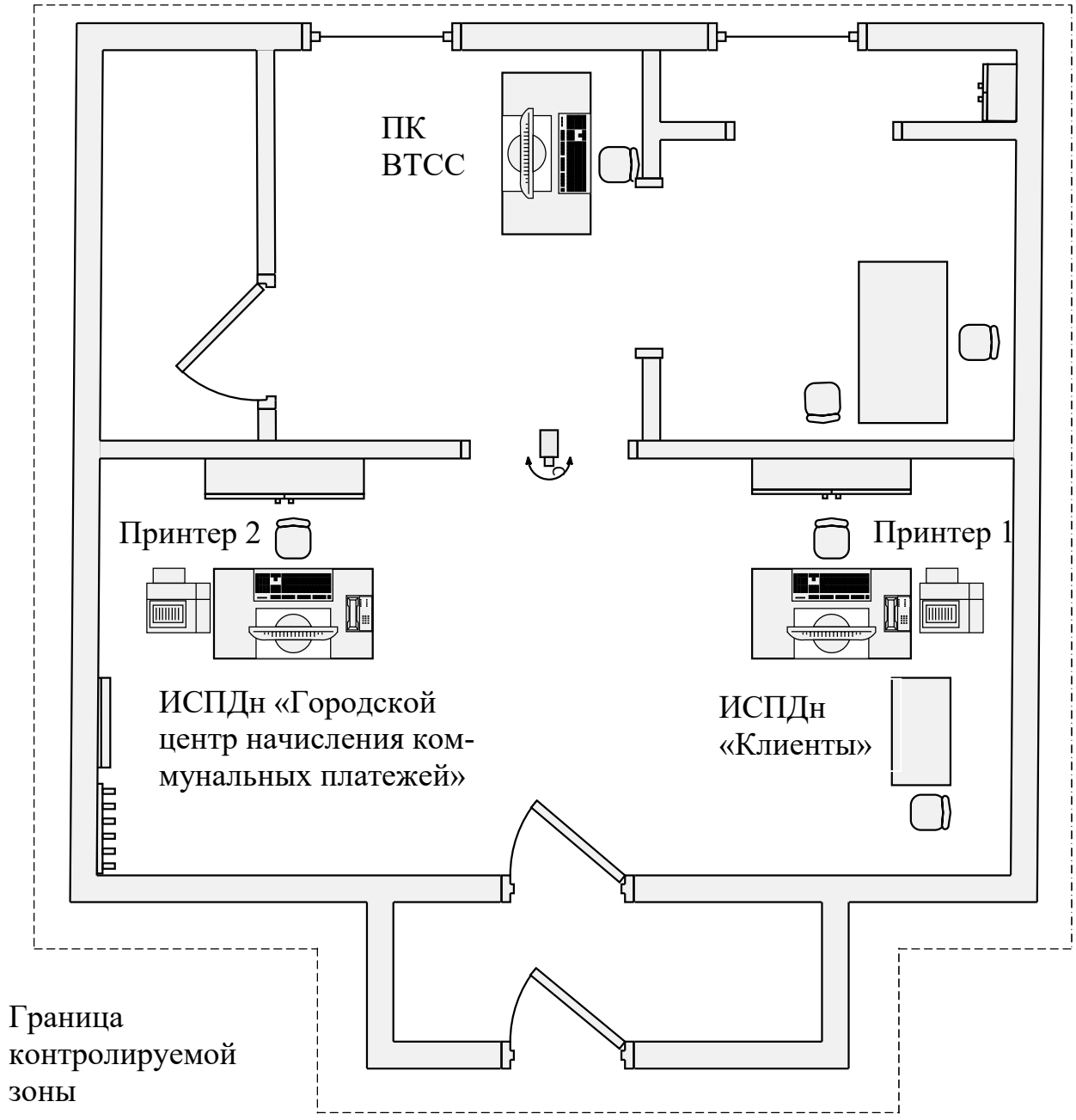

Рисунок 3 – Схема помещения.

12. Описание организационной структуры ООО «Мечелстрой»

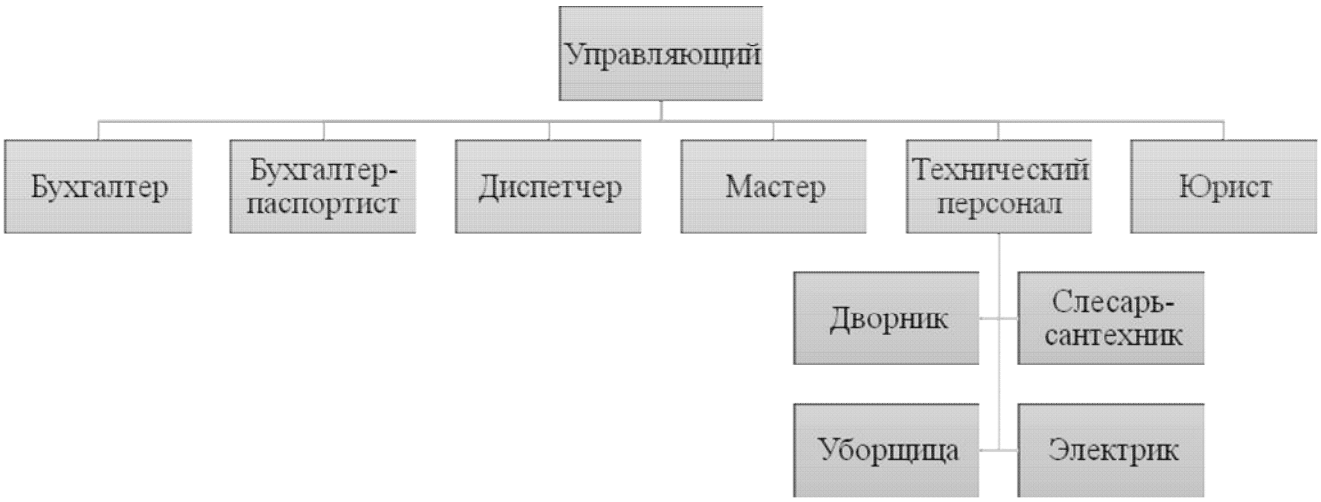

Рисунок 4 - Организационная структура предприятия.

ПРИЛОЖЕНИЕ Б

Утверждаю
Исполнительный директор
Управляющей компании
ООО «Мечелстрой»
Петров Д.Н.

_____
_____ 2018 г.

Акт
установления уровня защищенности персональных данных при их обработке в информационной системеперсональных данных «Клиенты» на предприятии ООО «Мечелстрой» г. Челябинска

Комиссия, сформированная в составе:

Председатель комиссии:
_____.

Члены комиссии:

Чернышёва Полина Сергеевна;

_____.

Комиссия, рассмотрев следующие исходные данные:

1. ИСПДн«Клиенты»расположена по адресу: г. Челябинск, ул. Электростальская 23, 1 этаж.
2. Категория обрабатываемых данных в информационной системе– иные категории персональных данных, принадлежащие жильцам многоквартирных домов.
3. В информационной системе обрабатываются персональные данные менее чем 100000 субъектов персональных данных.
4. ИСПДн«Клиенты» представляет собой автоматизированное рабочее место, (локальная информационная система).
5. ИСПДн «Клиенты» не имеет подключение к сетям связи общего пользования и сетям международного информационного обмена.
6. Режим обработки персональных данных - однопользовательский.

7. Актуальными угрозами безопасности персональных данных являются угрозы 3-го типа - для информационной системы актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.
8. Степень ущерба для свойств информации определена экспертным путем:

   – конфиденциальность – низкая степень ущерба;

   – целостность – низкая степень ущерба;

   – доступность – низкая степень ущерба.
9. Уровень значимости информации:

   – низкий уровень значимости (УЗ 3), т.к. степень ущерба от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности) низкая для всех свойств безопасности информации.

Решила установить информационной системеИСПДн«Клиенты»4-й уровень защищенности персональных данных и установить класс защищенности – К3.

Председатель комиссии:

_____

Члены комиссии: Чернышёва П.С.

_____

Продолжение Приложения Б

Утверждаю
Исполнительный директор
Управляющей компании
ООО «Мечелстрой»
Петров Д.Н.

_____
_____ 2018 г.

Акт
установления уровня защищенности персональных данных при их обработке в информационной системеперсональных данных «Городской центр начисления коммунальных платежей» на предприятии ООО «Мечелстрой» г. Челябинска

Комиссия, сформированная в составе:

Председатель комиссии:

_____.

Члены комиссии:

Чернышёва Полина Сергеевна;

_____.

Комиссия, рассмотрев следующие исходные данные:

1. ИСПДн«Городской центр начисления коммунальных платежей»

   расположена по адресу: г. Челябинск, ул. Электростальская 23, 1 этаж.
2. Категория обрабатываемых данных в информационной системе – иные категории персональных данных, принадлежащие жильцам многоквартирных домов.
3. В информационной системе обрабатываются персональные данные менее чем 100000 субъектов персональных данных.
4. ИСПДн «Городской центр начисления коммунальных платежей» представляет собой автоматизированное рабочее место, (локальная информационная система).

5. ИСПДн «Городской центр начисления коммунальных платежей» имеет подключение к сетям связи общего пользования и сетям международного информационного обмена.
6. Режим обработки персональных данных - однопользовательский.
7. Актуальными угрозами безопасности персональных данных являются угрозы 3-го типа - для информационной системы актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.
8. Степень ущерба для свойств информации определена экспертным путем:

   – конфиденциальность – низкая степень ущерба;

   – целостность – низкая степень ущерба;

   – доступность – низкая степень ущерба.
9. Уровень значимости информации:

   – низкий уровень значимости (УЗ 3), т.к. степень ущерба от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности) низкая для всех свойств безопасности информации.

Решила установить информационной системеИСПДн«Городской центр начисления коммунальных платежей» 4-й уровень защищенности персональных данных и установить класс защищенности – К3.

Председатель комиссии:

_____

Члены комиссии: Чернышёва П.С.

_____

ПРИЛОЖЕНИЕ В

Утверждаю
Исполнительный директор
Управляющей компании
ООО «Мечелстрой»
Петров Д.Н.

_____
_____ 2018 г.

МОДЕЛЬ УГРОЗ
безопасности персональных данных
При их обработке в информационной системе персональных данных «Клиенты»
на предприятии ООО «Мечелстрой»

Окончание приложения В

Утверждаю
Исполнительный директор
Управляющей компании
ООО «Мечелстрой»
Петров Д.Н.

_____
_____ 2018 г.

МОДЕЛЬ УГРОЗ
безопасности персональных данных
При их обработке в информационной системе персональных данных «Городской центр начисления коммунальных платежей»
на предприятии ООО «Мечелстрой»

ПРИЛОЖЕНИЕ Г

ПОЛИТИКА В ОБЛАСТИ ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ СОБСТВЕННИКОВ И ПОЛЬЗОВАТЕЛЕЙ ПОМЕЩЕНИЙ В МНОГОКВАРТИРНЫХ ДОМАХ УПРАВЛЯЮЩЕЙ КОМПАНИЕЙ ООО «МЕЧЕЛСТРОЙ»

1. Общие положения

1.1. Настоящая Политика разработана в соответствии с Конституцией РоссийскойФедерации, Федеральным законом от 27.07.2006 г. № 149-ФЗ «Обинформации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», «Положением об особенностях обработки персональных данных, «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», утвержденных постановлением Правительства Российской Федерации от 01.11.2012г. N 1119, и иными нормативными актами в области защиты персональных данных, действующими на территории Российской Федерации.

1.2. Основные понятия, используемые в Политике:

- управляющая компания - юридическое лицо независимо от организационно-правовой формы, управляющие многоквартирным домом на основании договора управления многоквартирным домом, заключённого с клиентом;
- клиент - гражданин, использующий коммунальные услуги для личных, семейных, домашних и иных нужд, не связанных с осуществлением предпринимательской деятельности, субъект персональных данных;
- услуги управляющей компании - действия управляющей компании по оказанию услуг и выполнению работ по управлению, по надлежащему содержанию и ремонту общего имущества в многоквартирном доме, предоставлению коммунальных услуг собственникам помещений в таком доме и пользующимся помещениями в этом доме лицам, осуществление иной направленной на достижение целей управления многоквартирным домом деятельности;
- персональные данные - информация, сохраненная в любом формате относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), которая сама по себе или в сочетании с другой информацией, имеющейся в распоряжении управляющей компании, позволяет идентифицировать личность Клиента;
- обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;
- распространение персональных данных - действия) направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в

том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;
- использование персональных данных - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;
- конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

1.3. Настоящая Политика устанавливает порядок обработки персональных данных Клиентов, для которых Управляющая компания осуществляет весь спектр услуг по договору управления или по договору оказания услуг по содержанию и (или) выполнению работ по ремонту общего имущества.

1.4. Настоящая Политика обязательна к исполнению всеми сотрудниками Управляющей компании, описывает основные цели, принципы обработки и требования к безопасности персональных данных в Управляющей компании.

1.5. Настоящая Политика разработана с целью защиты прав и свобод человека и гражданина при обработке его персональных данных.

1.6. Персональные данные обрабатываются в целях исполнения договора по предоставлению услуг по договору, одной из сторон которого является Клиент. Управляющая компания собирает данные только в объеме, необходимом для достижения указанной в пункте 2.2 настоящей Политики цели.

1.7. Обеспечение безопасности и конфиденциальности персональных данных является одним из приоритетных направлений в деятельности Управляющей компании.

2. Принципы и цели обработки. Состав персональных данных

2.1. Обработка персональных данных Управляющей компанией осуществляется на основе принципов:
- обработка персональных данных Клиентов осуществляется исключительно для обеспечения соблюдения федеральных законов и иных нормативных правовых актов, соответствия целям, заранее определенным и заявленным при сборе персональных данных;
- объем и содержание обрабатываемых персональных данных субъектов, способы обработки персональных данных соответствуют требованиям федерального законодательства, а также другим нормативным актам и целям обработки персональных данных. Не допускается обработка персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
- персональные данные Управляющая компания получает только у самого Клиента;

- при обработке персональных данных обеспечивается точность персональных данных, их достаточность, а в необходимых случаях актуальность по отношению к целям обработки персональных данных.
Управляющей компанией принимаются необходимые меры по уничтожению (удалению) либо уточнению неполных или неточных данных.

2.2. Обработка персональных данных субъектов персональных данных проводится Управляющей компанией с целью исполнения договорных и иных гражданско-правовых отношений при осуществлении Управляющей компанией хозяйственной деятельности, повышения оперативности и качества обслуживания Клиентов.

2.3. Управляющей компанией обрабатываются следующие категории персональных данных:
- анкетные данные (фамилия, имя, отчество, число, месяц, год рождения и др.);
- паспортные данные;
- адрес регистрации;
- адрес места жительства;
- семейное положение;
- статус члена семьи;
- наличие льгот и преимуществ для начисления и внесения платы за содержание жилого помещения и коммунальные услуги;
- сведения о регистрации права собственности в Едином государственном реестра прав на недвижимое имущество (ином уполномоченном органе), а равно о иных правах на пользование помещением, в том числе о его площади, количестве проживающих, зарегистрированных и временно пребывающих;
- размер платы за содержание жилого помещения и коммунальные услуги (в т.ч. и размер задолженности);
- иные персональные данные необходимые для исполнения договоров.

3. Условия обработки

3.1. Порядок работы с персональными данными Клиентов в Управляющей компании регламентирован действующим законодательством Российской Федерации, внутренними документами Управляющей компании и осуществляется с соблюдением строго определенных правил и условий.

3.2. Обработка персональных данных в Управляющей компании осуществляется путемсбора, систематизации, накопления, хранения, уточнения (обновления, изменения),использования, передачи (предоставления, доступа), обезличивания, блокирования, уничтожения персональных данных исключительно для обеспечения соблюдения федерального законодательства и иных нормативных правовых актов, соответствия целям, заранее определенным и заявленным при сборе персональных данных, учета результатов выполнения договорных и иных гражданско-правовых обязательств с субъектом персональных данных. При этом используется смешанный (автоматизированный и неавтоматизированный) способ обработки персональных данных.

3.3. Согласие на обработку персональных данных не требуется, поскольку обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных - Клиент. Передача персональных данных третьим лицам осуществляется только в соответствии с действующим законодательством, в том числе с использованием защищенных телекоммуникационных каналов связи.

3.4. Управляющая компания не осуществляет трансграничную передачу персональных данных Клиентов.

3.5. Сроки хранения документов, содержащих персональные данные субъектов, определяются в соответствии со сроком действия договора с субъектом персональных данных, Федеральным законом РФ «Об архивном деле в Российской Федерации» № 125-ФЗ от 22.10.2004 г., сроком исковой давности, а также иными требованиями законодательства РФ. По истечении сроков хранения таких документов они подлежат уничтожению.

3.6. С целью защиты персональных данных при их обработке в информационныхсистемах персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий с ними Управляющей компанией применяются организационные и технические меры.

3.7. Персональные данные на бумажных носителях хранятся в служебных помещениях Управляющей компании в условиях, исключающих ознакомление лиц, не имеющих допуска к работе с персональными данными Клиента. Вынос персональных данных за пределы служебных помещений, а равно их передача третьим лицам запрещена.

3.8. Персональные данные Клиентов хранятся в электронном виде в локальной компьютерной сети Управляющей компании, в электронных папках и файлах в персональных компьютерах сотрудников, допущенных к обработке персональных данных Клиентов и защищенных индивидуальным паролем. Передача, а равно разглашение пароля доступа к персональному компьютеру сотрудника управляющей компании не допускается.

4. Основные мероприятия по обеспечению безопасности обработки персональных данных

.4.1. Управляющая компания обязана при обработке персональных данных Клиентов принимать необходимые организационные и технические меры для защиты персональных данных от несанкционированного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий

4.2. Для эффективной защиты персональных данных Клиентов необходимо:

4.2.1. соблюдать порядок получения, учета и хранения персональных данных Клиентов;

4.2.2. применять технические средства охраны, сигнализации;

4.2.3. привлекать к дисциплинарной ответственности сотрудников, виновных в нарушении норм, регулирующих получение, обработку и защиту персональных данных Клиента.

4.3. Документы, содержащие персональные данные Клиентов, хранятся в помещениях Управляющей компании, обеспечивающих защиту от несанкционированного доступа.

4.4. Защита доступа к электронным базам данных, содержащим персональные данные Клиентов, обеспечивается:

использованием лицензионных программных продуктов, предотвращающих несанкционированный доступ третьих лиц к персональным данным Клиентов;

- системой паролей. Пароли устанавливаются системным администратором и сообщаются индивидуально сотрудникам, имеющим доступ к персональным данным Клиентов.

4.5. Копировать и делать выписки персональных данных Клиента разрешается исключительно в служебных целях с письменного разрешения руководителя

5. Порядок предоставления информации, содержащей персональные данные

5.1. При обращении субъекта персональных данных (владельца этих данных или его законного представителя) или получении запроса Управляющая компания безвозмездно предоставляет в течение 30 дней с даты получения запроса или обращения персональные данные, относящиеся к субъекту персональных данных, в доступной форме, исключающей предоставление персональных данных, относящихся к другим субъектам персональных данных.

5.2. Сторонние организации имеют право доступа к персональным данным субъектов персональных данных только, если они наделены необходимыми полномочиями в соответствии с законодательством Российской Федерации, либо на основании договоров с Управляющей компанией, заключенных в связи с требованиями законодательства Российской Федерации.

5.3. При передаче персональных данных субъектов Управляющая компания и уполномоченные им должностные лица соблюдают следующие требования:

- не сообщают персональные данные третьей стороне без письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, установленных федеральным законодательством;
- предупреждают лиц, получающих персональные данные, о том, что эти данные могут быть использованы только в целях, для которых они сообщены, и требуют от этих лиц подтверждения соблюдения этого условия, за исключением случаев, установленных федеральным законодательством;
- не отвечают на вопросы, связанные с предоставлением персональной информации, любым третьим лицам без законных оснований (письменного запроса);
- ведут учет передачи персональных данных субъектов по поступившим в Компанию запросам субъектов.

6. Обязанности управляющей компании

6.1. Управляющая компания обязана:

6.1.1. Осуществлять обработку персональных данных Клиентов исключительно в целях оказания законных услуг Клиентам.

6.1.2. Получать персональные данные Клиента непосредственно у него самого. Если персональные данные Клиента возможно получить только у третьей стороны, то Клиент должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Сотрудники Управляющей компании должны сообщить Клиентам о целях предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа клиента дать письменное согласие на их получение.

6.1.3. Не получать и не обрабатывать персональные данные Клиента о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни, за исключением случаев, предусмотренных законом.

6.1.4. Предоставлять доступ к своим персональным данным Клиенту или его законному представителю при обращении либо при получении запроса, содержащего номер основного документа, удостоверяющего личность Клиента или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись Клиента или его законного представителя. Запрос может быть направлен в электронной форме и подписан электронной цифровой подписью в соответствии с законодательством Российской Федерации. Сведения о наличии персональных данных должны быть предоставлены Клиенту в доступной форме и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

6.1.5. Ограничить право Клиента на доступ к своим персональным данным, если предоставление персональных данных нарушает конституционные права и свободы других лиц.

6.1.6. Обеспечить хранение и защиту персональных данных Клиента от неправомерного их использования или утраты.

6.1.7. В случае выявления недостоверных персональных данных или неправомерных действий с ними оператора при обращении или по запросу субъекта персональных данных или его законного представителя либо уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование персональных данных, относящихся к соответствующему субъекту персональных данных, с момента такого обращения или получения такого запроса на период проверки.

6.1.8. В случае подтверждения факта недостоверности персональных данных оператор на основании документов, представленных субъектом персональных данных или его законным представителем либо уполномоченным органом по защите

прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные и снять их блокирование.

6.1.9. В случае выявления неправомерных действий с персональными данными оператор в срок, не превышающий трех рабочих дней с даты такого выявления, обязан устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений оператор в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, обязан уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

6.1.10. В случае достижения цели обработки персональных данных оператор обязан незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий трех рабочих дней с даты достижения цели обработки персональных данных, если иное не предусмотрено федеральными законами, и уведомить об этом субъекта персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

7. Права Клиента

7.1. Клиент имеет право на:

- доступ к информации о самом себе, в том числе содержащей информацию подтверждения факта обработки персональных данных, а также цель такой обработки; способы обработки персональных данных, применяемые управляющей компанией; сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ; перечень обрабатываемых персональных данных и источник их получения, сроки обработки персональных данных, в том числе сроки их хранения; сведения о том, какие юридические последствия для Клиента может повлечь за собой обработка его персональных данных;
- определение форм и способов обработки его персональных данных;
- ограничение способов и форм обработки персональных данных;
- запрет на распространение персональных данных без его согласия;
- изменение, уточнение, уничтожение информации о самом себе;
- обжалование неправомерных действий или бездействий по обработке персональных данных и соответствующую компенсацию в судебном порядке;
- иные права предусмотренные Законом.

8. Конфиденциальность персональных данных Клиентов

8.1. Сведения о персональных данных Клиентов, являются конфиденциальными.

8.2. Управляющая компания обеспечивает конфиденциальность персональных данных и обязана не допускать их распространения третьим лицом без согласия Клиентов либо наличия иного законного основания.

8.3. Лица, имеющие доступ к персональным данным Клиентов, обязаны соблюдать режим конфиденциальности, они должны быть предупреждены о необходимости соблюдения режима секретности. В связи с режимом конфиденциальности информации персонального характера должны предусматриваться соответствующие меры безопасности для защиты данных от случайного или несанкционированного уничтожения, от случайной утраты, от несанкционированного доступа к ним, изменения или распространения.

8.4. Все меры конфиденциальности при сборе, обработке и хранении персональных данных Клиентов распространяются на все носители информации, как на бумажные, так и на автоматизированные.

8.5. Режим конфиденциальности персональных данных снимается в случае обезличивания или включения их в общедоступные источники персональных данных, если иное не определено законом.

9. Ответственность за нарушение требований, регулирующих получение, обработку и хранение персональных данных.

9.1. Должностные лица Управляющей компании, обрабатывающие персональные данные, несут ответственность в соответствии с действующим законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

9.2. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с действующим законодательством Российской Федерации.

10. Заключительные положения

10.1. Настоящая Политика вступает в силу с момента ее утверждения исполнительным директором Управляющей компании.

10.2. Настоящая Политика подлежит корректировке в случае изменения законодательства Российской Федерации, регулирующих органов в области защиты персональных данных, внутренних документов Управляющей компании в области защиты конфиденциальной информации. При внесении изменений в заголовке Политики указывается номер версии и дата последнего обновления редакции. Новая редакция Положения вступает в силу с момента ее утверждения исполнительным директором Управляющей компании и размещения на сайте Управляющей компании.

10.3. В случае изменения законодательства Российской Федерации в области защиты персональных данных, нормы настоящей Политики, противоречащие законодательству, не применяются до приведения их в соответствие.

10.4. Действующая редакция Политики хранится по адресу: Челябинская область, г. Челябинск, ул. Электростальская, д. 23, неж.пом. 2.

ПРИЛОЖЕНИЕ Д

Утверждаю
Исполнительный директор
Управляющей компании
ООО «Мечелстрой»
Петров Д.Н.

_____
_____ 2018 г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ
на создание системы защиты персональных данныхна предприятииООО «Мечелстрой»

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Полное наименование системы и ее условное обозначение

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

1.2. Наименование заказчика и исполнителя

Предприятие разработчик системы: ООО «Мечелстрой», в лице исполнительного директора.

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

1.3. Перечень документов, на основании которых создается система:

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

2. НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ СИСТЕМЫ

2.1. Назначение создания системы

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

2.2. Цели создания системы

Основной целью проведения работ является приведение всех этапов работы с информации в автоматизированной системе обработки персональных данных ООО «Мечелстрой» 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 автоматизированное рабочее место, носители информации ограниченного доступа, помещение, в котором расположена автоматизированная система:

1. Автоматизированные рабочие места:
   - АРМ АС «Клиенты»;
   - АРМ АС «Городской центр начисления коммунальных платежей».
2. Помещения для хранения и работы с защищаемой информацией:

– Кабинет паспортиста и оператора по работе с начислениями.

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:

– Монитор паспортиста;
– Монитор оператора по работе с начислениями;
– МФУKyocera;
– Оперативная память ПК, входящего в АРМ.

5. Система бесперебойного питания АРМ:

– Источник бесперебойного питания АРМ паспортиста.

6. Носители информации:

– Бумажные носители информации ограниченного доступа;
– Электронные (CD/DVD диски, флэш-накопители с документами, содержащими информацию ограниченного доступа);
– Персонал.

7. Персонал:

– Исполнительный директор;
– Паспортист;
– Оператор по работе с начислениями.

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

3.2.2. Присутствуют следующие уязвимости:

3.2.2.1. АРМ:

– Отсутствие актов категорирования и классификации объекта информатизации.

4. СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО СОЗДАНИЮ 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: Актаопределения уровня защищенности АС, описания технологического процесса обработки информации, 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:
– Программа и методика испытаний объекта информатизации;
– Акт обследования автоматизированной системы;
– Акт классификации автоматизированной системы;
– Описание технического процесса обработки информации ограниченного доступа;
– Технический паспорт.
7.2. Отчетные документы предоставляются Заказчику в электронном виде в формате документов MicrosoftOffice 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 Е