Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Южно-Уральский государственный университет
(национальный исследовательский университет)»
Высшая школа электроники и компьютерных наук
Кафедра «Защита информации»

РАБОТА ПРОВЕРЕНА
Рецензент, сотрудник IT-отдела
ОАО «Областной аптечный склад»
_____ А.С. Веденеева
_____ 2018 г

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

Построение комплексной системы защиты информации предприятия «ИП Суский»

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ – 10.05.03.2018.348.ПЗ ВКР

Консультанты

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

Экономическая часть,
ст. преп.
_____ С.А. Сабельников
_____ 2018 г.

Руководитель проекта,
н.с. МОЦ «Информационная безопасность»
_____ А.Е. Баринов
_____ 2018 г.

Автор проекта,
студент группы КЭ-530
_____ А.С. Суская
_____ 2018 г.

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

Челябинск 2018

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

Высшая школа электроники и компьютерных наук
Кафедра «Защита информации»

Специальность 10.05.03 «Информационная безопасность автоматизированных систем»

УТВЕРЖДАЮ
Заведующий кафедрой
_____ А.Н. Соколов

_____ 2018 г.

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

Суской Анастасии Сергеевны

Группа КЭ-530

1. Тема работы

Построение комплексной системы защиты информации предприятия «ИП Суский»

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

2. Срок сдачи студентом законченной работы 27.05.2018

3. Исходные данные к работе

Отчет о преддипломной практике, нормативно-правовые документы в области защиты информации, документация предприятия-базы практики

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

1. Проведение предпроектного обследования предприятия «ИП Суский»
2. Теоретическое обоснования средств защиты информации
3. Разработка проекта системы защиты информации

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

Презентация «Построение комплексной системы защиты информации предприятия «ИП Суский» в формате PowerPoint 2007 (pptx). Количество слайдов -

Всего ___ листов

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

Раздел	Консультант	Подпись, дата	
		Задание выдал (консультант)	Задание принял (студент)
Безопасность жизнедеятельности	Н.В. Глотова		
Оценка экономической эффективности проекта	С.А. Сабельников		

7. Дата выдачи задания 08 декабря 2017

Руководитель,
н.с. МОЦ «Информационная безопасность»_____ А.Е. Баринов

Задание принял к исполнению _____ А.С. Суская

КАЛЕНДАРНЫЙ ПЛАН

Наименование этапов выпускной квалификационной работы (проекта)	**Срок выполнения этапов работы**	**Отметки о выполнении руководителя**
Введение	*01.03.2018*	
Анализ состояние защиты в «ИП Суский» и существующие проблемы	06.03.2018	
Теоретическое обоснование средств защиты информации	26.04.2018	
Разработка проекта по внедрению комплексной системы защиты информации на предприятии «ИП Суский»	*17.05.2018*	
Безопасность жизнедеятельности	*18.05.2018*	
Заключение	*19.05.2018*	
Библиографический список	*20.05.2018*	
Предзащита ВКР	*09.06.2018*	
Защита ВКР	*16.06.2018*	

Заведующий кафедрой _____ А.Н. Соколов

Руководитель работы _____ А.Е. Баринов

Студент _____ А.С. Суская

АННОТАЦИЯ

Суская.А.С. Построение комплексной системы защиты информации предприятия – Челябинск: ЮУрГУ, КЭ-530, 108 с., 9 ил., 25 табл., библиогр. список – 16 наим., 18 прил.

Выпускная квалификационная работа выполнена с целью разработки комплексной системы защиты информации предприятия «ИП Суский». Данная работа состоит из четырех глав.

В первой главе проведен анализ информационной системы «ИП Суский», в результате которого был разработан паспорт предприятия, выявлены объекты защиты, разработана модель угроз и уязвимостей, произведён расчёт рисков для выявленных объектов защиты.

Во второй главе проведено теоретическое обоснование выбора средств защиты информации, сделаное на основании анализа выявленных угроз, уязвимостей и возможных методов по их устранению.

В третьей главе разработан проект комплексной системы защиты информации. В рамках разработки проекта КСЗИ «ИП Суский» были определены объекты поставки, рассчитаны риски реализации проекта, разработана структурная схема реализации проекта, построена матрица ответственности, разработана диаграмма Ганта.

В четвёртой главе проведен анализ потенциально опасных и вредных производственных факторов, на основе которых, выработаны рекомендации для работы организации.

ОГЛАВЛЕНИЕ

СОКРАЩЕНИЯ И ОПРЕДЕЛЕНИЯ

ЗИ – защита информации;
СЗИ – средство защиты информации;
ИС – информационная система;
НСД – несанкционированный доступ;
ПДн – персональные данные;
КСЗИ – комплексная система защиты информации;
КТ – коммерческая тайна;
АРМ – автоматизированное рабочие место;
ВКР – выпускная квалификационная работа;
ПО – программное обеспечение;
РД – руководящие документы;
РФ – Российская Федерация;
ФЗ – Федеральный закон;
ФСБ – Федеральная служба безопасности;
ФСТЭК – Федеральная служба по техническому и экспортному контролю;

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

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

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

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

Критичность ресурса – степень значимости ресурса для информационной системы, т.е. как сильно реализация угроз информационной безопасности на ресурс повлияет на работу информационной системы. Единица измерения рубли;

Критичность реализации угрозы – степень влияния реализации угрозы на ресурс, т.е. как сильно реализация угрозы повлияет на работу ресурса. Единица измерения проценты(%);

Вероятность реализации угрозы через данную уязвимость в течение года – степень возможности реализации угрозы через данную уязвимость в тех или иных условиях. Единица измерения проценты(%).

ВВЕДЕНИЕ

Очень часто мы слышим об утечках конфиденциальной информации из крупных предприятий и о мерах, которые принимаются ими для минимизации рисков возникновения инцидентов безопасности. Но в тоже время средства массовой информации практически не освещают вопрос информационной безопасности на предприятиях малого бизнеса.

Цели крупного и малого бизнеса одинаковые – получение прибыли. Для этого предприятия ежедневно обрабатывают различные данные, несущие большое значение для компании. Поэтому именно коммерческая тайна является сердцевиной многих видов и форм бизнеса. Для ее защиты издаются новые постановления, указы, стандарты, направленные на усиление ИБ.

Организация комплексной системы защиты информации обеспечивает непрерывность бизнеса, а так же устойчивое функционирование коммерческого предприятия и предотвращения угроз его безопасности.

Объектом выпускной квалификационной работы является «ИП Суский».

Предметом дипломной работы является комплексная система защиты информации.

Целью выпускной квалификационной работы является построение комплексной системы защиты информации.

Для достижения поставленной цели необходимо:

1. Проанализировать информационную среду «ИП Суский»;
2. Определить объекты защиты и привести теоретическое обоснование рекомендуемых средств защиты информации;
3. Разработать проект комплексной системы защиты информации «ИП Суский».

В рамках данной работы наибольшее внимание будет уделено коммерческой тайне, так как именно она имеет наибольшую значимость и необходимость защиты на предприятие.

1. АНАЛИЗ СОСТОЯНИЯ ЗАЩИТЫ ИНФОРМАЦИИ В «ИП СУСКИЙ» И СУЩЕСТВУЮЩИЕ ПРОБЛЕМЫ

1.1. Разработка паспорта

Для построения комплекса мер по защите информации и получения общего представления о защищаемом объекте был составлен паспорт предприятия (Приложение А).

В паспорте предприятия представлены реквизиты организации, перечислены основные виды деятельности предприятия, виды защищаемой информации, организационная структура, перечень конкурентов.

Данная информация была получена в результате устного опроса директора предприятия и непосредственного ознакомления с информационной системой компании.

В качестве объекта защиты была выбрана вся организация «ИП Суский», так как предприятие расположено в одном помещение, имеет 7 сотрудников и 3 защищаемых АРМ.

1.2. Разработка модели деятельности

В ходе анализа работы «ИП Суский» была построена модель его деятельности (Приложение Б). Эта модель позволяет ознакомиться с основными бизнес-процессами предприятия. В данной схеме отражены входные и выходные параметры, ресурсы, внешнее воздействие.

1.3. Выявление защищаемой информации

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

- сведения, составляющие коммерческую тайну (на основании Федерального закона от 29.07.2004 N 98-ФЗ (ред. от 12.03.2014) "О коммерческой тайне");
- сведения, составляющие персональные данные (Федеральный Закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»)
- общедоступная информация, располагаемая в общедоступных источниках и сети интернет (на основании Федерального закона от 27.07.2006 N 149-ФЗ (ред. от 21.07.2014) "Об информации, информационных технологиях и о защите информации").

На предприятии отсутствует режим коммерческой тайны, соответственно для установления режима необходима разработка и реализация комплекса мер:

1. Определение перечня информации, составляющей коммерческую тайну.
2. Ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка.

3. Учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана.

4. Регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров.

5. Нанесение на материальные носители, содержащие информацию, составляющую коммерческую тайну, или включение в состав реквизитов документов, содержащих такую информацию, грифа "Коммерческая тайна" с указанием обладателя такой информации.

В рамках данного пункта был разработан перечень сведений, составляющих коммерческую тайну (Приложение Г), положение о режиме коммерческой тайне (Приложение В) и подготовлены соответствующие приказы об их утверждении (Приложение Е), а так же разработана инструкция по работе с коммерческой тайной (Приложение Ж).

Так как на предприятии есть персональные данные, но автоматизированная обработка не производится в связи с малым объемом, то была разработана «Инструкция о порядке физической охраны помещений, содержащих носители персональных данных» (Приложение З), Положении о разграничении прав доступа к персональным данным» (Приложение И), «Инструкция по обработке персональных данных без использования средств автоматизации» (Приложение К), а также «Акт об уничтожении носителей, содержащих персональные данные» (Приложение Л).

1.4. Описание информационной среды

Для разработки комплексной системы защиты информации необходимо проанализировать информационную систему «ИП Суский». Данный анализ позволит выявить характеристики АРМ и программного обеспечения, которое установлено на оборудованиях.

Таблица 1- Аппаратное обеспечение

№	Наименование	Характеристики	Кол-во	Год выпуска
1	2	3	4	5
АРМ				
1	Системный блок Krauler	Inter Core i3, 2.93 ГГц, 5 Гб, HDD 1 Тб, NVIDIA GeForce GTX 650, Ethernet, DVD±RW	2	2012
2	Монитор Samsung S23C570	LED; 23; 1920x1080	2	2013
3	Клавиатура Smartbuy SBK-206US-K	Тип – проводная; Интерфейс – USB; Количество клавиш - 104	2	2014
4	Мышь Microsoft Wireless Mobile Mouse 3500	Оптическая лазерная мышь, 1000 dpi, ин-	2	2013

Продолжение Таблицы 1

1	2	3	4	5
		терфейс подключения – USB		
5	МФУ Samsung CLX-3305W	Лазерный, формат листа – А4, 2400x600 dpi, 18 стр/мин	1	2013
6	Маршрутизатор ASUS RT-N15U	Количество LAN портов – 4, базовая скорость передачи данных 1000 Мб/с	1	2012
7	Источник бесперебойного питания APC APC Back-UPS BE400-RS	Максимальная выходная мощность: 240 Ватт / 400 ВА	2	2012
8	Телефон ARK U3	Цветной TFT дисплей, 160x128px, телефонная книга на 1000 номеров	1	2016

Таблица 2 – Программные средства

№	Наименование	Описание	Версия
АРМ			
1	Windows 10	Операционная система	16299.309
2	Пакет Microsoft Office 2007	Офисный пакет для работы с договорами, приказами, отчетами и т.д.	12.0.6786.5000
3	Avast Antivirus	Антивирусное ПО	17.6.2310
4	1с:Предприятие	Программа для оформления отчетности предприятия	8
5	Adobe Reader DC	Программа для чтения, печати и рецензирования файлов PDF	15.020.20042
6	WinRAR	Программа для сжатия файлов	5.40
7	Mail.ru Агент	Программа для мгновенного обмена сообщениями	10.0.20182
8	Google Chrome	Интернет браузер	65.0.3325.181

1.5. Выявление объектов защиты

Объект защиты информации – это информация или носитель информации, или информационный процесс, который необходимо защищать в соответствии с целью защиты информации. Подробный перечень представлен в (Приложение Г).

На основании предпроектного обследования «ИП Суский» можно выделить следующий перечень объектов защиты информации:

– помещение для работы с защищаемой информацией;
– автоматизированные рабочие места сотрудников;
– линии и средства связи;
– устройства ввода-вывода и отображения информации;
– системы дублирования и хранения информации
– носители информации
– информационная инфраструктура;
– персональные данные, обрабатываемые без использования средств автоматизации;
– персонал.

1.6. Разработка модели угроз и уязвимостей для важных объектов защиты

Моделью угроз и уязвимостей является описание существующих угроз информационной безопасности и уязвимостей, через которые реализуется данная угроза.

Для составления модели угроз и уязвимостей мы руководствуемся главой «Определение актуальных угроз безопасности информации в информационной системе», описанной в методическом документе ФСТЭК, который утвержден указом президента от 16 августа 2004 г. №1085 («Методика определения угроз в информационных системах») и «Специальных требований и рекомендаций по технической защите конфиденциальной информации» (Утверждены приказом Гостехкомиссии России от 02.03.2001 № 282), а так же опросом сотрудников и руководителя.

Для выявления наиболее значимых угроз ИБ предприятия нужно выделить важные объекты защиты информации относительно коммерческой тайны и персональных данных, к которым относятся:

– персонал;
– ПДн на бумажных носителях;
– электронные носители информации;
– АРМ сотрудников, на которых обрабатывается коммерческая информация.

На основе выделенных важных объектов защиты информации выявим наиболее значимые угрозы, представленные в Таблице 3.

Таблица 3 – Модель угроз и уязвимостей

Объект	Угроза	Уязвимость
1	2	3
Персонал	Разглашение информации, составляющей коммерческую тайну	Нарушение соглашения о неразглашении информации, подлежащей защите

Продолжение Таблицы 3

1	2	3
		Отсутствие или неактуальность документов, регламентов по защите коммерческой тайны
	Утечка носителей информации	Отсутствие учета носителей содержащих коммерческую тайну
		Отсутствие пропускного режима
	Уничтожение, модификация, блокировка носителей информации содержащих коммерческую тайну, АРМ сотрудников	Отсутствие регламента доступа в помещение, в котором обрабатывается коммерческая тайна
		Отсутствие мероприятий по повышению информационной грамотности
		Несанкционированное проникновение в помещение
ПДн на бумажных носителях	Несанкционированный доступ в помещение, где хранятся бумажные носители	Отсутствие видеонаблюдения
		Отсутствие пропускного режима
Электронные носители информации	Модификация, уничтожение, хищение носителей информации	Отсутствие видеонаблюдения
		Отсутствие журнала учета носителей
АРМ сотрудников, на которых обрабатывается коммерческая информация	Несанкционированный доступ к АРМ сотрудников	Отсутствие средств защиты от НСД
		Отсутствие регламента доступа к АРМ
		Наличие вредоносного ПО в системе
		Отсутствие пломбирования корпуса АРМ
		Нарушение пропускного режима
		Отсутствие авторизации на аппаратном уровне

1.7. Расчет рисков важных объектов защиты

Чтобы выявить наиболее вероятные угрозы для объекта информации и уязвимостей, через которые они могут быть реализованы, необходим расчет рисков. Он является одним из важнейших этапов в создании КСЗИ.

Для расчета рисков важных объектов была использована «Методика определения актуальных угроз безопасности персональных данных при их обработки в информационных системах персональных данных» (утв. ФСТЭК РФ от 14 февраля 2008г)[1], так как утверждённой методики для коммерческой тайны нет.

Перед оценкой возможности реализации угрозы необходимо установить уровень исходной защищенности ИС. Для этого составляем Таблицу 4.

Таблица 4 – Исходный уровень защищенности ИС

Технические и эксплуатационные характеристики информационной системы	Уровень защищенности ИС
По территориальному размещению: локальная ИС	Высокий
По наличию соединения с сетями общего пользования: имеющая одноточечный выход в сеть общего пользования	Средний
По встроенным (легальным) операциям с записями баз персональных данных: запись, удаление, сортировка	Средний
По разграничению доступа к информации: ИС, к которой имеют доступ определенные перечнем сотрудники организации	Средний
По наличию соединений с другими базами данных и другими ИС: в которой используется одна база данных, принадлежащая организации – владельцу данной ИС	Высокий
По объему данных, которые предоставляются сторонним пользователям системы без предварительной обработки: предоставляющая часть	Средний

На основании составленной таблицы можно сделать вывод, что исходный уровень защищенности информационной системы является «средним», так как 4 показателя из 6 имеют средний уровень защищенности, поэтому числовой коэффициент Y_1 равен 5 ($Y_1 = 5$).

Затем определяем вероятность реализации угрозы Y_2. В зависимости от вероятности угрозы (маловероятно, низкая вероятность, средняя вероятность и высокая вероятность), каждой градации вероятности возникновения угрозы ставится в соответствие числовой коэффициент Y_2, а именно 0, 2, 5 и 10.

Составим таблицу вероятности для актуальных угроз в соответствие с числовыми коэффициентами (Таблица 5).

Таблица 5 – Вероятность реализации угроз

Объект	Угроза	Уязвимость	Вероятность реализации угрозы, Y_2
Персонал	Разглашение информации, составляющей коммерческую тайну	Высокая вероятность	10
	Утечка носителей информации	Высокая вероятность	10
	Уничтожение, модификация, блокировка носителей информации содержащих коммерческую тайну, АРМ сотрудников	Средняя вероятность	5
ПДн на бумажных носителях	Несанкционированный доступ в помещение, где хранятся бумажные носители	Высокая вероятность	10
Электронные носители информации	Модификация, уничтожение, хищение носителей информации	Высокая вероятность	10
АРМ сотрудников, на которых обрабатывается коммерческая информация	Несанкционированный доступ к АРМ сотрудников	Высокая вероятность	10

Полученные значения Y_1 и Y_2, необходимы для расчета коэффициента реализуемости угрозы Y. Данный коэффициент рассчитывается по формуле:

$$Y = {(Y_1 + Y_2)}/{20}$$

Рассчитаем коэффициент реализуемости угроз и внесем результаты в таблицу (Таблица 6).

Таблица 6 – Коэффициент реализуемости угроз

Объект	Угроза	Коэффициент реализации угрозы, Y	Вероятность реализации угрозы, Y_2
1	2	3	
Персонал	Разглашение информа-	0,75	Высокая

Продолжение таблицы 6

1	2	3	4
	ции, составляющей коммерческую тайну		
	Утечка носителей информации	0,75	Высокая
	Уничтожение, модификация, блокировка носителей информации содержащих коммерческую тайну, АРМ сотрудников	0,5	Средняя
ПДн на бумажных носителях	Несанкционированный доступ в помещение, где хранятся бумажные носители	0,75	Высокая
Электронные носители информации	Модификация, уничтожение, хищение носителей информации	0,75	Высокая
АРМ сотрудников, на которых обрабатывается коммерческая информация	Несанкционированный доступ к АРМ сотрудников	0,75	Высокая

В данном пункте мы установили исходный уровень защищенности ИС «ИП Суский», а так же рассчитали коэффициент реализуемости угроз выявленных в пункте 1.6. Возможность реализации угрозы позволяет выявить приоритетные направления для устранения установленных угроз.

1.8. Разработка технического задания для создания КСЗИ

В результате проведенной работы были получены сведения, которые необходимы для разработки технического задания на создание комплексной системы защиты информации (Приложение Д).

Основой для ТЗ является ГОСТ 34.602-1989 «Техническое задание на создание автоматизированной системы», который включает в себя следующие разделы:

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

8) требования к документированию;
9) источники разработки.

1.9. Вывод

В первой главе было проведено предпроектное обследование информационной системы «ИП Суский», был разработан паспорт предприятия, в котором представлены общие сведения об организации. Выявлены объекты защиты информации, разработана модель угроз и рассчитаны риски для важных объектов защиты.

Основываясь на модель деятельности «ИП Суский» и результатами анализа ИС предприятия была выявлена информация ограниченного доступа, то есть сведения, составляющие коммерческую тайну. В «ИП Суский» отсутствует режим коммерческой тайны. Для этого в рамках ВКР был разработан комплекс организационно-распорядительных документов и сформулированы рекомендации по реализации, требуемых законодательством, мер по защите информации.

В результате проведенной работы следует, что предприятие защищено не должным образом. В «ИП Суский» наивысшую степень реализации угроз имеют угрозы связанные с: разглашением, копированием, хищением информации, составляющую коммерческую тайну; утечкой, хищением носителей информации, составляющих коммерческую тайну, несанкционированный доступом к АРМ сотрудников, а так же несанкционированным доступом в помещение с хранящимся в нем ПДн.

2. ТЕОРЕТИЧЕСКОЕ ОБОСНОВАНИЕ ВЫБОРА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

2.1. Обзор возможных методов устранения уязвимостей

Одним из важнейших этапов работы по созданию комплексной системы защиты информации является определение методов и средств, необходимых для устранения выявленных у объектов угроз и уязвимостей.

На данном этапе необходимо найти наиболее эффективные пути решения задачи защиты объектов.

2.2. Угрозы, связанные с НСД

В условиях развития информационных технологий и высокой конкурентной среды, повышается интерес сторонних предприятий к информации, составляющую коммерческую тайну.

Большинство современных предприятий занимается обработкой информации в рамках внутренней информационной системы, а значит существует те, кто пытается завладеть ограниченной информации путем несанкционированного доступа.

Несанкционированный доступ – это противоправное действие, в результате которого злоумышленник получает доступ к защищаемой информации для сторонних лиц.

В результате предпроектного обследования, были выявлены следующие угрозы, связанные с несанкционированном доступом:

- несанкционированный доступ к АРМ сотрудников;
- несанкционированный доступ в серверное помещение.

2.2.1. Несанкционированный доступ к АРМ сотрудников

Несанкционированный доступ к АРМ сотрудников может быть реализован путем следующих уязвимостей:

- отсутствие регламента доступа к АРМ;
- отсутствие видеонаблюдения;
- отсутствие средств защит от НСД;
- наличие вредоносного ПО в системе.

Для устранения первой уязвимости требуется разработать матрицу доступа, содержащую список лиц, имеющих доступ в помещение с обработкой коммерческой тайны. Так же нужно назначить ответственное лицо, которое будет контролировать соблюдение этого мероприятия.

Вторую уязвимость можно устранить с помощью внедрения системы видеонаблюдения на объект. Система видеонаблюдения необходима для контроля сотрудников, имеющих доступ к информации ограниченного доступа и выявления несанкционированного проникновения в помещение с этой информацией.

Для устранения третьей уязвимости требуется установить специально программно-аппаратное средство защиты информации.

На компьютерах предприятия «ИП Суский» уже было установлено средство защиты от вирусов, которое постоянно обновляется. Вместе с сотрудником, отвечающим за безопасность IT-инфраструктуры, было принято решение оставить Avast Antivirus. Данное решение было принято на основе более низкой цены, по сравнению с другими антивирусами, а также с учетом системных требований.

2.2.2. Несанкционированный доступ помещение, где хранится информация ограниченного доступа

В данном виде угроз могут быть использованы следующие уязвимости:

- нарушение пропускного режима;
- отсутствие охранной сигнализации помещения;
- отсутствие регламента доступа к помещению.

Первая и третья уязвимость устраняется такими же методами, как и в предыдущем пункте главы 2.2.1 («Несанкционированный доступ к АРМ сотрудников»)

Путем опроса руководства и сотрудников, а также зрительного осмотра помещения, было выявлено, что в помещение подключены датчики охранной сигнализации.

2.2.3. Несанкционированный доступ в помещение, где хранятся персональные данные

Несанкционированный доступ в помещение, где хранятся персональные данные может быть реализован путем следующих уязвимостей:

- отсутствие видеонаблюдения;
- отсутствие пропускного режима.

Первую уязвимость можно устранить путем внедрения системы видеонаблюдения.

Для устранения второй уязвимости необходимо ограничить доступ в места хранения документов. Так как помещение одно, то все бумажные носители, содержащие ПДн, хранятся в сейфе с кодовым замком, отдельно от другой информации ограниченного доступа.

2.3. Разглашение информации, составляющую коммерческую тайну

Одним из путей разглашения информации, составляющей коммерческую тайну, является утечка информации по акустическому каналу, реализованному в подслушивании разговоров в помещении или открытой местности, с использованием средств для записи разговора.

Данная угроза реализуется через следующие уязвимости:

- несоблюдение соглашения о неразглашении информации подлежащей защите;
- отсутствие звукоизоляции помещений;

– нарушение пропускного режима;
– отсутствие документов и регламентов по защите коммерческой информации или их неактуальность.

Первая и четвертая уязвимость устраняется путем разработки новой организационно-распорядительной документации в области защиты коммерческой тайны предприятия, включающее в себя положение о коммерческой тайне, должностные инструкции, матрица доступа, политика допустимого использования в физической безопасности и т.д. Так же следует провести специальные тренинги и профилактические беседы с сотрудниками предприятия, включающее в себя подробное разъяснение и доведение до их сведения мер ответственности за разглашение защищаемой информации. Каждый сотрудник должен расписаться в договоре, что ознакомлен с положением и понимает ответственность за разглашение сведений, составляющих коммерческую тайну.

Обязательно нужно рассмотреть отсутствие звукоизоляции помещений и установку устройств генерации шумов.

Но по мнению сотрудника, отвечающего за IT-инфраструктуру, утечка через вышеописанные уязвимости маловероятна и предприятие готово принять данный риск. Поэтому было решено отказаться от предложенных средств и мер по улучшению звукоизоляции помещения и установки генераторов шумов в помещении.

2.4. Утечка носителей информации

Данный вид угрозы может быть реализован с помощью следующей уязвимости:

– Отсутствие учета носителей, содержащих коммерческую тайну.

Эта уязвимость может быть устранена, с помощью инструкции по организации работы с электронными носителями, содержащие коммерческую тайну (Приложение М).

В виду того, что доступ к носителям информации имеют только 3 сотрудника, а так же малое количество носителей, то на данном предприятии нецелесообразно вводить автоматизированную защиту носителей информации.

2.5. Вывод

На основе анализа угроз и уязвимостей на предприятии был разработан комплекс мероприятий, направленных на минимизацию вероятности реализации выявленных угроз:

1) угрозы, связанные с несанкционированным доступом к АРМ сотрудников:
   – отсутствие регламента доступа к АРМ;
   – отсутствие видеонаблюдения;
   – отсутствие средств защиты от НСД;
   – наличие вредносного ПО в системе.
2) угрозы, связанные с НСД:
   – несанкционированный доступ к АРМ сотрудников;

– несанкционированный доступ в серверное помещение.

3) угрозы, связанные с несанкционированным доступом в помещение:

– нарушение пропускного режима;

– отсутствие охранной сигнализации помещения;

– отсутствие регламента доступа к помещению.

4) угрозы, связанные с разглашением информации, составляющей коммерческую тайну:

– несоблюдение соглашения о неразглашении информации подлежащей защите;

– отсутствие звукоизоляции помещений;

– нарушение пропускного режима;

– отсутствие документов и регламентов по защите коммерческой информации или их неактуальность.

5) Угрозы, связанные с утечкой носителей информации:

– отсутствие учета носителей, содержащих коммерческую тайну.

Основываясь на мнении руководства было принято не использовать следующие меры защиты информации, в связи с тем, что данные угрозы были оценены как маловероятные:

– установка другого антивирусного ПО, было принято решение остаться на Avast Antivirus;

– улучшение звукоизоляции помещения;

– установка генератора акустических шумов.

3. РАЗРАБОТКА ПРОЕКТА ПО ВНЕДРЕНИЮ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ «ИП СУСКИЙ»

3.1. Описание объекта

Предприятие «ИП Суский» занимается оптовой торговлей приборами, оборудованием общепромышленного и специального назначения. Из чего можно заключить, что в организации имеются большие потоки информации, которые обрабатываются внутри предприятия и нуждаются в защите. Потоки защищаемой информации (Таблица 7).

Таблица 7 – Потоки защищаемой информации

Входящие	Исходящие
Переписка с клиентами	
Документооборот	
Информация о клиентах; Информация о поставщиках; Информация о закупках;	Отчеты о продажах; Договора поставки; Отчеты о задолженностях покупателей; База данных клиентов; База данных поставщиков;

3.2. Резюме проекта

Проект системы защиты информации разработан на основе утвержденного технического задания на создание КСЗИ предприятия «ИП Суский» (Приложение Д).

Для выполнения поставленной цели, требуется разработать ряд организационных, инженерно – технических и программно – аппаратных мер. Посредством матрицы ответственности за каждым этапом работы установлены ответственные лица. Результатом проекта будет являться созданная комплексная система защиты информации, содержащая внедрение программных и инженерно – технических средств, соответствующих требованием нормативно-правовых актов и поставленным целям.

3.3. Цели и задачи проекта

Целью разработки КСЗИ «ИП Суский» являются:

- предотвращение утечки, хищения, утраты, искажения, подделки информации;
- защита информации составляющей коммерческую тайну в соответствии с законодательством
- защита информации, содержащую сведения о персональных данных в соответствии с законодательством.

3.4. Объекты поставки проекта

3.4.1. Организационно-распорядительная работа

В данном проекте предусмотрено создание необходимых документов в области информационной безопасности:

- положение о коммерческой тайне;
- перечень сведений, составляющих коммерческую тайну;
- журнал учета носителей.

3.4.2. Программно-аппаратные инженерно-технические меры

Данный проект предусматривает приобретение и внедрение таких программно-аппаратных средств как:

- система защиты информации от несанкционированного доступа «Secret Net Studio»

3.4.3. Обучение персонала

Необходимо обучить сотрудников новым требованиям защиты информации, с разъяснением значимости введения организационно-распорядительных документов, предусмотренных проектом, а также программно-аппаратных решений.

3.4.4. Внедрение системы видеонаблюдения

Для уменьшения риска несанкционированного доступа в помещение с АРМ сотрудников и носителями, хранящими персональные данные, необходимо установить систему видеонаблюдения. Мной был предложен вариант установки видеокамер (Рисунок 1) с учетом угла обзора, а так же обязательной установки напротив входа в помещение.

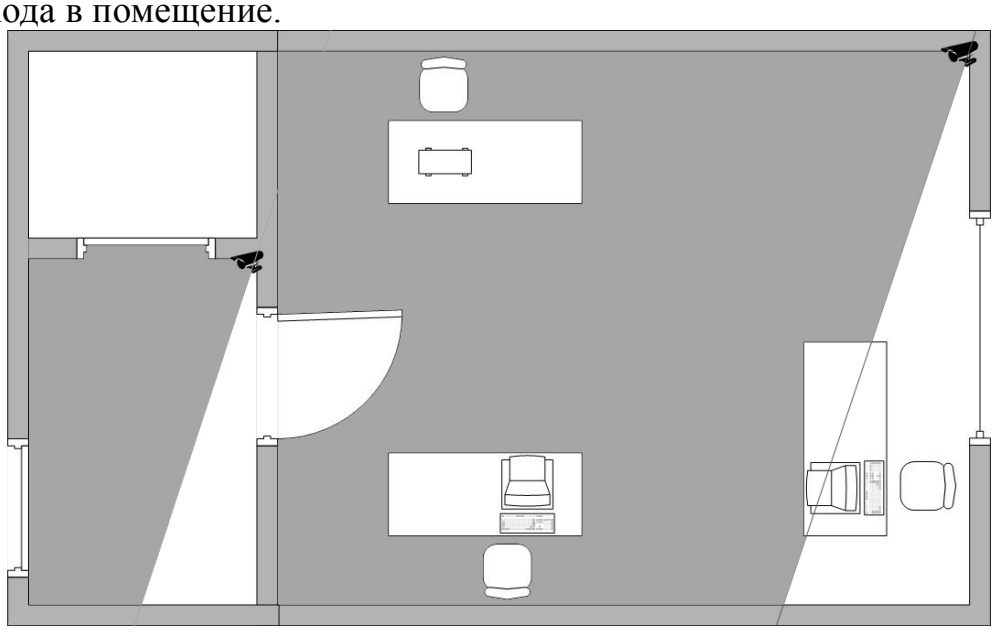

Рисунок 1 – Установка системы видеонаблюдения

Серые зоны показывают радиус обхвата изображения системами видеонаблюдения.

3.5. Риски реализации проекта

Одним из главных условий для внедрения проекта по созданию КСЗИ для предприятия «ИП Суский» является расчет рисков. Для расчета рисков используем формулу:

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

где величина Th означает уровень угрозы, который рассчитывается по следующей формуле:

$$Th = \frac{ER}{100} \times \frac{P(V)}{100}$$

где ER – критичность реализации угрозы (%);
P(V) – вероятность реализации угрозы (%).

Таблица 8 – Потоки защищаемой информации

Риски / пути их реализации	Критичность ER	Вероятность P(V)	Th	CTh
1	2	3	4	5
1. Риски изменений в стране, обществе				
1.1. Изменение политических и экономических характеристик и факторов				
– политические и экономические изменения	10	5	0,005	0,015
– изменение законодательства	20	5	0,01	
1.2. Влияние непредвиденных ситуаций				
– стихийные бедствия и природные катаклизмы	7	1	0,0007	0,0007
2. Риски окружения проекта в составе организации				
2.1. Изменение финансовой обстановки проекта				
– приостановка финансирования	90	10	0,09	0,827
– отсутствие денежного резерва для реагирование на события рисков (в т.ч. для ликвидации отставания от графика)	90	90	0,81	
2.2. Низкая организованность работ				
– отставание от графика работ, срыв сроков	20	10	0,02	0,116
– недостаток рабочей силы	40	20	0,08	
– преуменьшение стоимости работ и расход	40	5	0,02	

Продолжение Таблицы 8

1	2	3	4	5
финансовых средств для других задач				
2.3. Риски персонала				
– влияние личностных качеств сотрудников (переоценка собственных возможностей, преувеличение роли технологической стороны в ущерб менеджменту)	25	10	0,25	0,35
– риск отсутствия персонала, которому сложно подобрать замену (болезнь, увольнение и другие непредвиденные обстоятельства)	20	5	0,1	

На основе данной таблицы, показывающей численные значения уровня угрозы, можно увидеть, что максимальный риск связан с изменением финансовой обстановки проекта (0,827), а минимальный риск связан с влиянием непредвиденных обстоятельств.

3.6. Структура разбиения работ

Структура разбиения работ предоставляет возможность согласовать план проекта с потребностями заказчика, представленными в виде описаний работ. Структура разбиения работ представлена на рисунке 1. Описание процесса разбиения работ представлен в таблице 9.

Таблица 9 – Структура разбиения работ

Исполнитель/Работа	Описание работы
1	2
КСЗИ 1	Проектирование
КСЗИ 1.1	Определение важнейших показателей существующих бизнес-процессов с точки зрения информационной безопасности
КСЗИ 1.2	Анализ проблем существующих бизнес-процессов
КСЗИ 1.3	Разработка значений важнейших показателей новых бизнес-процессов
КСЗИ 1.4	Анализ и отбор наилучших способов и методов улучшения значений важнейших показателей бизнес-процессов
КСЗИ 1.5	Разработка и согласование структуры новых бизнес-процессов
КСЗИ 2	Разработка новой организационно-распорядительной документации
КСЗИ 2.1	Положение «О коммерческой тайне»
КСЗИ 2.2	Перечень сведений, составляющий коммерческую тайну
КСЗИ 2.3	Приказы об утверждении положения режима коммерческой тайны и перечня сведений, составляющих коммер-

Продолжение Таблицы 9

1	2
	ческую тайну
КСЗИ 2.4	Внесение изменений в должностные инструкции
КСЗИ 2.5	Согласование и утверждение ОРД
КСЗИ 3	Подготовка реализации проекта созданию КСЗИ
КСЗИ 3.1	Определение ответственных лиц и исполнителей проекта
КСЗИ 3.2	Приобретение программно-аппаратного средства защиты от НСД
КСЗИ 3.3	Приобретение средств видеонаблюдения
КСЗИ 4	Внедрение
КСЗИ 4.1	Установка и настройка программно-аппаратного средства защиты от НСД
КСЗИ 4.2	Установка средств видеонаблюдения
КСЗИ 4.3	Контроль защищенности
КСЗИ 4.4	Обучение персонала

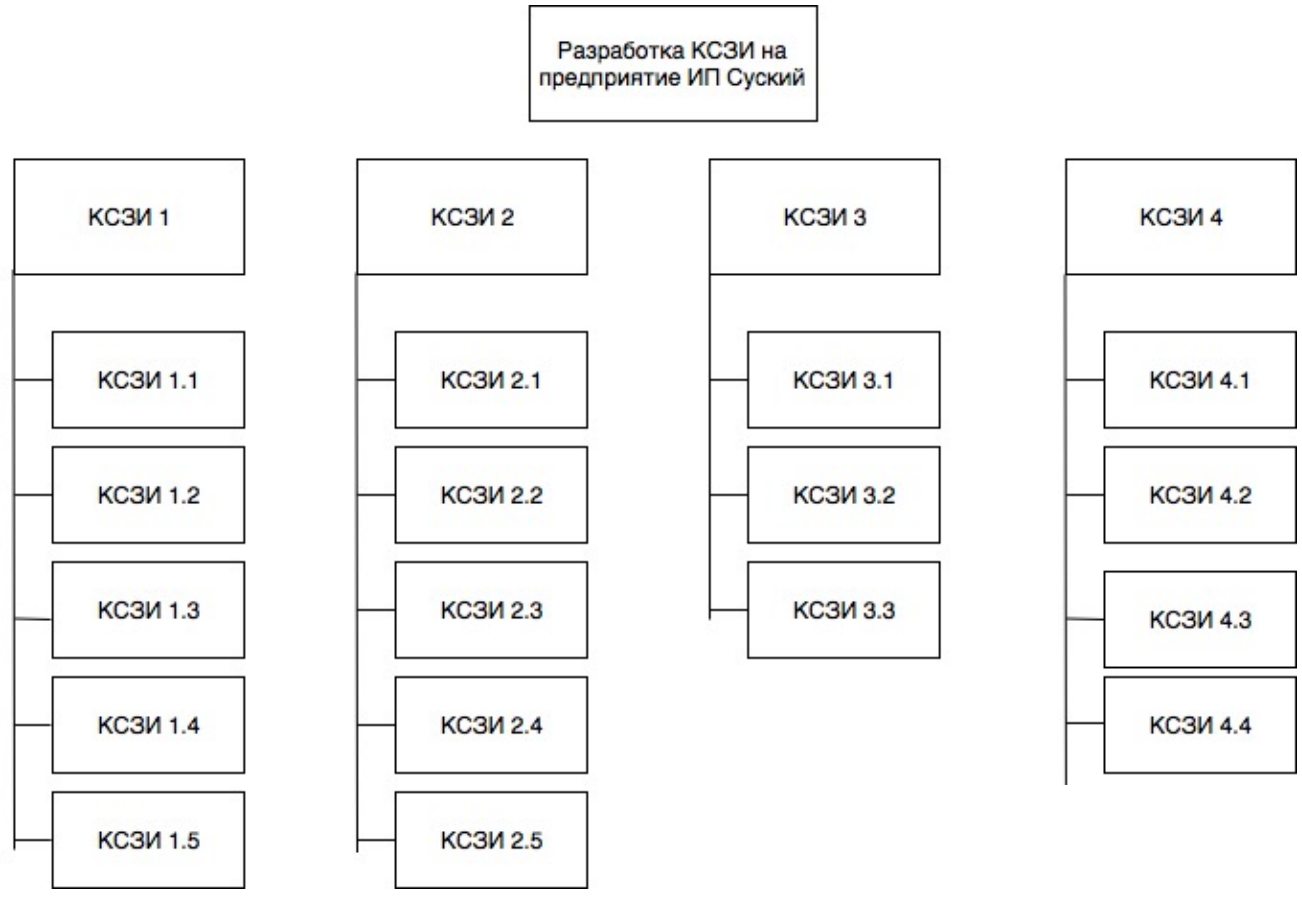

Рисунок 2 – Структурная схема разбиения работ

3.7. Структурная схема реализации проекта

Для более точного и своевременного выполнения проекта, требуется совместная работа всех задействованных сотрудников. Для этого была определенна структурная схема организации проекта. Структурная схема организации представлена на рисунке 2.

Рисунок 3 – Структурная схема организации проекта

3.8. Матрица ответственности

Все действия исполнителей по работам делятся на три условные группы:

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

Матрица ответственности представлена в таблице 10.

Таблица 10 – Структура разбиения работ

Исполнитель/Работа	1	2	3	4
КСЗИ 1	К			
КСЗИ 1.1	К/У		И	
КСЗИ 1.2	И		К	
КСЗИ 1.3	И		К	
КСЗИ 1.4	К/У		И	
КСЗИ 1.5	И		К	
КСЗИ 2	К	У/И		
КСЗИ 2.1	К	У/И		
КСЗИ 2.2	К	У/И		
КСЗИ 2.3	К	У/И		
КСЗИ 2.4	К	У/И		
КСЗИ 2.5	К	У/И		
КСЗИ 3	К			
КСЗИ 3.1	К		И	
КСЗИ 3.2	К			
КСЗИ 3.3	К			

Продолжение Таблицы 10

	1	2	3	4
КСЗИ 4	К			И
КСЗИ 4.1	И		К	
КСЗИ 4.2	К			И
КСЗИ 4.3	К	И		
КСЗИ 4.4	И	К	К	

3.9. Диаграмма Ганта и сетевой график

Диаграмма Ганта иллюстрирует план, график работ по выбранному проекту. Представляет собой столбчатые гистограммы.

Разработка диаграммы Ганта необходима для наглядного показа плана и графика работ данного проекта, а так же является одним из методов планирования проектов и используется в приложениях по управлению проектами. Для построения диаграммы Ганта необходимо определить перечень задач и сроки их выполнения. Результаты анализа в Таблице 11.

Таблица 11 – Перечень задач и сроков их выполнения

Работы	Название работы	Длительность	Начало	Окончание
1	2	3	4	5
1	Проектирование	13	02.04.2018	15.04.2018
1.1	Определение важнейших показателей существующих бизнес-процессов с точки зрения информационной безопасности	3	02.04.2018	05.04.2018
1.2	Анализ проблем существующих бизнес-процессов	2	05.04.2018	07.04.2018
1.3	Разработка значений важнейших показателей новых бизнес-процессов	2	07.04.2018	09.04.2018
1.4	Анализ и отбор наилучших способов и методов улучшения значений важнейших показателей бизнес-процессов	3	09.04.2018	12.04.2018
1.5	Разработка и согласование структуры новых бизнес-процессов	3	12.04.2018	15.04.2018
2	Разработка новой организационно-распорядительной документации	8	16.04.2018	24.04.2018

Продолжение Таблицы 11

1	2	3	4	5
2.1	Положение «О коммерческой тайне»	3	16.04.2018	19.04.2018
2.2	Перечень сведений, составляющий коммерческую тайну	2	19.04.2018	21.04.2018
2.3	Приказы об утверждении положения режима коммерческой тайны и перечня сведений, составляющих коммерческую тайну	1	21.04.2018	22.04.2018
2.4	Внесение изменений в должностные инструкции	2	22.04.2018	24.04.2018
2.5	Согласование и утверждение ОРД	1	24.04.2018	25.04.2018
3	Подготовка реализации проекта созданию КСЗИ	2	25.04.2018	26.04.2018
3.1	Определение ответственных лиц и исполнителей проекта	1	25.04.2018	26.04.2018
3.2	Приобретение программно-аппаратного средства защиты от НСД	1	25.04.2018	26.04.2018
3.3	Приобретение средств видеонаблюдения	1	25.04.2018	26.04.2018
4	Внедрение	3	26.04.2018	29.05.2018
4.1	Установка и настройка программно-аппаратного средства защиты от НСД	1	26.04.2018	27.04.2018
4.2	Установка средств видеонаблюдения	1	27.04.2018	28.04.2018
4.3	Контроль защищенности	1	29.04.2018	29.04.2018
4.4	Обучение персонала	1	29.04.2018	29.04.2018
Проект по созданию КСЗИ		26	02.04.2018	29.04.2018

На основе данных из таблицы 11 построим диаграмму Ганта для проекта разработки КСЗИ на предприятии «ИП Суский» (Приложение М).

Сетевой график – это динамическая модель производственного процесса, отражающий технологическую зависимость и последовательность выполнения комплекса работ с их выполнением по временному интервалу. Для определения соот-

ветствия плану работ определим необходимые сроки выполнения работ. Сетевой график представлен в Таблице 12.

Т – длительность работы, дней;

$Т_{рн}$ – ранний срок начала работы;

$Т_{пн}$ – поздний срок начала работы;

$Т_{ро}$ – ранний срок окончания работы;

$Т_{по}$ – поздний срок окончания работы.

Таблица 12 – Расписание выполнения работ

Работа	Название работы	Т	$Т_{рн}$	$Т_{пн}$	$Т_{ро}$	$Т_{по}$
1	2	3	4	5	6	7
1	Проектирование	13	02.04. 2018	02.04. 2018	15.04. 2018	20.04. 2018
1.1	Определение важнейших показателей существующих бизнес-процессов с точки зрения информационной безопасности	3	02.04. 2018	02.04. 2018	04.04. 2018	06.04. 2018
1.2	Анализ проблем существующих бизнес-процессов	2	05.04. 2018	06.04. 2018	06.04. 2018	09.04. 2018
1.3	Разработка значений важнейших показателей новых бизнес-процессов	2	06.04. 2018	09.04. 2018	08.04. 2018	12.04. 2018
1.4	Анализ и отбор наилучших способов и методов улучшения значений важнейших показателей бизнес-процессов	3	08.04. 2018	12.04. 2018	11.04. 2018	16.04. 2018
1.5	Разработка и согласование структуры новых бизнес-процессов	3	11.04. 2018	16.04. 2018	14.04. 2018	20.04. 2018
2	Разработка новой организационно-распорядительной документации	8	14.04. 2018	20.04. 2018	23.04. 2018	29.04. 2018
2.1	Положение «О коммерческой тайне»	3	14.04. 2018	20.04. 2018	16.04. 2018	24.04. 2018
2.2	Перечень сведений, составляющий коммерческую тайну	2	16.04. 2018	24.04. 2018	18.04. 2018	26.04. 2018
2.3	Приказы об утверждении положения режима коммерческой тайны и перечня сведений, составляющих коммерческую тайну	1	18.04. 2018	26.04. 2018	19.04. 2018	27.04. 2018
2.4	Внесение изменений в должностные инструкции	2	19.04. 2018	27.04. 2018	21.04. 2018	29.04. 2018

Продолжение Таблицы 12

1	2	3	4	5	6	7
2.5	Согласование и утверждение ОРД	1	21.04. 2018	29.04. 2018	22.04. 2018	30.04. 2018
3	Подготовка реализации проекта созданию КСЗИ	2	22.04. 2018	30.04. 2018	24.04. 2018	02.05. 2018
3.1	Определение ответственных лиц и исполнителей проекта	1	24.04. 2018	02.05. 2018	25.04. 2018	03.05. 2018
3.2	Приобретение программно-аппаратного средства защиты от НСД	1	25.04. 2018	03.05. 2018	26.04. 2018	04.05. 2018
3.3	Приобретение средств видеонаблюдения	1	25.04. 2018	03.05. 2018	26.04. 2018	04.05. 2018
4	Внедрение	3	26.04. 2018	04.05. 2018	29.04. 2018	07.05. 2018
4.1	Установка и настройка программно-аппаратного средства защиты от НСД	1	26.04. 2018	04.05. 2018	27.04. 2018	08.05. 2018
4.2	Установка средств видеонаблюдения	1	27.04. 2018	08.05. 2018	28.04. 2018	09.05. 2018
4.3	Контроль защищенности	1	28.04. 2018	09.05. 2018	29.04. 2018	10.05. 2018
4.4	Обучение персонала	1	28.04. 2018	09.05. 2018	29.04. 2018	10.05. 2018

Основываясь на диаграмму Ганта и сетевой график, мы можем определить точные сроки выполнения данного проекта.

3.10. Оценка экономической эффективности проекта

В результате предпроектного обследования, были выявлены уязвимости, подлежащие устранению. Эти уязвимости можно устранить с помощью создания комплексной системы защиты информации. Для этого необходимо произвести расчет эффективности проекта, отвечающий на вопрос о целесообразности реали-

зации мер по созданию комплексной системы защиты информации. Стоимость программных и технических средств представлена в таблице 13. Стоимость услуг по реализации проекта представлена в таблице 14. Поток денежных платежей представлен в таблице 15.

Таблица 13 – Стоимость обеспечения

№ п/п	Наименование	Количество	Цена за шт. (руб.)	Сумма (руб.)
1	СЗИ НСД «Secret Net Studio»	3	7500	22500
2	Комплект видеонаблюдения FALCON EYE FE-104MHD KIT Light	1	7250	7250
Итог				29750

Таблица 14 – Стоимость услуг по обеспечению проекта

№ п/п	Наименование	Стоимость
1	Разработка и описание бизнес-процессов компании с точки зрения ИБ	10000
2	Разработка организационно-распорядительной документации	7400
3	Установка и настройка СЗИ от НСД «Secret Net»	6000
4	Установка и настройка комплекта видеонаблюдения FALCON EYE FE-104MHD KIT Light	5000
6	Обучение пользователей	2000
Итог		30400

Стоимость внедрения КСЗИ в «ИП Суский» составляет 60150 рублей.

Таблица 15 – Поток денежных платежей по проекту

Периоды	0	1	2	3
Первоначальные инвестиции (руб.)	-60150			
Выгоды (размеры риска) (руб.)		200000	200000	200000
Стоимость годовой поддержки (руб.)		-3500	-3500	-3500
Затраты на администрирование и инфраструктуру		-10000	-10000	-10000
Итого	-60150	186500	186500	186500

Денежные вложения в реализацию проекта комплексной системы защиты информации составляют 60150 рублей. Для поддержания системы ежегодно требуется выделять по 3500 рублей, на протяжении трех лет.

Для показа отличия вложений средств в проект от дохода хранения денег в банке используем метод Net Present Value (NPV). Рассчитаем NPV по формуле:

$$NPV = \sum_{t=1}^{n} \frac{CF_t}{(1+r)^t} - \sum_{t=0}^{n} \frac{I_t}{(1+r)^t}$$

где CF – денежный поток;

I – сумма инвестиционных вложений в проект в t-ом периоде;

r – ставка дисконтирования;

n – количество периодов.

Значение финансовых поступлений будем считать равным размеру ставки Центробанка России. Ставка центрального банка составляет 7,25%

NPV = -60150 + 186500/1,0725 + 186500/$(1,0725)^2$ + 186500/$(1,0725)^3$ =
= - 60150 + 173893 + 162138 + 151177 = 427058

После расчета видно, что значение NPV больше 0, а значит на данном предприятие целесообразен проект внедрения КСЗИ. Создание КСЗИ на предприятие будет эффективным, так как величина потерь при отсутствие реализованных мер будет превышать затраты на ее реализацию и обслуживание.

3.11. Вывод

Итогом выполненных работ является проект по созданию комплексной системы защиты информации на предприятие «ИП Суский». Были определены цели и задачи проекта, потоки защищаемой информации. Все выполняемые работы были разделены и структурированы. Были представлены структурные схемы разбиения работ и реализации проекта. Также были разработаны графики, наглядно показывающие сроки и объемы выполнения работ.

В результате расчета стоимости создания КСЗИ в «ИП Суский» и ее обслуживания, была произведена оценка эффективности. По данным оценки суммарные затраты на реализацию проекта составляют 60150 рублей, а проект займет 26 дней. Проект признан эффективным с точки зрения экономической целесообразности, об этом говорят расчеты по методу Net Present Value. Данный проект позволит получить дополнительную выгоду, ликвидируя угрозы.

4. БЕЗОПАСОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ

4.1. Введение

Безопасность жизнедеятельности – это совокупность многих правил и норм, созданных для обеспечения защиты жизни и сохранения здоровья человека. При приеме на работу будущий сотрудник обязательно должен пройти инструктаж по технике безопасности. Руководители предприятий и их подразделений осуществляют четкий контроль над своевременными инструктажами. Обязательно ведут журнал, где ставят подписи все работники, которые прошли инструктаж.

Требования санитарных правил направлены на предотвращение неблагоприятного влияния на здоровье человека вредных факторов производственной среды и трудового процесса при работе с ПЭВМ.

4.2. Рекомендации по организации рабочего места пользователя

4.2.1. Общие требования к организации рабочих мест пользователей

Рабочее место оператора ЭВМ проектируется согласно СанПиН 2.2.2/2.4.1340-03 «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы».

1. При размещении рабочих мест с ПЭВМ расстояние между рабочими столами с видеомониторами (в направлении тыла поверхности одного видеомонитора и экрана другого видеомонитора), должно быть не менее 2,0 м, а расстояние между боковыми поверхностями видеомониторов – не менее 1,2 м.

2. Рабочие места с ПЭВМ при выполнении творческой работы, требующей значительного умственного напряжения или высокой концентрации внимания, рекомендуется изолировать друг от друга перегородками высотой 1,5 – 2,0 м.

3. Экран видеомонитора должен находиться от глаз пользователя на расстоянии 600 – 700 мм, но не ближе 500 мм с учетом размеров алфавитно-цифровых знаков и символов.

4. Конструкция рабочего стола должна обеспечивать оптимальное размещение на рабочей поверхности используемого оборудования с учетом его количества и конструктивных особенностей, характера выполняемой работы. При этом допускается использование рабочих столов различных конструкций, отвечающих современным требованиям эргономики. Поверхность рабочего стола должна иметь коэффициент отражения 0,5 – 0,7.

5. Конструкция рабочего стула (кресла) должна обеспечивать поддержание рациональной рабочей позы при работе на ПЭВМ, позволять изменять позу с целью снижения статического напряжения мышц шейно-плечевой области и спины для предупреждения развития утомления. Тип рабочего стула (кресла) следует выбирать с учетом роста пользователя, характера и продолжительности работы с ПЭВМ. Рабочий стул (кресло) должен быть подъемно-поворотным, регулируемым по высоте и углам наклона сиденья и спинки, а также расстоянию спинки от

переднего края сиденья, при этом регулировка каждого параметра должна быть независимой, легко осуществляемой и иметь надежную фиксацию.

6. Поверхность сиденья, спинки и других элементов стула (кресла) должна быть полумягкой, с нескользящим, слабо электризующимся и воздухопроницаемым покрытием, обеспечивающим легкую очистку от загрязнений.

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

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

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

10. Конструкция рабочего стула должна обеспечивать:

- Ширину и глубину поверхности сиденья не менее 400 мм.
- Поверхность сиденья с закругленным передним краем.
- Регулировку высоты поверхности сиденья в пределах 400 – 550 мм и углам наклона вперед до 15 град, и назад до 5 град..
- Высоту опорной поверхности спинки 300 +-20 мм, ширину – не менее 380 мм и радиус кривизны горизонтальной плоскости – 400 мм.
- Угол наклона спинки в вертикальной плоскости в пределах +-30 градусов.
- Регулировку расстояния спинки от переднего края сиденья в пределах 260 – 400 мм.
- Стационарные или съемные подлокотники длиной не менее 250 мм и шириной – 50 – 70 мм.
- регулировку подлокотников по высоте над сиденьем в пределах 230 +-30 мм и внутреннего расстояния между подлокотниками в пределах 350 -500 мм;

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

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

4.2.2. Требования к помещениям для размещения рабочего места

При работе с вычислительной техникой важным фактором, обеспечивающим высокий уровень работоспособности, является правильно спроектированное помещение в котором будут располагаться рабочие места, оборудование ЭВМ с ВДТ.

По требованиям СанПиН 2.2.2/2.4.1340-03 помещения для эксплуатации ПЭВМ должны отвечать следующим требованиям:

1. Помещения для эксплуатации ПЭВМ должны иметь естественное и искусственное освещение.

2. Естественное и искусственное освещение должно соответствовать требованиям действующей нормативной документации. Оконные проемы должны быть оборудованы регулируемыми устройствами типа: жалюзи, занавесей, внешних козырьков и др..

3. Площадь на одно рабочее место пользователей ПЭВМ с ВДТ на базе плоских дискретных экранов (жидкокристаллические, плазменные), должна составлять не менее 4,5 м^2.

4. Для внутренней отделки интерьера помещений, где расположены ПЭВМ, должны использоваться диффузно-отражающие материалы с коэффициентом отражения для потолка – 0,7 – 0,8; для стен – 0,5 – 0,6; для пола – 0,3 – 0,5;

5. Помещения, где размещаются рабочие места с ПЭВМ, должны быть оборудованы защитным заземлением (занулением) в соответствии с техническими требованиями по эксплуатации.

6. Не следует размещать рабочие места с ПЭВМ вблизи силовых кабелей и вводов, высоковольтных трансформаторов, технологического оборудования, создающего помехи в работе ПЭВМ.

4.2.3. Требования к уровням шума на рабочих местах

Уровень шума на рабочих местах, при выполнении основных и вспомогательных производственных работ с использованием ПЭВМ не должен превышать показателей, устанавливаемых нормами СанПиН 2.2.2/2.4.1340-03 предельно допустимых значений для данных видов работ в соответствии с действующими санитарно-эпидемиологическими нормативами. А именно должен соответствовать нормам СанПиН 2.2.4.3359-16 для высококвалифицированной работы, требующей сосредоточенности, в рабочих комнатах. Источниками шума в данной организации являются рабочие станции и сервер. На основании СанПиН 2.2.4.3359-16, нормативным эквивалентным уровнем звука на рабочих местах является 80 Дба. В соответствии с нормами, ограничивающими предельно допустимое звуковое давление для рабочих мест, оснащенных ПЭВМ: шумящее оборудование, уровни шума которого превышают нормативные, должно размещаться вне помещений ПЭВМ.

4.2.4. Требования к освещению на рабочих местах

При работе с вычислительной техникой важным фактором, обеспечивающим высокий уровень работоспособности, является правильно спроектированное освещение, не вызывающее раннего переутомления.

Согласно СанПиН 2.2.2/2.4.1340-03, есть следующие требования к освещению на рабочих местах:

1. Рабочие столы следует размещать таким образом, чтобы видеодисплейные терминалы были ориентированы боковой стороной к световым проемам, чтобы естественный свет падал преимущественно слева.

2. Искусственное освещение в помещениях для эксплуатации ПЭВМ должно осуществляться системой общего равномерного освещения. В производственных и административно-общественных помещениях, в случаях преимущественной работы с документами, следует применять системы комбинированного освещения.

3. Освещенность на поверхности стола в зоне размещения рабочего документа должна быть 300 – 500 лк. Освещение не должно создавать бликов на поверхности экрана. Освещенность поверхности экрана не должна быть более 300 лк.

4. Следует ограничивать прямую блесткость от источников освещения, при этом яркость светящихся поверхностей (окна, светильники и др.), находящихся в поле зрения, должна быть не более 200 кд/м.

5. Яркость светильников общего освещения в зоне углов излучения от 50 до 90° с вертикалью в продольной и поперечной плоскостях должна составлять не более 200 кд/м , защитный угол светильников должен быть не менее 40°.

6. Общее освещение при использовании люминесцентных светильников следует выполнять в виде сплошных или прерывистых линий светильников, расположенных сбоку от рабочих мест, параллельно линии зрения пользователя при рядном расположении видеодисплейных терминалов. При периметральном расположении компьютеров линии светильников должны располагаться локализовано над рабочим столом ближе к его переднему краю, обращенному к оператору;

7. Коэффициент пульсации не должен превышать 5%.

8. Для обеспечения нормируемых значений освещенности в помещениях для использования ПЭВМ следует проводить чистку стекол оконных рам и светильников не реже двух раз в год и проводить своевременную замену перегоревших ламп.

4.2.5. Требования к микроклимату

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

Нормативные требования к показателям микроклимата рабочих мест производственных помещений приведены в СанПиН 2.2.4.3359-16 «Санитарно-эпидемиологические требования к физическим факторам на рабочих местах» .
Оптимальные величины параметров микроклимата для категории работ 1а приведены в таблице 16.

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

Таблица 16 – Оптимальные величины параметров микроклимата

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

4.2.6. Требования к электробезопасности

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

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

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

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

1. Обеспечение недоступности токоведущих частей, находящихся под напряжением для случайного прикосновения.

2. Устранение опасности поражения при появлении напряжения на нетоковедущих частях электрооборудования посредством заземления (зануления).

4.3. Пожарная безопасность

Постановление Правительства РФ от 25.04.2012 N 390 (ред. От 21.03.2017) «О противопожарном режиме» устанавливают следующие правила:

1. В отношении каждого объекта (за исключением индивидуальных жилых домов) руководителем (иным уполномоченным должностным лицом) организации (индивидуальным предпринимателем), в пользовании которой на праве собственности или на ином законном основании находятся объекты (далее – руководитель организации), утверждается инструкция о мерах пожарной безопасности в соответствии с требованиями.

2. Лица допускаются к работе на объекте только после прохождения обучения мерам пожарной безопасности;

3. Лица допускаются к работе на объекте только после прохождения обучения мерам пожарной безопасности.

4. Обучение лиц мерам пожарной безопасности осуществляется путем проведения противопожарного инструктажа и прохождения пожарно-технического минимума.

5. Порядок и сроки проведения противопожарного инструктажа и прохождения пожарно-технического минимума определяются руководителем организации. Обучение мерам пожарной безопасности осуществляется в соответствии с нормативными документами по пожарной безопасности.

6. Руководитель организации назначает лицо, ответственное за пожарную безопасность, которое обеспечивает соблюдение требований пожарной безопасности на объекте.

7. В складских, производственных, административных и общественных помещениях, местах открытого хранения веществ и материалов, а также размещения технологических установок руководитель организации обеспечивает наличие табличек с номером телефона для вызова пожарной охраны.

8. На объекте с массовым пребыванием людей (кроме жилых домов), а также на объекте с рабочими местами на этаже для 10 и более человек руководитель организации обеспечивает наличие планов эвакуации людей при пожаре.

9. На объекте с массовым пребыванием людей руководитель организации обеспечивает наличие инструкции о действиях персонала по эвакуации людей при пожаре, а также проведение не реже 1 раза в полугодие практических тренировок лиц, осуществляющих свою деятельность на объекте.

10. Хранение огнетушителя осуществляется в соответствии с требованиями инструкции по его эксплуатации.

11. Запрещается на территориях, прилегающих к объектам, в том числе к жилым домам, а также к объектам садоводческих, огороднических и дачных некоммерческих объединений граждан, оставлять емкости с легковоспламеняющимися и горючими жидкостями, горючими газами.

12. Руководитель организации обеспечивает наличие на дверях помещений производственного и складского назначения и наружных установках обозначение их категорий по взрывопожарной и пожарной опасности.

13. Руководитель организации обеспечивает устранение повреждений толстослойных напыляемых составов, огнезащитных обмазок, штукатурки, облицовки плитными, листовыми и другими огнезащитными материалами, в том числе на каркасе, комбинации этих материалов, в том числе с тонкослойными вспучивающимися покрытиями строительных конструкций, горючих отделочных и теплоизоляционных материалов, воздуховодов, металлических опор оборудования и эстакад, а также осуществляет проверку состояния огнезащитной обработки (пропитки) в соответствии с инструкцией завода-изготовителя с составлением протокола проверки состояния огнезащитной обработки (пропитки). Проверка состояния огнезащитной обработки (пропитки) при отсутствии в инструкции сроков периодичности проводится не реже 1 раза в год.

14. Руководитель организации организует проведение работ по заделке негорючими материалами, обеспечивающими требуемый предел огнестойкости и дымогазонепроницаемость, образовавшихся отверстий и зазоров в местах пересечения противопожарных преград различными инженерными (в том числе электрическими проводами, кабелями) и технологическими коммуникациями.

15. На объектах запрещается:

– Хранить и применять на чердаках, в подвалах и цокольных этажах легковоспламеняющиеся и горючие жидкости, порох, взрывчатые вещества, пиротехнические изделия, баллоны с горючими газами, товары в аэрозольной упаковке, целлулоид и другие пожаровзрывоопасные вещества и материалы, кроме случаев, предусмотренных иными нормативными документами по пожарной безопасности.

– Использовать чердаки, технические этажи, вентиляционные камеры и другие технические помещения для организации производственных участков, мастерских, а также для хранения продукции, оборудования, мебели и других предметов.

– Размещать в лифтовых холлах кладовые, киоски, ларьки и другие подобные помещения.

– Устраивать в подвалах и цокольных этажах мастерские, а также размещать иные хозяйственные помещения, размещение которых не допускается нормативными документами по пожарной безопасности, если нет самостоятельного выхода или выход из них не изолирован противопожарными преградами от общих лестничных клеток.

– Снимать предусмотренные проектной документацией двери эвакуационных выходов из поэтажных коридоров, холлов, фойе, тамбуров и лестничных клеток, другие двери, препятствующие распространению опасных факторов пожара на путях эвакуации.

– Производить изменение объемно-планировочных решений и размещение инженерных коммуникаций и оборудования, в результате которых ограничивается доступ к огнетушителям, пожарным кранам и другим системам обеспечения пожарной безопасности или уменьшается зона действия автоматических систем противопожарной защиты (автоматической пожарной сигнализации, стационарной автоматической установки пожаротушения, системы дымоудаления, системы оповещения и управления эвакуацией).

– Загромождать мебелью, оборудованием и другими предметами двери, люки на балконах и лоджиях, переходы в смежные секции и выходы на наружные эвакуационные лестницы, демонтировать межбалконные лестницы, заваривать и загромождать люки на балконах и лоджиях квартир.

– Проводить уборку помещений и стирку одежды с применением бензина, керосина и других легковоспламеняющихся и горючих жидкостей, а также производить отогревание замерзших труб паяльными лампами и другими способами с применением открытого огня.

– Остеклять балконы, лоджии и галереи, ведущие к незадымляемым лестничным клеткам.

– Устраивать в лестничных клетках и поэтажных коридорах кладовые и другие подсобные помещения, а также хранить под лестничными маршами и на лестничных площадках вещи, мебель и другие горючие материалы.

– Устраивать в производственных и складских помещениях зданий (кроме зданий V степени огнестойкости) антресоли, конторки и другие встроенные помещения из горючих материалов и листового металла.

– Устанавливать в лестничных клетках внешние блоки кондиционеров.

– Загромождать и закрывать проходы к местам крепления спасательных устройств.

16. Руководитель организации обеспечивает содержание наружных пожарных лестниц и ограждений на крышах (покрытиях) зданий и сооружений в исправном состоянии, организует не реже 1 раза в 5 лет проведение эксплуатационных испытаний пожарных лестниц и ограждений на крышах с составлением соответствующего протокола испытаний, а также периодического освидетельствования состояния средств спасения с высоты в соответствии с технической документацией или паспортом на такое изделие.

17. Приямки у оконных проемов подвальных и цокольных этажей зданий (сооружений) должны быть очищены от мусора и посторонних предметов.

18. Руководитель организации обеспечивает сбор использованных обтирочных материалов в контейнеры из негорючего материала с закрывающейся крышкой и удаление по окончании рабочей смены содержимого указанных контейнеров.

19. В зданиях с витражами высотой более одного этажа не допускается нарушение конструкций дымонепроницаемых негорючих диафрагм, установленных в витражах на уровне каждого этажа.

20. Руководителем организации, на объекте которой возник пожар, обеспечивается доступ пожарным подразделениям в закрытые помещения для целей локализации и тушения пожара.

21. Руководитель организации при расстановке в помещениях технологического, выставочного и другого оборудования обеспечивает наличие проходов к путям эвакуации и эвакуационным выходам.

22. Запрещается оставлять по окончании рабочего времени не обесточенными электроустановки и бытовые электроприборы в помещениях, в которых отсутствует дежурный персонал, за исключением дежурного освещения, систем

противопожарной защиты, а также других электроустановок и электротехнических приборов, если это обусловлено их функциональным назначением и (или) предусмотрено требованиями инструкции по эксплуатации.

23. Запрещается:

– эксплуатировать электропровода и кабели с видимыми нарушениями изоляции;

– пользоваться розетками, рубильниками, другими электроустановочными изделиями с повреждениями;

– обертывать электролампы и светильники бумагой, тканью и другими горючими материалами, а также эксплуатировать светильники со снятыми колпаками (рассеивателями), предусмотренными конструкцией светильника;

– пользоваться электроутюгами, электроплитками, электрочайниками и другими электронагревательными приборами, не имеющими устройств тепловой защиты, а также при отсутствии или неисправности терморегуляторов, предусмотренных конструкцией;

– применять нестандартные (самодельные) электронагревательные приборы;

– оставлять без присмотра включенными в электрическую сеть электронагревательные приборы, а также другие бытовые электроприборы, в том числе находящиеся в режиме ожидания, за исключением электроприборов, которые могут и (или) должны находиться в круглосуточном режиме работы в соответствии с инструкцией завода-изготовителя;

– размещать (складировать) в электрощитовых (у электрощитов), у электродвигателей и пусковой аппаратуры горючие (в том числе легковоспламеняющиеся) вещества и материалы;

– при проведении аварийных и других строительно-монтажных и реставрационных работ использовать временную электропроводку, включая удлинители, сетевые фильтры, не предназначенные по своим характеристикам для питания применяемых электроприборов.

24. Руководитель организации обеспечивает исправное состояние знаков пожарной безопасности, в том числе обозначающих пути эвакуации и эвакуационные выходы.

25. Запрещается пользоваться неисправными газовыми приборами, а также устанавливать (размещать) мебель и другие горючие предметы и материалы на расстоянии менее 0,2 метра от бытовых газовых приборов по горизонтали и менее 0,7 метра – по вертикали (при нависании указанных предметов и материалов над бытовыми газовыми приборами).

26. В соответствии с инструкцией завода-изготовителя руководитель организации обеспечивает проверку огнезадерживающих устройств (заслонок, шиберов, клапанов и др.) в воздуховодах, устройств блокировки вентиляционных систем с автоматическими установками пожарной сигнализации или пожаротушения, автоматических устройств отключения вентиляции при пожаре.

27. При эксплуатации систем вентиляции и кондиционирования воздуха запрещается:

– оставлять двери вентиляционных камер открытыми;

– закрывать вытяжные каналы, отверстия и решетки;

– подключать к воздуховодам газовые отопительные приборы

– выжигать скопившиеся в воздуховодах жировые отложения, пыль и другие горючие вещества;

28. Руководитель организации определяет порядок и сроки проведения работ по очистке вентиляционных камер, циклонов, фильтров и воздуховодов от горючих отходов с составлением соответствующего акта, при этом такие работы проводятся не реже 1 раза в год.

29. Руководитель организации обеспечивает укомплектованность пожарных кранов внутреннего противопожарного водопровода пожарными рукавами, ручными пожарными стволами и вентилями, организует перекатку пожарных рукавов (не реже 1 раза в год).

30. Руководитель организации обеспечивает исправное состояние систем и средств противопожарной защиты объекта (автоматических (автономных) установок пожаротушения, автоматических установок пожарной сигнализации , установок систем противодымной защиты, системы оповещения людей о пожаре, средств пожарной сигнализации, противопожарных дверей, противопожарных и дымовых клапанов, защитных устройств в противопожарных преградах) и организует не реже 1 раза в квартал проведение проверки работоспособности указанных систем и средств противопожарной защиты объекта с оформлением соответствующего акта проверки.

31. Выбор типа и расчет необходимого количества огнетушителей следует производить в зависимости от огнетушащей способности, предельной площади, класса пожара горючих веществ и материалов защищаемом помещении или на объекте согласно СП 9.13130.2009.

Для помещений телерадиокомпании актуальны следующие классы пожаров:

Класс А – пожары твердых веществ, основном органического происхождения, горение которых сопровождается тлением (древесина, текстиль, бумага).

Класс Е – пожары, связанные с горением электроустановок.

Для данных классов пожаров, исходя из рекомендации СП 9.13130.2009, следует применять порошковые огнетушители.

Огнетушители следует располагать на защищаемом объекте в соответствии с требованиями ГОСТ 12.4.009 таким образом, чтобы они были защищены от воздействия прямых солнечных лучей, тепловых потоков, механических воздействий и других неблагоприятных факторов (вибрация, агрессивная среда, повышенная влажность и т.д.). Они должны быть хорошо видны и легкодоступны в случае пожара. Предпочтительно размещать огнетушители вблизи мест наиболее вероятного возникновения пожара, вдоль путей прохода, а также около выхода из помещения. Огнетушители не должны препятствовать эвакуации людей во время пожара. Огнетушители, введенные в эксплуатацию, должны подвергаться техническому обслуживанию, которое обеспечивает поддержание огнетушителей в постоянной готовности к использованию и надежную работу всех узлов огнетушителя в течение всего срока эксплуатации. Техническое обслуживание включает в себя периодические проверки, осмотры, ремонт, испытания и перезарядку огнетушителей.

4.4. Сравнение параметров рабочего места с допустимыми нормами

Для того чтобы определить соответствие условий труда требованиям нормативных документов необходимо провести сравнительный анализ требований, установленных к рабочим местам, оборудованным ПЭВМ и фактических параметров рабочего места. Схема размещения рабочего места приведена на Рисунке 4. Площадь помещения 20м^2, оконный проем, шириной 1,7м размещается справа. В помещении присутствует естественное и искусственное освещение.

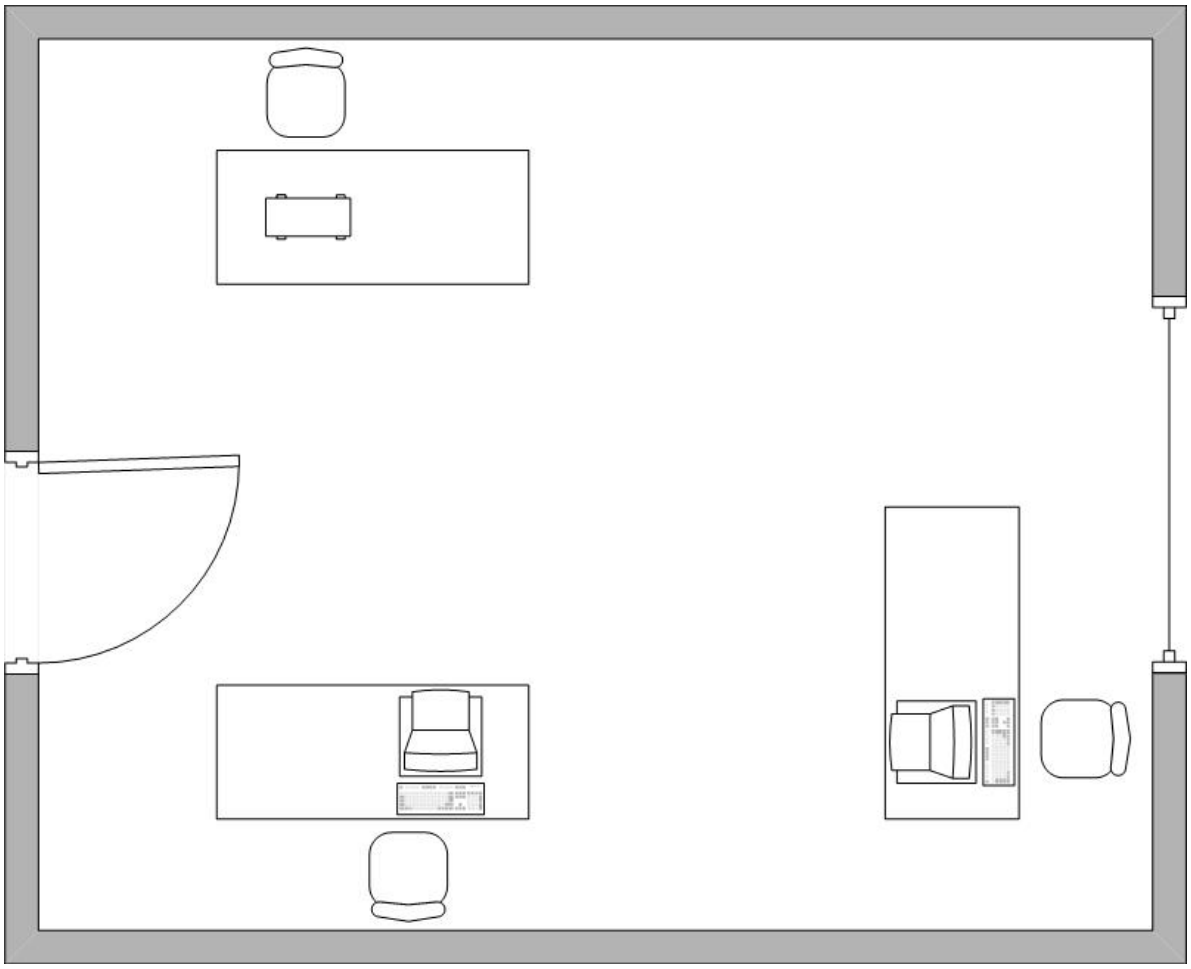

Рисунок 4 – Схема рабочего места.

Перечень нормируемых параметров для рабочего места, сравнение их допустимых нормы и фактические значений на рабочем месте представлены в Таблице 17.

Таблица 17 – Сравнение параметров рабочего места с допустимыми нормами.

Нормируемые параметры	Допустимые нормы	Фактические значения
1	2	3
Высота рабочей поверхности стола	от 680 до 800мм, либо 725мм	725мм

Продолжение Таблицы 17

1	2	3
Модульные размеры рабочей поверхности стола	Ширина 800, 1000, 1200, 1400мм, глубина 800 и 1000мм	
Ширина и глубина поверхности сиденья	Не менее 400мм	
Площадь на одно рабочее место	не менее 4,5м2	Ширина 1400мм глубина 600 мм
Падение естественного света	Преимущественно слева	Ширина 500мм Глубина 450мм
Освещенность поверхности стола	300-500 лк	6м2
Подставка для ног	Ширина не менее 300мм, глубина не менее 400мм, регулировка по высоте не менее 150мм, поверхность рифленая, спереди бортик	Справа
Размеры рабочего стула	Конструкция рабочего стула должна обеспечивать: - ширину и глубину поверхности сиденья не менее 400 мм; - поверхность сиденья с закругленным передним краем; - регулировку высоты поверхности сиденья в пределах 400 – 550 мм и углам наклона вперед до 15 град, и назад до 5 град.; - высоту опорной поверхности спинки 300 20 мм, ширину – не менее 380 мм и радиус кривизны горизонтальной плоскости – 400 мм; - угол наклона спинки в вертикальной плоскости в пределах	400 лк

Продолжение Таблицы 17

1	2	3
	30 градусов; - регулировку расстояния спинки от переднего края сиденья в пределах 260 – 400 мм; - стационарные или съемные подлокотники длиной не менее 250 мм и шириной – 50 – 70 мм; - регулировку подлокотников по высоте над сиденьем в пределах 230 30 мм и внутреннего расстояния между подлокотниками в пределах 350 – 500 мм.	
Уровень звука	80 Дба	51 Дба
Параметры микроклимата (кат. 1а)	Температура воздуха 22-24° С Влажность воздуха 40-60%	Температура 22° С Влажность воздуха 55%

4.5. Вывод

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

ЗАКЛЮЧЕНИЕ

В результате выполнения выпускной квалификационной работы был проведен анализ состояния защиты информации на предприятии «ИП Суский».

В результате этого были выявлены угрозы, которые требуют устранения. На основании этого был разработан проект КСЗИ «ИП Суский». Данный проект, включает в себя мероприятия, с помощью которых возможно устранение угроз и уязвимостей на данном предприятии.

В ходе ВКР было проведено предпроектное обследование, включающее в себя:

- разработку паспорта предприятия с точки зрения обеспечения информационной безопасности – были проанализированы организационно-правовая форма и организационная структура, виды деятельности, предполагаемые виды защищаемой информации, поставщики, клиенты и конкуренты, информационная среда предприятия, строительная инфраструктура зданий и сооружений и местоположение предприятия;
- разработку модели деятельности предприятия – были выявлены базовые бизнес-процессы, а также определенны информационные потоки и информация, подлежащая защите;
- описание информационной системы предприятия – были выявлены характеристики АРМ, ПО установленное на них;
- выявление объектов защиты – были выявлены объекты защиты, обрабатывающие и циркулирующие информацию ограниченного доступа;
- были выявлены угрозы и уязвимости, с помощью которых могла быть разглашена информация, нуждающаяся в защите. Поэтому были разработаны мероприятия, которые затрудняют или полностью исключают реализацию угроз через эти уязвимости.

Так же была рассчитана экономическая целесообразность внедрения данного проекта, которая показала, что создание КСЗИ на предприятие «ИП Суский» экономически целесообразно.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (Выписка) (утв. ФСТЭК РФ 15.02.2008) // КонсультантПлюс [Электронный ресурс]. – http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=99662&fld=134&dst=1000000001,0&rnd=0.8630855495122507#0
2. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. (утв. Приказом Ростехрегулирования от 27.12.2006 N 373-ст) // КонсультантПлюс [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?base=EXP&n=418509&req=doc#0
3. ГОСТ 34.602-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы. – М.: Стандартинформ, 2009. – 12 с.
4. ГОСТ 12.4.009-83. Межгосударственный стандарт. Система стандартов безопасности труда. Пожарная техника для защиты объектов. Основные виды. Размещение и обслуживание // КонсультантПлюс [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=ESU&n=9134#0
5. «Методика определения актуальных угроз безопасности персональных данных при их обработки в информационных системах персональных данных» (утв. ФСТЭК РФ от 14 февраля 2008г) // КонсультантПлюс [Электронный ресурс]. – http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=77814&fld=134&dst=1000000001,0&rnd=0.7356947169060526#0
6. «О коммерческой тайне»: федеральный закон Российской Федерации от 29 июля 2004 №98-ФЗ: (в ред. от 12.03.14) // КонсультантПлюс [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=160225&fld=134&dst=1000000001,0&rnd=0.7837671849669785#0
7. Постановление Правительства РФ от 25.04.2012 N 390 (ред. от 21.03.2017) «О противопожарном режиме» (вместе с «Правилами противопожарного режима в Российской Федерации») // КонсультантПлюс [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=214359&fld=134&dst=1000000001,0&rnd=0.02918617286551339 3#0
8. СанПиН 2.2.2/2.4.1340-03. Гигиенические требования к персональным электронно-вычислительным машинам и организации работы — М.: Изд-во стандартов, 2003. — 32 с.
9. СанПиН 2.2.4.3359-16. Санитарно-эпидемиологические требования к физическим факторам на рабочих местах // Информационная система МЕГАНОРМ [Электронный ресурс]. – Режим доступа: http://meganorm.ru/Index2/1/4293753/4293753139.htm
10. СП 9.13130.2009. Свод правил. Техника пожарная. Огнетушители. Требования к эксплуатации" (утв. Приказом МЧС РФ от 25.03.2009 N 179) // КонсультантПлюс [Электронный ресурс]. – Режим доступа:

http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=91587&fld=134&dst=100001,0&rnd=0.26064711048474565#0

11. "Трудовой кодекс Российской Федерации" от 30.12.2001 N 197-ФЗ (ред. от 03.07.2016) (с изм. и доп., вступ. в силу с 01.01.2017) // КонсультантПлюс [Электронный ресурс]. – http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=201079&fld=134&dst=1000000001,0&rnd=0.7021406734602476#0

Основная литература

1. Безопасность жизнедеятельности. /Под ред. Н.А. Белова - М.: Знание, 2000 – 364 с.
2. Борьба с шумом на производстве: Справочник / Е.Я. Юдин, Л.А. Борисов; Под общ. ред. Е.Я. Юдина – М.: Машиностроение, 1985. – 400 с.
3. Дубовцев, В.А. Безопасность жизнедеятельности. / Учеб. пособие для дипломников. - Киров: изд. КирПИ, 1992. – 213 с.
4. Репин В., Елиферов В. Процессный подход к управлению. Моделирование бизнес-процессов. - М: РИА Стандарты и качество, 2006. - 405 с.\
5. Управление финансовой устойчивостью предприятий / Божко В. П., Балычев С.Ю., Батьковский А. М. и др., 2013. №4. С. 36-41.

ПРИЛОЖЕНИЕ А

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ЧЕЛЯБИНСКАЯ ОБЛАСТЬ

Индивидуальный предприниматель

СУСКИЙ СЕРГЕЙ ЛЕОНИДОВИЧ

ОГРН 310744809900028; ИНН 745203358162

БИК 046577774 к/сч 30101810400000000774; р/сч 40802810600120000617 в ООО банк «Нейва»

Юридический адрес: 454014, г. Челябинск, ул. Ворошилова, 12А, 86

Фактический адрес: 454030, г. Челябинск, ул. Бейвеля 54

ПАСПОРТ ПРЕДПРИЯТИЯ

С точки зрения обеспечения информационной безопасности
«__» _____ 2018 №____
г. Челябинск

Паспорт предприятия «ИП Суский»
Содержание паспорта предприятия:

1. Организационно-правовая форма предприятия (организации, учреждения) и его реквизиты
   1.1. Название предприятия: Индивидуальный предприниматель Суский.
   1.2. Численность сотрудников: 7.
   1.3. Банковские реквизиты:
   ИНН 745203358162
   р/сч. № 40802810600120000617
   к/сч. № 30101810400000000774
   в банке «Нейва» ООО, Екатеринбург.
   БИК 046577774

2. Виды деятельности предприятия:
   2.1. Торговля оптовая прочими машинами, оборудованием и принадлежностями
   2.2. Торговля оптовая неспециализированная
   2.3. Торговля оптовая прочими бытовыми товарами
   2.4. Торговля автомобильными деталями, узлами и принадлежностями
   2.5. Торговля оптовая прочими машинами и оборудованием
3. Предполагаемые виды защиты информации.
   3.1. Коммерческая тайна
   3.2. Персональные данные
4. Перечень предприятий поставщиков, клиентов и конкурентов.
   4.1. Клиентами «ИП Суский» являются как физические, так и юридические лица
   4.2. Конкуренты «ИП Суский»
   - ООО ТД «Элмаш»
   - ООО «ДЛН»

5. Описание организационной структуры предприятия.

Организационная структура «ИП Суский» включает в себя следующее:

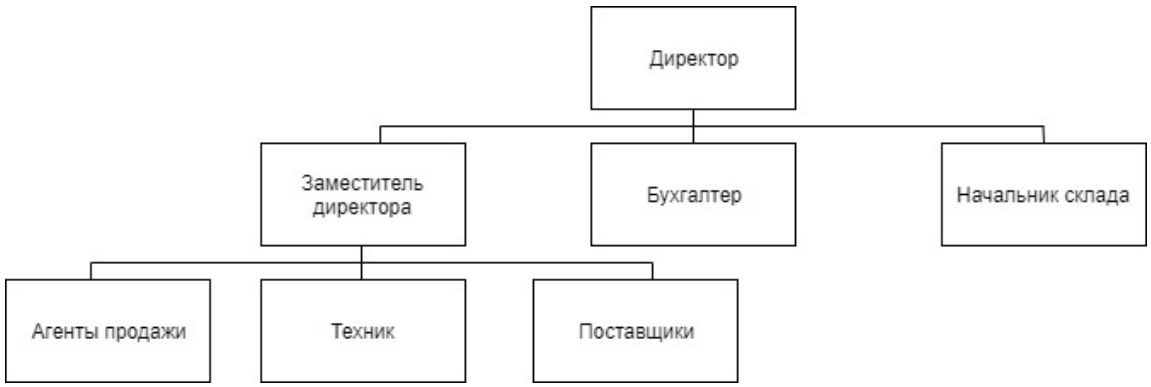

Рисунок А 1 – Организационная структура «ИП Суский»

6. Описание строительной инфраструктуры здания.

Предприятие расположено по адресу Бейвеля 54:
   6.1. 10 этажное здание
   6.2. Ничем не ограждено
   6.3. Система центрального водяного отопления
   6.4. Система пожаротушения

7. Программно-аппаратные средства:

7.1. Пакет Microsoft Oficce 2007 – необходим при оформлении (дополнении и изменении) договоров, приказов, распоряжений;

7.2. Avast Antivirus – антивирусное ПО, установленное на АРМ

7.3. 1С Предприятие 8 – необходимо для автоматизации бухгалтерского и налогового учета.

8. Описание информационной среды предприятия.

Таблица А 1 – Информационная среда предприятия

Программа	Назначение
Windows 10	Операционная система, установленная на АРМ сотрудников
Пакет Microsoft Office 2007	Офисный пакет для работы с документами
Avast Antiviruse	Антивирусное ПО, установленное на АРМ
1с:Предприятие	Программа для оформления отчетности предприятия
Adobe Reader DC	Программа для чтения, печати и рецензирования файлов PDF
WinRAR	Программа для открытия и сжатия файлов и папок
Mail.ru Агент	Программа для мгновенного обмена сообщениями
Google Chrome	Интернет браузер

9. Схема помещения предприятия.

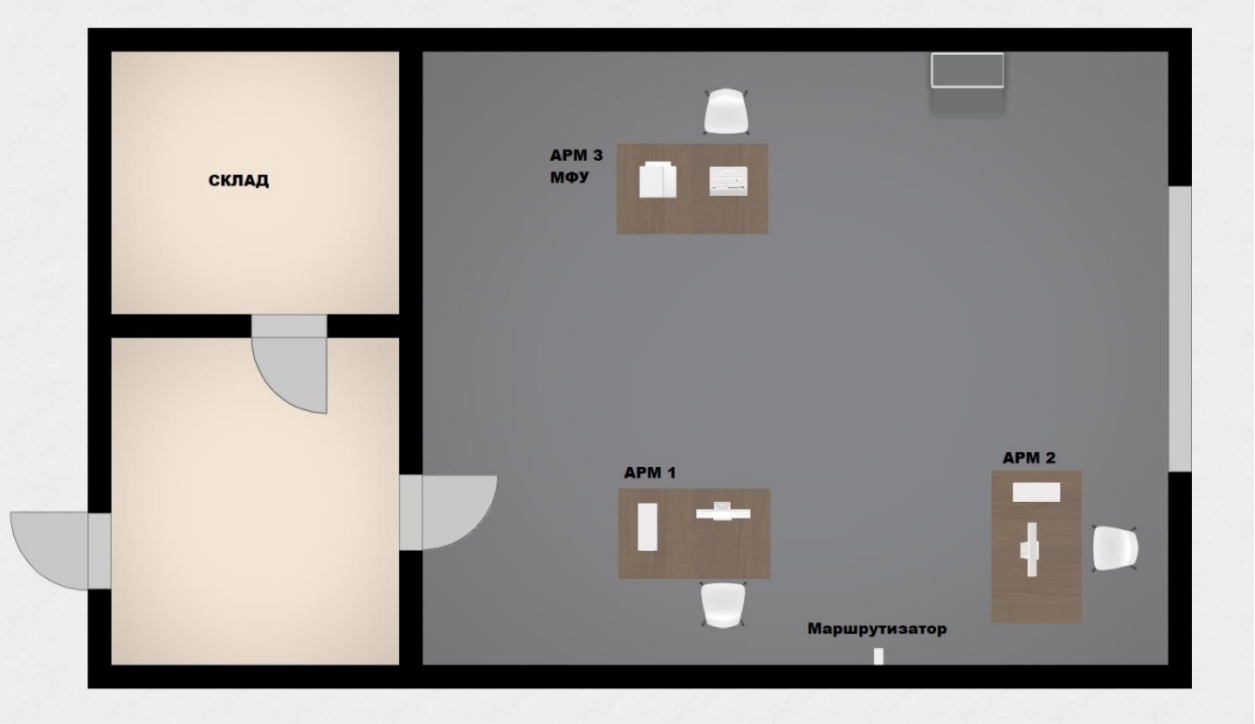

Рисунок А 2 – Схема помещения

Границы помещения так же являются контролируемой зоной.

ПРИЛОЖЕНИЕ Б

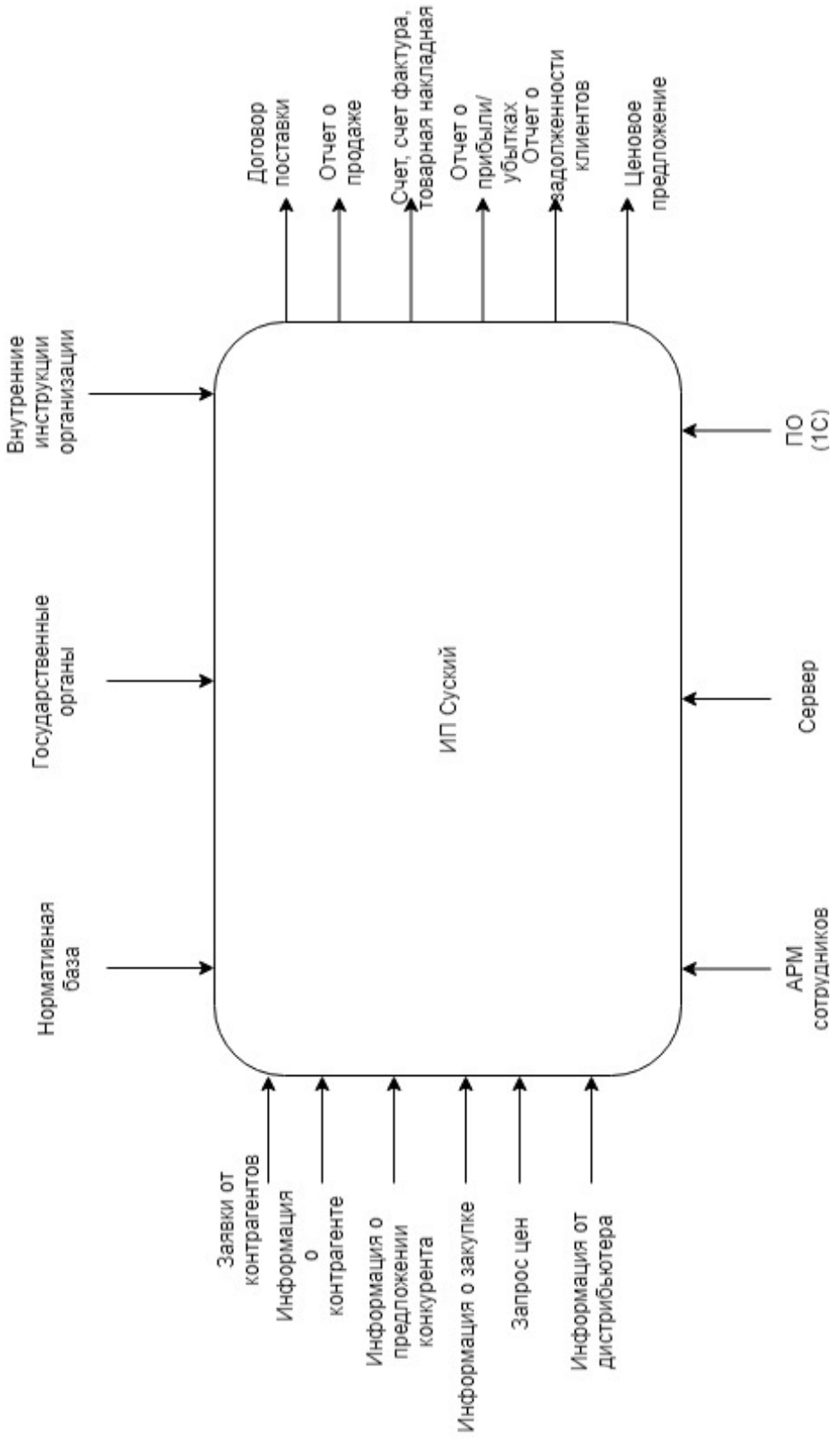

Рисунок Б 1 – Общая модель деятельности

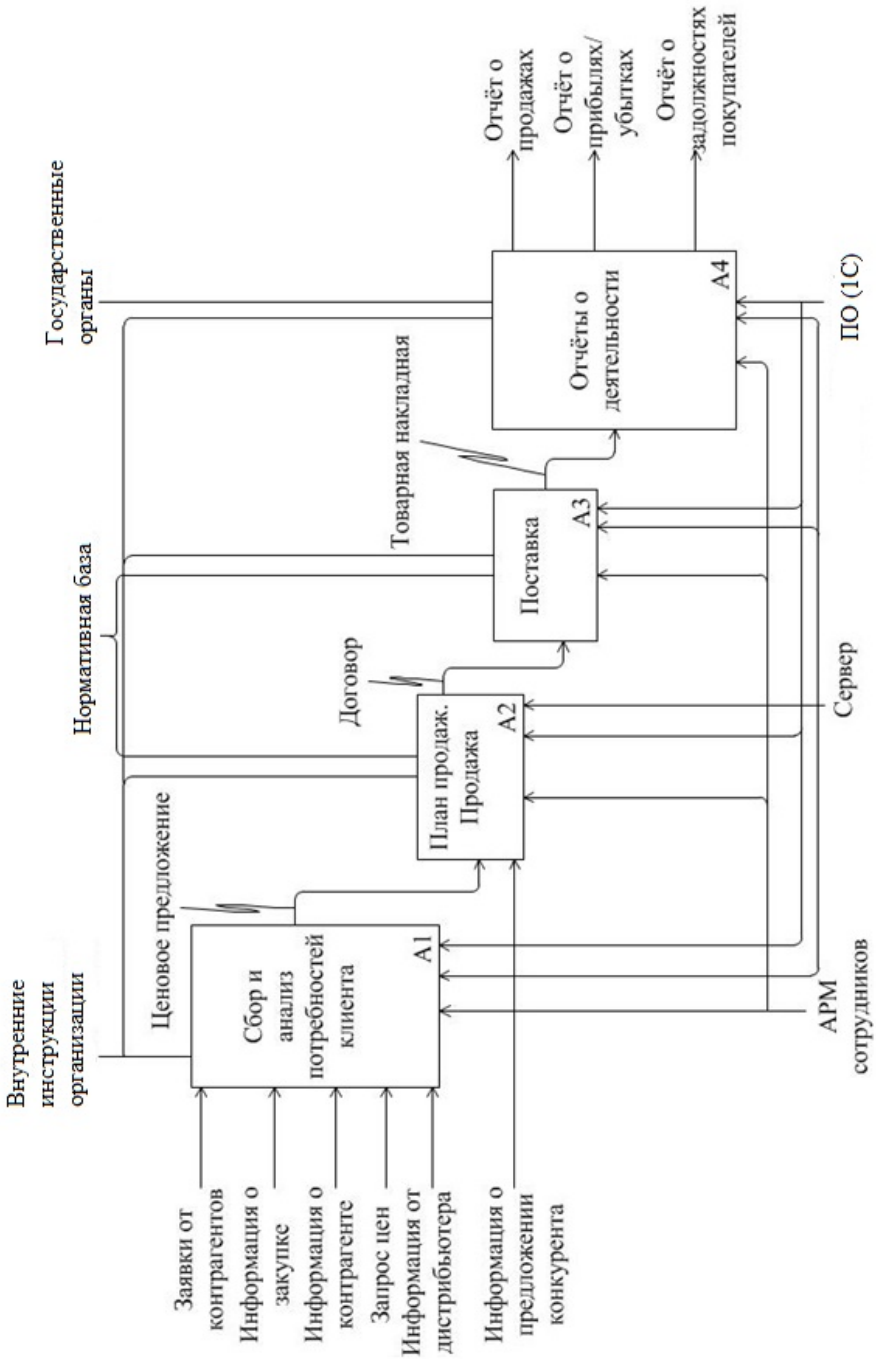

Рисунок Б 2 – Частная модель деятельности предприятия

ПРИЛОЖЕНИЕ В

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее положение разработано на основании Гражданского кодекса, ФЗ «О коммерческой тайне» от 29.07.2004г. №98-ФЗ, других федеральных законов РФ;

1.2. Настоящее положение регулирует отношения, связанные с отнесением информации к коммерческой тайне, передачей такой информации, охраной ее конфиденциальности в целях обеспечения баланса интересов обладателя информации, составляющей коммерческую тайну, и других участников регулируемых отношений, в том числе государства, на рынке товаров, работ, услуг и предупреждения недобросовестной конкуренции, а также определяет сведения, которые не могут составлять коммерческую тайну;

1.3. Настоящее Положение распространяется на информацию, составляющую коммерческую тайну, независимо от вида носителя, на котором она зафиксирована;

1.4. Настоящее Положение не распространяется на сведения, отнесенные в установленном порядке к государственной тайне, в отношении которой 58люю58няются положения законодательства Российской Федерации о государственной тайне;

1.5. Законодательство Российской Федерации о коммерческой тайне состоит из Гражданского кодекса Российской Федерации, Федерального закона «О коммерческой тайне» № 98-ФЗ от 29.07.2004г., других федеральных законов.

II. ПОРЯДОК ОПРЕДЕЛЕНИЯ ИНФОРМАЦИИ СОСТАВЛЯЮЩЕЙ КОММЕРЧЕСКУЮ ТАЙНУ

2.1. Право на отнесение информации к сведениям, составляющим коммерческую тайну, и на определение Перечня и состава таких сведений принадлежит обладателю такой информации в рамках действующего законодательства Российской Федерации и настоящего Положения;

2.2. Непосредственное отнесение сведений к коммерческой тайне и присвоение грифа «Коммерческая тайна» является обязанностью исполнителя и должностного лица, изготовившего, подписавшего (утвердившего) документ, на основании Перечня сведений, составляющих коммерческую тайну «ИП Суский»;

2.3. Перечень сведений, составляющих коммерческую тайну (далее – Перечень) создается на основе предложений директора с учетом настоящего Положения и действующего законодательства Российской Федерации;

Перечень, изменения и дополнения в него принимаются и утверждаются в соответствии с Уставом «ИП Суский»;

2.4. Информация, самостоятельно полученная лицом при осуществлении исследований, систематических наблюдений или иной деятельности, считается полученной законным способом несмотря на то, что содержание указанной информации может совпадать с содержанием информации, составляющей коммерческую тайну, обладателем которой является другое лицо;

2.5. Информация, составляющая коммерческую тайну, полученная от ее обладателя на основании договора или другом законном основании, считается полученной законным способом;

2.6. Ограничения на распространение сведений, составляющих коммерческую тайну, возникающие в результате совместной деятельности «ИП Суский», его партнеров или клиентов, должны быть оговорены в договоре о сотрудничестве (взаимной деятельности, обслуживании), в котором также отражаются взаимные обязательства и ответственность сторон за сохранность этих сведений;

2.7. Информация, составляющая коммерческую тайну, обладателем которой является другое лицо, считается полученной незаконно, если ее получение осуществлялось с умышленным преодолением принятых обладателем информации, составляющей коммерческую тайну, мер по охране конфиденциальности этой информации, а также, если получающее эту информацию лицо знало или имело достаточные основания полагать, что эта информация составляет коммерческую тайну, обладателем которой является другое лицо, и что осуществляющее передачу этой информации лицо не имеет на передачу этой информации законного основания.

III. ПРАВА ОБЛАДАТЕЛЯ ИНФОРМАЦИЕЙ СОСТАВЛЯЮЩЕЙ КОММЕРЧЕСКУЮ ТАЙНУ

3.1 Обладатель информации, составляющей коммерческую тайну вправе:

3.1.1. Использовать информацию, составляющую коммерческую тайну, для собственных нужд в порядке, не противоречащем законодательству Российской Федерации;

3.1.2. Вводить в гражданский оборот информацию, составляющую коммерческую тайну, на основании договоров, предусматривающих включение в них условий об охране конфиденциальности этой информации;

3.1.3. Требовать от юридических и физических лиц, получивших доступ к информации, составляющей коммерческую тайну, органов государственной власти, иных государственных органов, органов местного самоуправления, которым предоставлена информация, составляющая коммерческую тайну, соблюдения обязанностей по охране ее конфиденциальности;

3.1.4. Требовать от лиц, получивших доступ к информации, составляющей коммерческую тайну, в результате действий, осуществленных случайно или по ошибке, охраны конфиденциальности этой информации;

3.1.5. Защищать в установленном законом порядке свои права в случае разглашения, незаконного получения или незаконного использования третьими лицами информации, составляющей коммерческую тайну, в том числе требовать возмещения убытков, причиненных в связи с нарушением его прав.

IV. КРУГ ЛИЦ ИМЕЮЩИХ ДОСТУП К ИНФОРМАЦИИ СОСТАВЛЯЮЩЕЙ КОММЕРЧЕСКУЮ ТАЙНУ

4.1. Должностные лица и сотрудники «ИП Суский» могут иметь доступ к коммерческой тайне (к сведениям, составляющим коммерческую тайну Предприятия, материальным или электронным носителях которые непосредственно создаются, контролируются или используются в работе в процессе исполнения трудовых обязанностей лицом, имеющим доступ);

4.2. Доступ к сведениям, составляющим коммерческую тайну «ИП Суский», имеют лица, получившие допуск, о чем свидетельствует запись в журналах учета лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;

4.3. Предоставление сведений, составляющих коммерческую тайну «ИП Суский», иным работникам, не имеющим доступ в соответствии с журналами лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана, не допускается.

V. ОХРАНА ИНФОРМАЦИИ СОСТАВЛЯЮЩЕЙ КОММЕРЧЕСКУЮ ТАЙНУ

5.1. Меры по охране конфиденциальности информации, принимаемые ее обладателем, должны включать в себя:

5.1.1. Определение перечня информации, составляющей коммерческую тайну;

5.1.2. Ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

5.1.3. Учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;

5.1.4. Регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

5.1.5. Нанесение на материальные носители (документы), содержащие информацию, составляющую коммерческую тайну, грифа «Коммерческая тайна» с указанием обладателя этой информации (для юридических лиц – полное наименование и место нахождения, для индивидуальных предпринимателей – фамилия,

имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

5.2. Наряду с мерами, указанными в части 1 настоящего раздела, обладатель информации, составляющей коммерческую тайну, вправе применять при необходимости средства и методы технической защиты конфиденциальности этой информации, другие не противоречащие законодательству Российской Федерации меры;

5.3. Меры по охране конфиденциальности информации признаются разумно достаточными, если:

5.3.1. Исключается доступ к информации, составляющей коммерческую тайну, любых лиц без согласия ее обладателя;

5.3.1. Обеспечивается возможность использования информации, составляющей коммерческую тайну, работниками и передачи ее контрагентам без нарушения режима коммерческой тайны.

5.4. Режим коммерческой тайны не может быть использован в целях, противоречащих требованиям защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

VI. ПРАВИЛА ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИИ СОСТАВЛЯЮЩЕЙ КОММЕРЧЕСКУЮ ТАЙНУ

6.1. Информация, составляющая коммерческую тайну Предприятия, не может быть сообщена сотрудником Предприятия третьим лицам, не имеющим допуска с данной информации;

6.2. Сотрудник «ИП Суский» имеет право передавать информацию, составляющую коммерческую тайну «ИП Суский» только лицам, имеющим допуск к данной информации, в объемах, предварительно согласованных в журналах учета лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;

6.3. В тех случаях, когда сотрудник «ИП Суский» выполняет свои непосредственные должностные обязанности, информация, составляющая коммерческую тайну «ИП Суский», может разглашаться сотрудником «ИП Суский» только в рамках вопросов, входящих в компетенцию данного сотрудника и при условии соблюдения требований, предусмотренных п.6.2. настоящего Положения;

6.4. Сотрудник должен знать также, кому из сотрудников «ИП Суский» разрешено работать с информацией, составляющей коммерческую тайну, к которой он сам допущен, и в каком объеме эта информация может быть доведена до этих сотрудников;

6.5. При участии в работе сторонних организаций сотрудник может знакомить их представителей с информацией, составляющей коммерческую тайну, только с разрешения директора. При этом руководитель должен определить кон-

кретные вопросы, подлежащие рассмотрению, и указать, кому и в каком объеме может быть сообщена информация, подлежащая защите;

Продолжение приложения В

6.6. Запрещается помещать без необходимости информацию, составляющую коммерческую тайну Предприятия, в документы открытого характера. Такое нарушение порядка обращения с информацией, составляющей коммерческую тайну Предприятия, рассматривается как их разглашение и влечет ответственность в соответствии с установленным порядком;

6.7. В целях защиты информации, составляющей коммерческую тайну, для распечатки документов, содержащих такую информацию, может применяться специальная бумага (не позволяющая делать аутентичные копии), а также различные специальные средства и методы, позволяющие однозначно выявить источник и способ утечки информации, содержащей коммерческую тайну;

6.8. Об утрате или недостаче документов, изделий, содержащих информацию, составляющую коммерческую тайну Предприятия, удостоверений, пропусков, 62люючей от режимных помещений, хранилищ, сейфов, металлических шкафов, личных печатей, а также о причинах и условиях возможной утечки такой информации сотрудник обязан немедленно сообщить непосредственному директору Предприятия;

6.9. При увольнении, перед уходом в отпуск, отъездом в командировку или предполагаемым отсутствием на рабочем месте в течение более или менее длительного срока сотрудник обязан сдать директору Предприятия все носители информации, составляющие коммерческую тайну (рукописи, черновики, документы, чертежи, магнитные ленты, дискеты, распечатки на принтерах и т.д.), которые находились в распоряжении сотрудника в связи с выполнением им служебных обязанностей;

6.10. Сотрудник обязан по первому требованию уполномоченного лица предъявлять для проверки все числящиеся за ним материалы, содержащие информацию, составляющую коммерческую тайну Предприятия, представлять устные или письменные объяснения о нарушениях установленных правил выполнения работ, учета и хранения документов и т.д., фактов разглашения коммерческой тайны, утраты документов, содержащих коммерческую тайну Предприятия;

6.11. В случае попытки посторонних лиц получить информацию, составляющую коммерческую тайну, сотрудник обязан сообщить об этом директору «ИП Суский»;

6.12. Общество по мотивированному требованию органа государственной власти, иного государственного органа, органа местного самоуправления предоставляет им информацию, содержащую коммерческую тайну, на безвозмездной основе. Мотивированное требование должно быть подписано уполномоченным должностным лицом, содержать указание цели и правового основания затребования информации, составляющей коммерческую тайну, и срок предоставления этой информации, если иное не установлено федеральными законами;

6.13. Общество, а также органы государственной власти, иные государственные органы, органы местного самоуправления, получившие информацию обязаны предоставить эту информацию по запросу судов, органов прокуратуры,

органов предварительного следствия, органов дознания по делам, находящимся в их

Продолжение приложения В

производстве, в порядке и на основаниях, которые предусмотрены законодательством Российской Федерации.

VII. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ ИНФОРМАЦИИ СОСТАВЛЯЩЕЙ КОММЕРЧЕСКУЮ ТАЙНУ

7.1. Обладатель информации, составляющей коммерческую тайну, по мотивированному требованию органа государственной власти, иного государственного органа, органа местного самоуправления предоставляет им на безвозмездной основе информацию, составляющую коммерческую тайну. Мотивированное требование должно быть подписано уполномоченным должностным лицом, содержать указание цели и правового основания затребования информации, составляющей коммерческую тайну, и срок предоставления этой информации, если иное не установлено федеральными законами;

7.2. В случае отказа обладателя информации, составляющей коммерческую тайну, предоставить ее органу государственной власти, иному государственному органу, органу местного самоуправления данные органы вправе затребовать эту информацию в судебном порядке;

7.3. Обладатель информации, составляющей коммерческую тайну, а также органы государственной власти, иные государственные органы, органы местного самоуправления, получившие такую информацию в соответствии с пунктом 7.1 настоящего раздела, обязаны предоставить эту информацию по запросу судов, органов прокуратуры, органов предварительного следствия, органов дознания по делам, находящимся в их производстве, в порядке и на основаниях, которые предусмотрены законодательством Российской Федерации;

7.4. На документах, предоставляемых указанным в пунктах 7.1 и 7.3 настоящего раздела органам и содержащих информацию, составляющую коммерческую тайну, должен быть нанесен гриф "Коммерческая тайна".

VIII. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ ИНФОРМАЦИИ СОСТАВЛЯЮЩЕЙ КОММЕРЧЕСКУЮ ТАЙНУ

8.1.Нарушение настоящего Положения влечет за собой дисциплинарную гражданско-правовую, административную или угол ответственность в соответствии с гражданским законодательством РФ;

8.2. Работник, который в связи с исполнением должностных обязанностей получил доступ к информации, составляющей коммерческую тайну обладателем которой является «ИП Суский» и его контрагенты, в случае умышленного или неосторожного разглашения этой информации при отсутствии в действиях такого работника состава преступления несет дисциплинарную ответственность в соответствии законодательством РФ;

8.3. Лицо, которое использовало информацию, составляющую коммерческую тайну и не имело достаточных оснований считать использование данной информации незаконным, в том числе получило доступ к ней в результате слу-

Продолжение приложения В

чайной ошибки, не может в соответствии с законодательством РФ быть привлечено к ответственности;

8.4. По требованию «ИП Суский» лицо, указанное в пункте 9.2 настоящей статьи, обязано принять меры по охране конфиденциальности информации. При отказе такого лица принять меры «ИП Суский» вправе требовать в судебном порядке защиты своих прав;

8.5. Работники Предприятия подписывают обязательство о неразглашении коммерческой тайны и несут ответственность за допуск на территорию предприятия третьих лиц, проведения этими лицами осмотров, фото-, видеосъемок, объектов находящихся на территории «ИП Суский».

IX. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

9.1. Настоящее Положение утверждается приказом директора «ИП Суский». Изменения и дополнения в настоящее Положение вносятся по решению директора «ИП Суский»;

9.2. Если в результате изменения законодательства Российской Федерации отдельные статьи настоящего Положения вступают в противоречие с Законом, указанные статьи утрачивают силу и до момента внесения изменений и дополнений в настоящее Положение применяются нормы законодательства Российской Федерации;

9.3. Все приложения к настоящему Положению являются его неотъемлемой частью и имеют юридическую силу наравне с Положением.

СОГЛАСОВАНО
Заместитель директора К.С. Дроздова

ПРИЛОЖЕНИЕ Г

Перечень сведений, составляющих коммерческую тайну

1. Структура и персонал:

1.1. Организационно-штатная структура и сведения, содержащиеся в личных делах сотрудников Предприятия.

1.2. Адреса проживания руководителей и сотрудников Предприятия.

1.3. Номера личных автомашин сотрудников.

1.4. Сведения о распорядке дня и передвижениях руководящих работ-работников Предприятия и их служебных командировках.

1.5. Местонахождения руководителей Предприятия и средств оперативной связи с ними (если указанная информация запрашивается частными лицами).

1.6. Сведения о фонде заработной платы.

2. Планы:

2.1. Сведения о стратегии развития Предприятия, о перспективных планах изменения, расширения или свертывания отдельных видов деятельности, услуг и их технико-экономических обоснованиях.

3. Финансовая информация:

3.1. Сведения, раскрывающие плановые и фактические показатели финансового года.

3.2. Сведения, содержащие анализ финансовой устойчивости пред-предприятия, оценку факторов, оказывающих влияние на финансовое состояние предприятия и результаты финансовых операций.

4. Рынок:

4.1. Методы изучения рынка сбыта.

4.2. Сведения о внутри региональной деятельности Компании

5. Партнеры и конкуренты:

5.1. Круг клиентов, списки покупателей и представителей или посредников

5.2. Сведения о конкурентах и деловых партнерах Компании, которые не содержатся в открытых источниках информации, а так же сведения, раскрывающие источники или способы получения этой информации.

6. Переговоры и контракты:

6.1. Сведения о подготовке и результатах проведения переговоров

6.2. Сведения о содержании и фактах заключения сделок.

6.3. Сведения, условия конфиденциальности которых установлены в договорах, контрактах, соглашениях и других обязательствах Компании.

7. Обеспечение безопасности

7.1. Сведения о состоянии и порядке организации в Компании системы обеспечения защиты коммерческой тайны.

7.2. Сведения о состоянии и порядке организации системы обес-обеспечения информационной безопасности Компании.

7.3. Сведения, раскрывающие содержание и методы проведения конкретных мероприятий, направленных на обеспечение безопасности Компании.

ПРИЛОЖЕНИЕ Д

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ЧЕЛЯБИНСКАЯ ОБЛАСТЬ

Индивидуальный предприниматель

СУСКИЙ СЕРГЕЙ ЛЕОНИДОВИЧ

ОГРН 310744809900028; ИНН 745203358162

БИК 046577774 к/сч 30101810400000000774; р/сч 40802810600120000617 в ООО банк «Нейва»

Юридический адрес: 454014, г. Челябинск, ул. Ворошилова, 12А, 86

Фактический адрес: 454030, г. Челябинск, ул. Бейвеля 54

ТЕХНИЧЕСКОЕ ЗАДАНИЕ
по разработке КСЗИ предприятия «ИП Суский»

СОГЛАСОВАНО

Заместитель директора

«ИП Суский»

_____ К.С. Дроздова

Дата_____

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Полное наименование системы и ее условное обозначение.

Полное наименование системы: Комплексная система защиты информации, содержащей коммерческую тайну предприятия «ИП Суский».

Условное обозначение системы: КСЗИ на «ИП Суский».

1.2. Наименования заказчика и исполнителя

Заказчик системы защиты: «ИП Суский» в лице директора предприятия.

Разработчик системы защиты: «ИП Суский» в лице директора предприятия.

1.3. Перечень документов, на основании которых создается КСЗИ:

1.3.1. Конституция Российской Федерации;

1.3.2. Федеральный закон от 29 июля 2004 года N 98-ФЗ «О коммерческой тайне»;

1.3.3. Трудовой кодекс РФ от 30.12.2001 N 197-ФЗ;

1.3.4. Федеральный закон от 08.02.1998 N 14 «Об обществах с ограниченной ответственностью»;

1.3.5. «Уголовный кодекс Российской Федерации» от 13.06.1996 N 63-ФЗ;

1.3.6. Федеральный закон «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» от 05.04.2013 N 44;

1.3.7. Федеральный закон "О закупках товаров, работ, услуг отдельными видами юридических лиц" от 18.07.2011 N 223;

1.3.8. Федеральный закон «Об информации, информационных технологиях и защите информации» от 27 июля 2006 г. N 149;

1.3.9. Гражданский кодекс Российской Федерации часть 4 от 18 декабря 2006 года N 230-ФЗ.

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

Результаты работы оформляются и предъявляются генеральному директору по мере исполнения в виде предварительных проектов. Окончательный вариант проекта согласуется и предоставляется на рассмотрение заказчику в лице генерального директора предприятия.

1.5. Изменения в техническом задании на КСЗИ оформляются дополнением или согласованы и подписаны сторонами протоколом. Дополнение или протокол являются в будущем неотъемлемой частью технического задания.

2. НАЗНАЧЕНИЕ И ЦЕЛИ РАЗРАБОТКИ КСЗИ

2.1. Назначение и цели

Основной целью проведения работ является приведение порядка обработки, хранения и передачи коммерческой тайны «ИП Суский» в соответствие требованиям перечисленных в данном Техническом задании.

3. ХАРАКТЕРИСТИКА ОБЪЕКТОВ ЗАЩИТЫ

3.1. Краткие сведения об объектах защиты

3.1.1. Автоматизированные рабочие места:

3.1.1.1. АРМ директора;

3.1.1.2. АРМ сотрудников организации.

3.1.2. Помещение для хранения и работы с важной информацией:

3.1.2.1. Помещение с АРМ.

3.1.3. Персонал:

3.1.3.1. Директор;

3.1.3.2. Сотрудники организации (7 человек).

4. ТРЕБОВАНИЯ К КСЗИ

4.1. Требования организации-заказчика КСЗИ:

4.1.1. Определить перечень информации, составляющей коммерческую тайну;

4.1.2. Ограничить доступ к информации, составляющей коммерческую тайну;

4.1.3. Произвести учёт лиц, получивших доступ к информации, составляющей коммерческую тайну;

4.1.4. Урегулировать отношения по использованию информации, составляющей коммерческую тайну;

4.1.5. Нанести на материальные носители, содержащие информацию, составляющую коммерческую тайну, грифа "Коммерческая тайна".

5. СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО РАЗРАБОТКЕ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

5.1. КСЗИ 1. Проектирование;

5.2. КСЗИ 1.1. Определение важнейших показателей существующих бизнес-процессов с точки зрения информационной безопасности;

5.3. КСЗИ 1.2. Анализ проблем существующих бизнес-процессов;

5.4. КСЗИ 1.3. Разработка значений важнейших показателей новых бизнес-процессов;

5.5. КСЗИ 1.4. Анализ и отбор наилучших способов и методов улучшения значений важнейших показателей бизнес-процессов;

5.6. КСЗИ 1.5. Разработка и согласование структуры новых бизнес-процессов;

5.7. КСЗИ 2. Разработка новой организационно-распорядительной документации;

5.8. КСЗИ 2.1. Положение «О коммерческой тайне»;

5.9. КСЗИ 2.2. Перечень сведений, составляющих коммерческую тайну;

5.10. КСЗИ 2.3. Приказы об утверждении положения режима коммерческой тайны и перечня сведений, составляющих коммерческую тайну;

5.11. КСЗИ 2.4. Внесение изменений в должностные инструкции;

5.12. КСЗИ 2.5. Согласование и утверждение ОРД;

5.13. КСЗИ 3. Подготовка реализации проекта создания КСЗИ;

5.14. КСЗИ 3.1. Определение ответственных лиц и исполнителей проекта;

5.15. КСЗИ 3.2. Приобретение программно-аппаратного средства защиты от НСД;

5.16. КСЗИ 3.4. Приобретение средств видеонаблюдения;

5.17. КСЗИ 4. Внедрение

5.18. КСЗИ 4.1. Установка и настройка программно-аппаратного средства защиты от НСД;

5.19. КСЗИ 4.2. Установка средств видеонаблюдения;

5.20. КСЗИ 4.3. Контроль защищенности;

5.21. КСЗИ 4.4. Обучение персонала.

6. ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ

6.1. Критериями для приемки работ является полное выполнения требований, установленных в пункте 4 данного технического задания;

6.2. Порядок приемки осуществляется единовременно;

6.3. Порядок оформления замечаний в письменном виде.

7. ТРЕБОВАНИЯ К СОСТАВУ И СОДЕРЖАНИЮ РАБОТ ПО ВВОДУ КСЗИ В ЭКСПЛУАТАЦИЮ

7.1. Требованиями к составу и содержанию работ является выполнение всех разработанных мероприятий по вводу КСЗИ в ООО «Диджитер».

8. ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

8.1. Перечень документов которые должны быть разработаны и соответство-соответствовать требованиям технического задания:

8.1.1. Перечень сведений, составляющих коммерческую тайну;

8.1.2. Положение о режиме коммерческой тайны;

8.1.3. Приказы об утверждении документов.

8.2. Порядок предоставления документов в письменном виде.

9. ИСТОЧНИКИ РАЗРАБОТКИ КСЗИ

9.1. Источники финансирования и бюджет.

Таблица Д 1 – Стоимость обеспечения

№ п/п	Наименование	Количество	Цена за шт. (руб.)	Сумма (руб.)
1	СЗИ НСД «Secret Net»	3	7500	22500
2	Комплект видеонаблюдения FALCON EYE FE-104MHD KIT Light	1	7250	7250
Итог				29750

Таблица Д 2 – Стоимость услуг по обеспечению проекта

№ п/п	Наименование	Стоимость
1	Разработка и описание бизнес-процессов компании с точки зрения ИБ	10000
2	Разработка организационно-распорядительной документации	7400
3	Установка и настройка СЗИ от НСД «Secret Net»	6000
4	Установка и настройка комплекта видеонаблюдения FALCON EYE FE-104MHD KIT Light	5000
6	Обучение пользователей	2000
Итог		30400

ПРИЛОЖЕНИЕ Е

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ЧЕЛЯБИНСКАЯ ОБЛАСТЬ

Индивидуальный предприниматель

СУСКИЙ СЕРГЕЙ ЛЕОНИДОВИЧ

ОГРН 310744809900028; ИНН 745203358162

БИК 046577774 к/сч 30101810400000000774; р/сч 40802810600120000617 в ООО банк «Нейва»

Юридический адрес: 454014, г. Челябинск, ул. Ворошилова, 12А, 86

Фактический адрес: 454030, г. Челябинск, ул. Бейвеля 54

ПРИКАЗ

«___»_____2018 № ___

Об утверждении перечня сведений, составляющих коммерческую тайну

В соответствии с Федеральным законом Российской Федерации от 02.02.2006 № 98-ФЗ «О коммерческой тайне».

ПРИКАЗЫВАЮ:

1. Утвердить прилагаемый Перечень сведений, составляющих коммерческую тайну, обрабатываемых на предприятии «ИП Суский» составленный на 4 (четырех) листах, прошитых и пронумерованных.

2. За поддержанием перечня в актуальном состоянии назначить ответственного:

2.1. Заместителя директора – Дроздову Ксению Сергеевну.

3. Обновление перечня производить один раз в квартал.

4. С приказом ознакомить:

4.1. Бухгалтера – Сускую Елену Владимировну.

Контроль исполнения приказа возложить на заместителя директора – Ксению Сергеевну Дроздову.

Директор С.Л. Суский

С приказом ознакомлен(а):

Бухгалтер Е.В. Суская

Продолжение приложения Е

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ЧЕЛЯБИНСКАЯ ОБЛАСТЬ

Индивидуальный предприниматель

СУСКИЙ СЕРГЕЙ ЛЕОНИДОВИЧ

ОГРН 310744809900028; ИНН 745203358162

БИК 046577774 к/сч 30101810400000000774; р/сч 40802810600120000617 в ООО банк «Нейва»

Юридический адрес: 454014, г. Челябинск, ул. Ворошилова, 12А, 86

Фактический адрес: 454030, г. Челябинск, ул. Бейвеля 54

ПРИКАЗ

«___»_____2018 № ___

Об утверждении положения о коммерческой тайне

В соответствии с Федеральным законом Российской Федерации от 02.02.2006 № 98-ФЗ «О коммерческой тайне».

ПРИКАЗЫВАЮ:

1. Утвердить прилагаемое Положение о коммерческой тайне «ИП Суский» составленный на 11 (одиннадцати) листах, прошитых и пронумерованных.

2. За поддержанием перечня в актуальном состоянии назначить ответственного:

2.2. Заместителя директора – Ксению Сергеевну Дроздову.

3.Обновление перечня производить один раз в квартал.

4. С приказом ознакомить:

4.2. Бухгалтера – Сускую Елену Владимировну.

Контроль исполнения приказа возложить на заместителя директора – Ксению Сергеевну Дроздову.

Директор С.Л. Суский

С приказом ознакомлен(а):

Бухгалтер Е.В. Суская

ПРИЛОЖЕНИЕ Ж

Инструкция по обеспечению сохранности коммерческих тайн на предприятии «ИП Суский»

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая инструкция разработана в соответствии с требованиями законодательства Российской Федерации и учредительных документов организации. Она предусматривает административные и экономические механизмы по защиты коммерческой тайны предприятия с целью предотвращения нанесения возможного экономического и морального ущерба организации со стороны юридических и физических лиц, вызванного их неправомерными или не осторожными действиями путем безвозмездного присвоения чужой информации или разглашения коммерческой тайны.

Под коммерческой тайной предприятия понимаются не являющиеся государственными секретами сведения, связанные с предоставлением организацией услуг, технологической информацией, управлением, финансами и другой деятельностью организации, разглашение (передача, утечка) которых может нанести ущерб ее интересам. К сведениям, составляющим коммерческую тайну, относятся несекретные сведения, предусмотренные "Перечнем сведений, составляющих коммерческую тайну организации", утвержденным и введенным в действие приказом руководителя организации. Коммерческая тайна организации является его собственностью. Если она представляет собой результат совместной деятельности с другими организациями, основанной на договорных началах, то коммерческая тайна может быть собственностью двух сторон, что должно найти отражение в договоре.

Под разглашением коммерческой тайны подразумевается умышленные или неосторожные действия должностных или иных физических лиц, приведшие к не вызванному служебной необходимостью или преждевременному открытому опубликованию сведений, подпадающих под категорию сведений, составляющих

коммерческую тайну, а также передача подобных сведений по открытым техническим каналам связи.

Под открытым опубликованием таких сведений подразумевается их публикация в открытой печати, сети передачи данных «Интернет», передача по радио и телевидению, оглашение на международных, зарубежных и открытых внутрироссийских симпозиумах, совещаниях, конференциях, съездах, при публичных вступлениях и защите диссертаций, вывоз материалов за границу или передача их в любой форме иным фирмам, организациям или отдельным лицам.

Необходимость открытого опубликования сведений, составляющих коммерческую тайну, их объемы, формы и время опубликования определяются руководителем организации.

Использование для открытого опубликования сведений, полученных на договорной или доверительной основе или являющихся результатом совместной деятельности, допускается только с общего согласия партнеров.

При определении сведений, которые не могут составлять коммерческую тайну необходимо руководствоваться Постановлением правительства РСФСР от 5 декабря 1991 г. N 35.

Передача информации сторонним организациям, с которыми организация не связано прямыми служебными контактами, должна регулироваться, как правило, договорными отношениями, предусматривающими обязательства и ответственность пользователей, включая возмещение материальных затрат за предоставление информации и компенсацию за нарушение договорных обязательств.

Предоставление коммерческой информации представителям служебных, ревизионных, фискальных и следственных органов, народным депутатам, органам печати, радио, телевидения и т.п. допускается только с разрешения руководства организации.

Документы и издания с грифом "КОММЕРЧЕСКАЯ ТАЙНА" ("КТ") рассматриваются как материалы, содержащие сведения ограниченного распространения.

Защита коммерческой тайны предусматривает: порядок определения информации, содержащей коммерческую тайну, и сроков ее действия систему допуска сотрудников организации, частных и командированных лиц к сведениям, составляющим коммерческую тайну организации, обязанности лиц, допущенных к таким сведениям порядок работы с документами, имеющими гриф "КТ" обеспечение сохранности документов, дел и изданий с грифом "КТ" принципы организации и проведения контроля за обеспечением установленного порядка при работе со сведениями, составляющими коммерческую тайну ответственность за разглашение сведений и утрату документов, содержащих коммерческую тайну.

Ответственность за организацию работы с материалами, имеющими гриф "КТ", разработку и осуществление необходимых мер по сохранности коммерческой тайны Директор предприятия возлагает на руководство предприятия.

Контроль за осуществлением мер, обеспечивающих сохранность коммерческой тайны, возлагается на ответственного за безопасность предприятия.

2. ОПРЕДЕЛЕНИЕ ИНФОРМАЦИИ И ОБОЗНАЧЕНИЕ ДОКУМЕНТОВ, СОДЕРЖАЩИХ КОММЕРЧЕСКУЮ ТАЙНУ, И СРОКОВ ЕЕ ДЕЙСТВИЯ.

Необходимость проставления грифа "Коммерческая тайна" ("КТ") определяется в соответствии с Перечнем, указанным в части 1 настоящей Инструкции: руководителем предприятия или заместителем руководителя.

На документах, делах и изданиях, содержащих сведения, составляющие коммерческую тайну, проставляется гриф "Коммерческая тайна" ("КТ"), а на документах и изданиях, кроме того, - номера экземпляров. Гриф и номера экземпляров, проставляются в правом верхнем углу первой страницы документа, на обложке или титульном листе издания и на первой странице сопроводительного письма к этим материалам.

На обратной стороне последнего листа каждого экземпляра печатается разметка, в которой указывается: количество отпечатанных экземпляров, номер, фа-

милия исполнителя и его телефон, дата, и срок действия коммерческой тайны (регистрационный номер проставляется на каждом листе документа).

Срок действия коммерческой тайны, содержащейся в документе, определяется в каждом конкретном случае руководителем предприятия или заместителем руководителя в виде конкретной даты или в виде пометок: "до заключения контракта", "бессрочно" и т.п.

Основанием для снятия грифа "Коммерческая тайна" является решение должностного лица, принявшего решение о присвоении данному документу грифа «коммерческая тайна»

Гриф "КТ" после принятия решения о его снятия погашается штампом или записью от руки с указанием даты и подписи руководителя, принявшего решение о снятии грифа

3. ОРГАНИЗАЦИЯ РАБОТЫ С ДОКУМЕНТАМИ, ИМЕЮЩИМИ ГРИФ "КОММЕРЧЕСКАЯ ТАЙНА" ("КТ")

Документы, имеющие гриф "КТ", подлежат обязательной регистрации руководителей .

Права на информацию, порядок пользования ею, сроки ограничения на публикацию могут оговариваться дополнительно в тексте документа и его реквизитах.

Отсутствие грифа "КТ" и предупредительных оговорок в тексте и реквизитах означает свободную рассылку и предполагает, что автор информации и лицо, подписавшее или утвердившее документ, предусмотрели возможные последствия от свободной рассылки и несут за это ответственность.

Вся поступающая корреспонденция, имеющая гриф "КТ" (или другие соответствующие этому понятию грифы, например, "секрет предприятия, "тайна предприятия" и др.) принимается и вскрывается сотрудниками предприятия, которым поручена работа с этими материалами. При этом проверяется количество листов и экземпляров, а также наличие указанных в сопроводительном письме

приложений. При обнаружении отсутствия в конвертах (пакетах) указанных документов составляется акт в двух экземплярах: один экземпляр акта направляется отправителю.

Все входящие, исходящие и внутренние документы, а также издания с грифом "КТ" подлежат регистрации и учитываются по количеству листов, а издания - поэкземплярно.

Учет документов и изданий с грифом "КТ" ведется в журналах или карточках отдельно от учета другой служебной несекретной документации. Листы журналов нумеруются, прошиваются и опечатываются. Документы, которые не подшиваются в дела, учитываются в журнале инвентарного учета.

Движение документов и изданий с грифом "КТ" своевременно отражается в журналах или карточках.

На зарегистрированном документе с грифом "КТ" (или на сопроводительном листе к изданиям с грифом "КТ") должен быть проставлен штамп с указанием наименования предприятия, регистрационный номер документа и дата его поступления.

Издания с грифом "КТ" регистрируются в журнале учета и распределения изданий.

Отпечатанные и подписанные документы вместе с их черновиками передаются для регистрации сотруднику подразделения делопроизводства службы безопасности, осуществляющему их учет. Черновики уничтожаются исполнителем и этим сотрудником, что подтверждается росписью указанных лиц в журнале или на карточках учета. При этом проставляется дата и подпись.

Размножение документов и изданий с грифом "КТ" в типографиях и других множительных участках производится с разрешения и под контролем специально назначенных сотрудников службы безопасности по заказам, подписанным руководителем предприятия.

Размноженные документы "КТ" (копии, тираж) должны быть полистно подобраны, пронумерованы поэкземплярно и, при необходимости, сброшюрованы

(сшиты). Нумерация дополнительно размноженных экземпляров, производится от последнего номера, ранее учтенных экземпляров этого документа.

Перед размножением на последнем листе оригинала (подлинника) проставляется запись: " Регистрационный номер _____. Дополнительно размножено _____ экз., на _____ листах текста. Наряд N ___ от _____. Подпись (" исполнитель заказа) ". Одновременно делается отметка об этом в соответствующих журналах и карточках учета.

Рассылка документов и изданий с грифом "КТ" производиться на основании подписанных руководителем структурного подразделения разнарядок с указанием учетных номеров отправляемых экземпляров.

Пересылка пакетов с грифом "КТ" может осуществляться через органы спецсвязи или фельдсвязи.

Документы с грифом "КТ" после исполнения группируются в отдельные дела. Порядок их группировки предусматривается специальной номенклатурой дел, в которую в обязательном порядке включаются все справочные картотеки и журналы на документы и издания с грифом "КТ".

Снятия рукописных, машинописных, микро – ксеро и фотокопий, электрографических и др. копий, а также производство выписок из документов и изданий с грифом "КТ" сотрудниками предприятия производится по разрешению руководителя предприятия.

Обработка информации с грифом "КТ" производится на учетных СВТ, которые имеют категорию не ниже 4-Б.

4. ПОРЯДОК ОБЕСПЕЧЕНИЯ СОХРАННОСТИ ДОКУМЕНТОВ, ДЕЛ И ИЗДАНИЙ

Все имеющие гриф "КТ" документы, дела и издания должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах. По-

мещения должны отвечать требованиям внутри объектного режима, обеспечивающего физическую сохранность находящейся в них документации.

Дела с грифом "КТ", выдаваемые исполнителю, подлежат возврату в подразделение делопроизводства службы безопасности (СБ) в тот же день. При необходимости, с разрешения начальника подразделения делопроизводства СБ или уполномоченного СБ они могут находиться у исполнителя в течении срока, необходимого для выполнения задания, при условии полного обеспечения их сохранности и соблюдения правил хранения.

С документацией с грифом "КТ" разрешается работать только в служебных помещениях. Для работы вне служебных помещений необходимо разрешение руководителя предприятия или структурного подразделения.

Документы, дела и издания с грифом "КТ" могут передаваться другим сотрудникам, допущенным к этим документам, только через делопроизводство СБ или уполномоченного СБ.

Изъятия из дел или перемещение документов с грифом "КТ" из одного дела в другое без санкции руководителя делопроизводства СБ или уполномоченного СБ, осуществляющего их учет, запрещается.

Смена сотрудников, ответственных за учет и хранение документов, дел и изданий с грифом "КТ", оформляется распоряжением руководства. При этом составляется по произвольной форме акт приема-передачи этих материалов, утверждаемый указанным руководителем.

Уничтожение документов "КТ" производится комиссией в составе не менее трех человек с составлением акта.

Печатание документов "КТ" разрешается в машинописном бюро или непосредственно в подразделениях. Для учета отпечатанных документов ведется специальный журнал.

5. ПОРЯДОК ДОПУСКА К СВЕДЕНИЯМ, СОСТАВЛЯЮЩИМ КОММЕРЧЕСКУЮ ТАЙНУ ПРЕДПРИЯТИЯ

Допуск сотрудников к сведениям, составляющим коммерческую тайну, осуществляется руководителем предприятия или заместителем руководителя.

Ответственный за службу безопасности обязан обеспечить систематический контроль за допуском к этим сведениям только тех лиц, которым они необходимы для выполнения служебных обязанностей.

К сведениям, составляющим коммерческую тайну, допускаются лица, личные и деловые качества которых обеспечивают их способность хранить коммерческую тайну, и только после оформления в службе безопасности письменного обязательства по сохранению коммерческой тайны.

Допуск сотрудников к работе с делами "КТ" осуществляется согласно оформленному не внутренней стороне обложки дела или на отдельном листе списку за подписью руководителя предприятия структурного подразделения, а к документам - в соответствии с указаниями, содержащимися в резолюциях руководителей предприятия и подразделений.

Представители сторонних организаций и частные лица могут быть допущены к ознакомлению и работе с документами и изданиями с грифом "КТ" с письменного разрешения руководителей предприятия или заместителя руководителя, в ведении которых находятся эти материалы.

Выписки из документов и изданий, содержащих сведения с грифом "КТ", производятся в блокнотах (или тетрадях), которые имеют такой же гриф. После окончания работы они высылаются в адрес той организации, которая будет указана данным представителем.

Выдача дел и изданий с грифом "КТ" исполнителям и прием от них производится под расписку в "Карточке учета выдаваемых дел и изданий."

Дела и издания непосредственно представителям сторонних организаций и частным лицам не выдаются. При необходимости с их содержанием они ознакомятся только с разрешения руководителя предприятия через уполномоченного службы безопасности или представителя заинтересованного подразделения.

6. КОНТРОЛЬ ЗА ВЫПОЛНЕНИЕМ ТРЕБОВАНИЙ ВНУТРИ ОБЪЕКТНОГО РЕЖИМА ПРИ РАБОТЕ СО СВЕДЕНИЯМИ СОДЕРЖАЩИМИ КОММЕРЧЕСКУЮ ТАЙНУ.

Под внутри объектовым режимом при работе с коммерческой тайной подразумевается соблюдение условий работы, исключающих возможность утечки информации о сведениях, содержащих коммерческую тайну.

Контроль за соблюдением указанного режима осуществляется в целях изучения и оценки состояния сохранности коммерческой тайны, выявления и установления причин недостатков, и выработки предложений по их устранению.

Контроль за обеспечением режима при работе со сведениями, содержащими коммерческую тайну, осуществляют ответственный за службу безопасности предприятия и руководитель путем текущих и плановых проверок.

При проведении проверок создается комиссия, которая комплектуется из опытных и квалифицированных работников в составе не менее двух человек, допущенных к работе с материалами "КТ".

Участие в проверке не должно приводить к необоснованному увеличению осведомленности в этих сведениях.

Плановые проверки проводятся не реже одного раза в год комиссиями на основании приказа или распоряжения руководителя предприятия.

Проверяющие имеют право знакомиться со всеми документами, журналами (карточками) и другими материалами, имеющими отношение к проверяемым вопросам, а также проводить беседы, консультироваться со специалистами и исполнителями, требовать представления письменных объяснений, справок и отчетов по всем вопросам, входящим в компетенцию комиссии.

При проверках присутствует руководитель предприятия или его заместитель.

По результатам проверок составляется акт или справка с отражением в нем наличия документов, состояния работы с материалами "КТ", выявленных недостатков и предложений по их устранению. Акт утверждается руководителем предприятия.

При выявлении случаев утраты документов или разглашения сведений, составляющих коммерческую тайну, ставятся в известность руководитель предприятия и его заместитель (помощник) по безопасности. Для расследования указанных случаев приказом руководителя предприятия создается комиссия, которая: определяет соответствие содержания утраченного документа проставленному грифу "КТ" и выявляет обстоятельства утраты (разглашения). По результатам работы комиссии составляется акт.

7. ОБЯЗАННОСТИ СОТРУДНИКОВ ПРЕДПРИЯТИЯ РАБОТАЮЩИХ СО СВЕДЕНИЯМИ, ПРЕДСТАВЛЯЮЩИМИ КОММЕРЧЕСКУЮ ТАЙНУ, И ИХ ОТВЕТСТВЕННОСТЬ ЗА ЕЕ РАЗГЛАШЕНИЕ.

Сотрудники предприятия, допущенные к сведениям, составляющим коммерческую тайну, несут ответственность за точное выполнение требований, предъявляемых к ним в целях обеспечения сохранности указанных сведений.

До получения доступа к работе, связанной с коммерческой тайной, им необходимо изучить настоящую инструкцию и дать в службе безопасности письменное обязательство о сохранении коммерческой тайны.

Сотрудники предприятия, допущенные к коммерческой тайне должны:

- строго хранить коммерческую тайну. О ставших им известной утечке сведений, составляющих коммерческую тайну, а также об утрате документов с грифом "КТ", сообщать непосредственному руководителю и в службу безопасности.

- предъявлять для проверки по требованию представителей службы безопасности все числящиеся документы с грифом "КТ", а в случае нарушения установленных правил работы с ними представлять соответствующие объяснения.

- знакомиться только с теми документами и выполнять только те работы, к которым они допущены.

- строго соблюдать правила пользования документами, имеющими гриф "КТ". Не допускать их необоснованной рассылки.

- все полученные в делопроизводстве службы безопасности или у ее уполномоченного документы с указанным грифом немедленно вносить во внутреннюю опись документов которой отводится специальный раздел по учету "КТ".

- исполненные входящие документы, а также документы, предназначенные для рассылки, подшивки в дело или уничтожения сдавать в делопроизводство службы безопасности или уполномоченному службы безопасности.

- выполнять требования внутри объектного режима: исключающие возможность ознакомления с документами "КТ" посторонних лиц, включая и своих сотрудников, не имеющих к указанным документам прямого отношения.

- при ведении деловых переговоров с представителями сторонних организаций или частными лицами ограничиваться выдачей минимальной информации, действительно необходимой для их успешного завершения.

- исключить использование ставшей известной коммерческой тайны предприятия в свою личную пользу, а также деятельность, которая может быть использована конкурентами в ущерб предприятию - владельцу данной коммерческой тайны.

- ответственность за разглашение сведений, составляющих коммерческую тайну предприятия, и утрату документов или изделий, содержащих такие сведения устанавливается в соответствии с действующим законодательством.

При этом подразумевается:

Под разглашением сведений, составляющих коммерческую тайну - предание огласке сведений лицом, которому эти сведения были доверены по службе, работе или стали известны иным путем, в результате чего они стали достоянием посторонних лиц.

Под утратой документов или изделий (предметов), содержащих сведения, относящиеся к коммерческой тайне, - выход (в том числе и временный) документов или изделий из владения ответственного за их сохранность лица, которому они были доверены по службе или работе, являющийся результатом наруше-

ния установленных правил обращения с ними, вследствие чего эти документы или изделия стали либо могли стать достоянием посторонних лиц.

ПРИЛОЖЕНИЕ 3

Инструкция о порядке физической охраны помещений, содержащих носители персональных данных.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая инструкция о порядке физической охраны помещений, содержащих носители персональных данных (далее Инструкция) определяет обязанности должностных лиц и порядок взаимодействия между структурными подразделениями «ИП Суский» (далее Оператор) по обеспечению безопасности носителей персональных данных.

1.2. Данная Инструкция разработана в соответствии с: Федеральным законом «О персональных данных»; Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации; Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных.

1.3. Обеспечение безопасности физической охраны помещений, содержащих носители персональных данных, является частью комплексной системы безопасности Оператора.

2.ПОРЯДОК ФИЗИЧЕСКОЙ ОХРАНЫ ПОМЕЩЕНИЙ, СОДЕРЖАЩИХ НОСИТЕЛИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Под носителями персональных данных (ПДн) в настоящей инструкции понимаются бумажные документы, содержащие ПДн, и элементы информационных систем персональных данных.

2.2. Помещения, содержащие носители персональных данных (далее Помещения), в нерабочее время должны быть закрыты на ключ и сданы под охрану.

2.3. В Помещения имеют допуск только лица, допущенные в установленном порядке к обработке ПДн. Возможность неконтролируемого проникновения или пребывания в этих Помещениях посторонних лиц должна быть исключена.

2.4. По окончании рабочего дня Помещение запирает и сдает под охрану работник, имеющий право доступа в Помещение.

2.5. В начале рабочего дня работник, имеющий право доступа в Помещение, перед вскрытием Помещения проверяет целостность и исправность сигнализации и дверных запоров. В случае обнаружения нарушений, указывающих на возможность проникновения в Помещение посторонних лиц, работник Помещение не вскрывает, а о случившемся незамедлительно сообщает администратору безопасности (АБ), который в свою очередь незамедлительно сообщает _____, составляет акт.

2.6. При срабатывании охранной сигнализации, извещающей о несанкционированном доступе или попытке доступа в Помещение АБ незамедлительно дол-

жен прибыть к входной двери Помещения, выяснить причину срабатывания сигнализации и поставить об этом в известность непосредственного руководителя.

ПРИЛОЖЕНИЕ И

Положение о разграничении прав доступа к персональным данным

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящее Положение о разграничении прав доступа к обрабатываемым персональным данным в «ИП Суский» (далее Предприятие) разработано в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Правилами внутреннего трудового распорядка Предприятия и определяет уровень доступа должностных лиц к персональным данным клиентов. Положение применяется в Предприятие, сотрудники которого обрабатывают персональные данные неавтоматизированным способом.

2. ОСНОВНЫЕ ПОНЯТИЯ

- **Правила разграничения доступа-** совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.
- **Персональные данные** - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы и другая информация.
- **Безопасность персональных данных** - состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.
- **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.
- **Обработка персональных данных** - сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение персональных данных клиентов Предприятия;
- **Неавтоматизированная обработка персональных данных** - обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека. Неавтоматизированная обработка регулируется Постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

3. РАЗГРАНИЧЕНИЕ ПРАВ ДОСТУПА ПРИ НЕАВТОМАТИЗИРОВАННОЙ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Разграничение прав осуществляется исходя из характера и режима обработки персональных данных на материальных носителях.
Категории работников, ответственных за неавтоматизированную обработку персональных, а так же их уровень прав доступа к персональным данным представлены в таблице.

Группа	Уровень доступа к ПДн	Разрешенные действия
Руководители предприятия (Директор, Зам. директора)	Обладают полной информацией о клиентах Доступ к носителям, содержащих ПДн клиентов	сбор и систематизация; накопление и хранение; уточнение (обновление, изменение); использование; уничтожение; блокирование; обезличивание.
Бухгалтер	Доступ к носителям, содержащих ПДн клиентов	сбор и систематизация; накопление и хранение; уточнение (обновление, изменение); использование; уничтожение;

Таблица Л 1 – Уровень прав доступа к ПДн

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

Работники Предприятия, допущенные к обработке ПДн и виновные в нарушении норм, регулирующих получение, обработку и защиту ПДн, несут дисциплинарную административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

ПРИЛОЖЕНИЕ К

Инструкция по обработке персональных данных без использования средств автоматизации

I. Общие положения

1.1. Инструкция разработана в соответствии и во исполнение Конституции Российской Федерации, Трудового Кодекса РФ, федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», федерального закона от 27 июля 2006 года № 149 -ФЗ «Об информации, информационных технологиях и о защите информации», в соответствии с «Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденным Постановлением Правительства РФ от 15 сентября 2008 года № 687, Уставом «ИП Суский» (далее Предприятие) и иными локальными нормативными документами Предприятия.

1.2. Настоящая Инструкция устанавливает порядок работы с документами – носителями конфиденциальной информации, содержащей персональные данные, в целях:

1) предотвращения несанкционированного уничтожения, хищения, утраты, искажения, копирования, блокирования информации, содержащей персональные данные;

2) соблюдения правового режима использования информации, содержащей персональные данные;

3) обеспечения возможности обработки и использования персональных данных Предприятием и должностными лицами, имеющими соответствующие полномочия.

1.3. В целях обеспечения сохранности и конфиденциальности информации, содержащей персональные данные, все операции по оформлению, формированию, ведению и хранению данной информации должны выполняться сотрудниками Предприятия, осуществляющими данную работу в соответствии со своими служебными обязанностями, зафиксированными в их должностных инструкциях.

II. Порядок обеспечения безопасности при обработке и хранении персональных данных

2.1. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна вестись таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных.

2.2. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкцио-

нированный доступ к ним.

2.3. Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе лица, осуществляющие такую обработку по договору с Предприятием), должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки.

2.4. Материальные носители с персональными данными должны храниться в запирающихся на ключ помещениях, металлических шкафах, сейфах, иных шкафах, имеющих запираемые блок-секции.

2.5. Должностным лицам, работающим с персональными данными, запрещается разглашать информацию, содержащую персональные данные, устно или письменно кому бы то ни было, если это не вызвано служебной необходимостью, либо необходимостью защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных.

2.6. На Предприятии должно обеспечиваться раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо несовместимы.

2.7. Ответы на запросы граждан и организаций даются в том объеме, который позволяет не разглашать в ответах конфиденциальные данные, за исключением данных, содержащихся в материалах запроса или опубликованных в общедоступных источниках.

2.8. При приеме посторонних лиц не допускается:

1) присутствие в открытом доступе на столе рабочих документов, содержащих персональные данные;

2) голосовая обработка информации, содержащей персональные данные.

2.9. Режим конфиденциальности персональных данных отменяется в случаях обезличивания этих данных, в отношении персональных данных, ставших общедоступными, или по истечении 75-летнего срока их хранения, если иное не предусмотрено законом.

III. Ответственность

7.1. Ответственность за неисполнение или ненадлежащее выполнение требований настоящей Инструкции возлагается на должностных лиц и руководителей Предприятия.

7.2. Повседневный контроль за выполнением положений настоящей Инструкции возлагается на руководителей Предприятия.

7.3. За нарушение правил обработки персональных данных, их неправомерное разглашение или распространение, виновные уполномоченные лица несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством.

7.4. В случае если в результате действий уполномоченного лица был причинен подлежащий возмещению работодателем ущерб третьим лицам, работник несет перед работодателем материальную ответственность в соответствии с действующим законодательством.

ПРИЛОЖЕНИЕ Л

Акт об уничтожении носителей на предприятие «ИП Суский», содержащих персональные данные

1. Общие положения

1.1. Настоящее Положение о порядке уничтожения в «ИП Суский» (далее Предприятие» носителей, содержащих персональные данные (далее по тексту - Положение) устанавливает периодичность и способы уничтожения носителей, содержащих персональные данные субъектов персональных данных.

1.2. Целью настоящего Положения является обеспечение защиты прав и свобод клиентов при обработке их персональных данных на Предприятии.

1.3. Основные понятия, используемые в Положении:

- субъект персональных данных – клиент, к которому относятся соответствующие персональные данные;

- 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 на Предприятии, позволяет идентифицировать личность субъекта персональных данных;

- 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;

- уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;

- носители персональных данных - как электронные (дискеты, компакт-диски, ленты, флеш-накопители и другие), так и неэлектронные (бумажные) носители персональных данных.

1.4. Настоящее Положение разработано на основе Федерального закона от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и других нормативных правовых актов.

2. Правила уничтожения носителей, содержащих персональные данные

Уничтожение носителей, содержащих персональные данные субъектов персональных данных, должно соответствовать следующим правилам:

- быть конфиденциальным, исключая возможность последующего восстановления;
- оформляться юридически, в частности, актом о выделении документов, содержащих персональные данные субъектов персональных данных, к уничтожению и актом об уничтожении носителей, содержащих персональные данные субъектов персональных данных;
- должно проводиться комиссией по уничтожению персональных данных;
- уничтожение должно касаться только тех носителей, содержащих персональные данные субъектов персональных данных, которые подлежат уничтожению в связи с истечением срока хранения, достижения цели обработки указанных персональных данных либо утраты необходимости в их достижении, не допуская случайного или преднамеренного уничтожения актуальных носителей.

3. Порядок уничтожения носителей, содержащих персональные данные

3.1. Персональные данные субъектов персональных данных хранятся не дольше, чем этого требуют цели их обработки, и подлежат уничтожению по истечении срока хранения, достижении целей обработки или в случае утраты необходимости в их достижении.

3.2. Носители, содержащие персональные данные субъектов персональных данных, уничтожаются в специально отведённом для этих целей помещении _____ Комиссией по уничтожению персональных данных, утвержденной приказом директора Предприятия (далее - Комиссия).

3.3. Носители, содержащие персональные данные субъектов персональных данных, уничтожаются Комиссией в срок, не превышающий тридцати дней с даты истечения срока хранения, достижения цели обработки персональных данных либо утраты необходимости в их достижении.

3.4. Комиссия производит отбор бумажных носителей персональных данных, подлежащих уничтожению, с указанием оснований для уничтожения.

3.5. На все отобранные к уничтожению документы составляется акт о выделении документов, содержащих персональные данные субъектов персональных данных, к уничтожению.

3.6. В актах о выделении документов, содержащих персональные данные субъектов персональных данных, к уничтожению и актах об уничтожении носителей, содержащих персональные данные субъектов персональных данных, исправления не допускаются.

3.7. Комиссия проверяет наличие всех документов, включенных в акт о выделении носителей, содержащих персональные данные субъектов персональных данных, к уничтожению.

3.8. По окончании сверки акт о выделении документов, содержащих персональные данные субъектов персональных данных, к уничтожению подписывается всеми членами Комиссии и утверждается директором Предприятия.

3.9. Носители, содержащие персональные данные субъектов персональных данных, отобранные для уничтожения и включенные в акт, после проверки их Комиссией передаются, ответственному за уничтожение документов в помещение_____.

3.10. Уничтожение носителей, содержащих персональные данные субъектов персональных данных, производится после утверждения акта в присутствии всех членов комиссии, которые несут персональную ответственность за правильность и полноту уничтожения перечисленных в акте носителей.

3.11. Уничтожение персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

3.12. Уничтожение носителей, содержащих персональные данные, осуществляется в следующем порядке:

- уничтожение персональных данных, содержащихся на бумажных носителях, осуществляется путем измельчения на мелкие части, исключающие возможность последующего восстановления информации. Измельчение осуществляется с использованием шредера (уничтожителя документов), установленного в помещении _____ либо передаются на переработку (утилизацию) организациям, собирающим вторсырье (пункты приема макулатуры);

- уничтожение персональных данных, содержащихся на машиночитаемых носителях, осуществляется путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления данных. Вышеуказанное достигается путем деформирования, нарушения единой целостности носителя;

- подлежащие уничтожению файлы с персональными данными субъектов персональных данных, расположенные на жестком диске, удаляются средствами операционной системы компьютера с последующим «очищением корзины»;

- в случае допустимости повторного использования носителя CD-RW, DVD-RW применяется программное удаление («затирание») содержимого диска путем его форматирования с последующей записью новой информации на данный носитель.

4. Порядок сдачи макулатуры

4.1. Документы, по истечении срока хранения, достижении целей обработки или в случае утраты необходимости в их достижении подлежат уничтожению путем сдачи организациям, собирающим вторсырье (пункты приема макулатуры).

4.2. Выделенные документы по акту о выделении документов, содержащих персональные данные субъектов персональных данных, к уничтожению передаются к уничтожению в упакованном виде.

4.3. Документы, подлежащие вывозу, не должны содержать бумагу и картон, не пригодные для переработки; бумагу и картон, покрытые полиэтиленом и другими полимерными пленками; материал, выделяющий ядовитые и токсичные вещества.

4.4. Документы, подлежащие вывозу, не должны содержать:

- тряпье, веревку, шпагат из лубяных волокон и полимеров;

- металлические и деревянные изделия, кусочки стекла и керамики, камень, уголь, слюду, целлофан, целлулоид, полимерные материалы в виде изделий (пленок, гранул), пенопласт, искусственную и натуральную кожу, клеенку, битум, парафин, остатки химических и минеральных веществ и красок;

- влажность документов, подлежащая вывозу, должна быть не более 10 %.

4.5. Сдача оформляется приемо-сдаточными накладными, данные которых (дата сдачи, номер накладной, вес сданной макулатуры) указываются в акте о выделении документов, содержащих персональные данные субъектов персональных данных, к уничтожению.

4.6. Погрузка и вывоз документов осуществляются под контролем лица, ответственного за обеспечение сохранности документов структурного подразделения.

4.7. Отобранные к уничтожению документы перед сдачей на переработку в качестве макулатуры должны в обязательном порядке измельчаться до степени, исключающей возможность прочтения текста.

5. Порядок оформления документов об уничтожении персональных данных

5.1. Об уничтожении носителей, содержащих персональные данные Комиссия составляет и подписывает акт об уничтожении носителей, содержащих персона-

льные данные субъектов персональных данных, который утверждается директором Предприятия.

5.2. Акт об уничтожении носителей, содержащих персональные данные субъектов персональных данных, составляется по установленной форме.

В акте указываются:

- дата, место и время уничтожения;
- должности, фамилии, инициалы членов Комиссии;
- вид и количество уничтожаемых носителей, содержащих персональные данные субъектов персональных данных;
- основание для уничтожения;
- способ уничтожения.

5.3. Факт уничтожения носителей, содержащих персональные данные субъектов персональных данных, фиксируется в журнале учета, документов переданных на уничтожение. Данный документ является документом конфиденциального характера и вместе с актами хранится в помещении _____ в течение одного года. По истечении срока хранения акт о выделении документов, содержащих персональные данные субъектов персональных данных, к уничтожению и акт об уничтожении носителей, содержащих персональные данные субъектов персональных данных перемещаются в архив Предприятия на хранение.

6. Ответственность руководителей

6.1. Ответственным лицом за организацию хранения документов являются руководители Предприятия.

6.2. Руководители Предприятия могут быть привлечены к административной ответственности за нарушение требований по организации хранения документов, содержащих персональные данные.

ПРИЛОЖЕНИЕ М

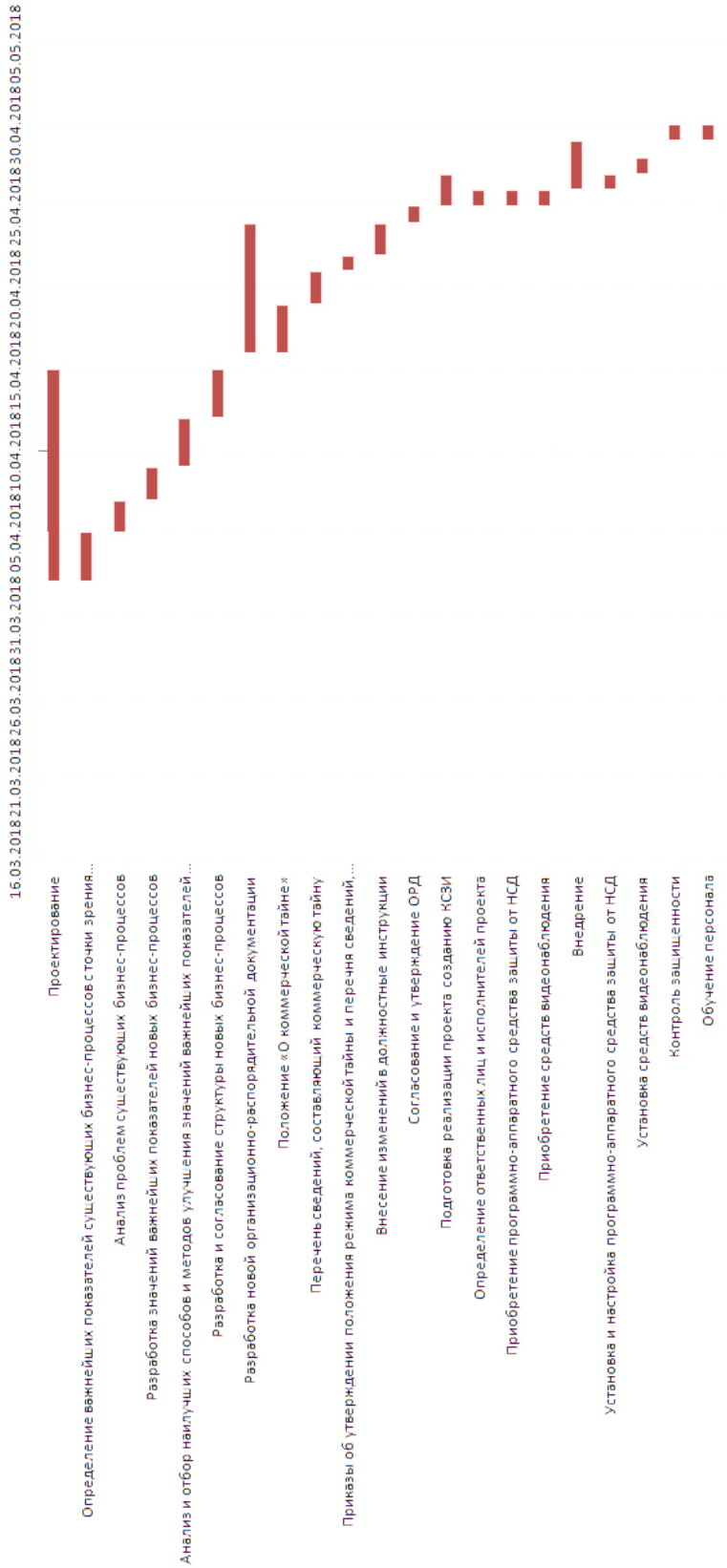

Рисунок М 1 – Диаграмма Ганта

ПРИЛОЖЕНИЕ Н

Инструкция по организации работы с электронными носителями, содержащих коммерческую тайну.

1. Общие положения

1.1. Настоящая Инструкция устанавливает основные требования к организации учета, использования, передачи и уничтожения электронных носителей информации (далее - носители), предназначенных для обработки КТ.

1.2. Под электронными носителям информации в данном документе понимаются: гибкие магнитные диски, CD- и DVD-диски, USB флеш-диски, НЖМД и др.

1.3. Ответственность за организацию учета, использования, передачи и уничтожения носителей, предназначенных для обработки и хранения КТ, затирание (удаление) информации возлагается ответственного за обеспечение ИБ на предприятии.

1.4. Положения данной инструкции обязательны для выполнения всеми сотрудниками предприятия, которые в ходе выполнения своих должностных обязанностей используют носители КТ, а так же имеющими допуск к обработке КТ.

2. Учёт и хранение электронных носителей информации

2.1. Учёту подлежат все носители информации, находящиеся в распоряжении Предприятия и предназначенные для хранения КТ.

2.2. Носители учитываются в специальном «Журнале регистрации и учета электронных носителей конфиденциальной информации и персональных данных» (Приложение О) в котором производится непосредственно регистрация и учёт носителей.

2.3. Регистрация и учет носителей информации осуществляется ответственным за ИБ.

2.4. Учётный номер носителя состоит из порядкового номера по журналу регистрации через дефис (например: уч. № 01/К, где 1 – порядковый номер в журнале, К – «Конфиденциально»).

2.5. Каждый носитель информации, применяемый при обработке информации на СВТ, должен иметь гриф конфиденциальности, соответствующий записанной на нём информации: конфиденциальной информации - «К». Исключается хранение на одном носителе информации разных грифов конфиденциальности, а так же хранение информации, имеющей разные цели обработки.

2.6. Для съемных носителей информации реквизиты наносятся непосредственно на носитель (корпус). Если невозможно маркировать непосредственно носитель (корпус), то применяется маркировка упаковки, в которой хранится носитель или другие доступные способы маркировки (бирки, брелоки и т.п.). Надпись реквизитов делается разборчиво и аккуратно. На дискеты и футляры носителей допускается наклеивать заранее заготовленную этикетку.

2.7. Каждому носителю в журнале должна соответствовать отдельная строка.

2.8. НЖМД в серверах и системных блоках компьютеров учитываются в паспорте (формуляре) на поставляемое оборудование с указанием марки носителя информации и его серийного номера.

2.9. Хранение носителей информации осуществляется в условиях (закрываемые шкафы, сейфы и т.п.), исключающих возможность хищения, приведения в негодность или уничтожения содержащейся на них информации.

2.10. О фактах утраты носителей необходимо незамедлительно докладывать руководителю предприятия или его заместителю**.**

2.11. Ответственный за ИБ не реже одного раза в год осуществляет проверку условий хранения носителей КТ.

3. Выдача/сдача и передача носителей

3.1. Выдача носителей сотрудникам осуществляется ответственным за ИБ под подпись с отметкой в «Журнале выдачи/сдачи электронных носителей конфиденциальной информации и персональных данных» (Приложение П). Факт сдачи носителя регистрируется аналогичным образом.

3.2. Носители, как правило, выдаются только непосредственно на время работы с данным носителем и сдаются сотрудником сразу по завершению таких работ.

3.3. Носители, которые выдаются сотруднику, должны пройти проверку на отсутствие записанной на ней информации. В случаи наличия какой-либо информации на выдаваемом носителе, ответственный за ИБ обязан удалить **(**затереть) информацию согласно п. 4. настоящей инструкции.

3.4. В случае повреждения носителей, содержащих КТ, сотрудник, в пользовании которого они находятся, обязан сообщить о случившемся руководителю и ответственному за ИБ.

3.5. При передаче в другие организации носители информации должны, по возможности, быть упакованы в пакет/конверт, обеспечивающий сохранность (работоспособность) передаваемого носителя. При этом носители информации передаются с сопроводительным письмом, в котором указывается, какая информация содержится на данном носителе, а для подтверждения достоверности информации прилагается таблица с реквизитами файлов (допускается прикладывать скриншот окна архиватора). Данное передвижение (передача) носителей КТ регистрируется в «Журнале передачи носителей конфиденциальной информации и персональных данных» (Приложение Р), где делается отметка об отправке (куда отправлен (реквизиты адресата), исходящий номер сопроводительного письма, дата отправки, способ отправки (курьер, заказная почта и т.п.)) и отметка о получении (номер «Уведомления о вручении» или «Накладной»). В случае если передача носителей осуществляется лично сотрудником Предприятия, то у адресата, необходимо взять расписку о получении носителя (Приложение С).

3.6. Для исключения утечки информации, находящейся на жестких дисках компьютеров, при необходимости ремонта компьютера в сервисном центре, жесткий диск с компьютера демонтируется и компьютер отправляется в ремонт без жесткого диска. При необходимости диагностирования самого жесткого диска информация должна быть предварительно скопирована на резервный носитель и затем стёрта с направляемого в ремонт винчестера с использованием специальных средств (сертифицированные программные или программно-аппаратные средства защиты информации, обеспечивающие невозможность восстановления информации), либо путём полного трехкратного его форматирования. Если невозможно произвести данные действия (поломка жесткого диска или ПЭВМ), то отправка такой ПЭВМ в ремонт возможна только по письменному разрешению ответственного за ИБ.

4. Порядок уничтожения носителей, затирания информации на носителях

4.1. Уничтожение носителей информации, пришедших в негодность или утративших практическую ценность, производится путем их физического разрушения без возможности дальнейшего восстановления.

4.2. Перед уничтожением носителя вся информация с него должна быть стерта (уничтожена) путем использования специальных средств (сертифицированные программные или программно-аппаратные средства защиты информации, обеспечивающие невозможность восстановления информации), либо путём полного трехкратного его форматирования, если это позволяют физические принципы работы носителя.

4.3. Уничтожение носителей, затирания (уничтожении) информации с носителей производиться комиссией из 3 человек, назначенной приказом руководителя Предприятия. В состав комиссии должен входить ответственный за ИБ.

4.4. По факту уничтожения носителей, а также затирания (уничтожения) информации на носителях, комиссией составляется Акт (Приложение Т). В Акте указываются учётные номера носителей, характер уничтожаемой (затираемой) информации, причина уничтожения носителя (затирания информации на нем). Реквизиты Акта заносятся председателем данной комиссии в графу «Сведения об уничтожении» «Журнала регистрации и учета электронных носителей конфиденциальной информации и персональных данных». Подписанный Акт должен храниться у ответственного за ИБ.

ПРИЛОЖЕНИЕ О

Журнал №__
регистрации и учета электронных носителей, содержащих коммерческую тайну

Журнал начат «____» _____
201_ г.
Должность
_____/
/

подпись фамилия, имя, отчество
Журнал завершен «____» _____
201_ г.
Должность
_____/
/

подпись фамилия, имя, отчество
Журнал составлен на _____ листах

№ п/п	Регистрационный номер электронного носителя	Вид (тип, модель) электронного носителя	Характер информации, которая будет содержаться на носителе	Дата регистрации электронного носителя	ФИО лица, регистрирующего носитель	Подпись лица, регистрирующего носитель
1	2	3	4	5	6	7

ПРИЛОЖЕНИЕ П

Журнал №__
выдачи/сдачи электронных носителей, содержащих коммерческую тайну

Журнал начат
«____»_____ 201_ г.
Должность
_____/
/
подпись фамилия, имя, отчество
Журнал завершен
«____»_____ 201_ г.
Должность
_____/
/
подпись фамилия, имя, отчество
Журнал составлен на _____ листах

Дата	Время	Регистрационный номер электронного носителя	Сдал		Принял	
			ФИО, должность	Подпись	ФИО, должность	Подпись
1	2	3	4	5	6	7

ПРИЛОЖЕНИЕ Р

Журнал №__
передачи носителей, содержащих коммерческую тайну

Журнал начат
«____»_____ 201_ г.
Должность
_____/
/
подпись фамилия, имя, отчество
Журнал завершен
«____»_____ 201_ г.
Должность
_____/
/
подпись фамилия, имя, отчество
Журнал составлен на _____ листах

Дата	Регистрационный номер электронного носителя	Характер информации, содержащейся на передаваемом носителе	Исходящий номер сопроводительного письма	Адресат (название организации, отдел, должность, ФИО и т.п.	Способ передачи/отправки носителя (лично, курьер, заказная почта)	Отправитель (лицо, записавшее информацию на носитель)		Отметка о доставке (дата, реквизиты документа, подтверждающие отправку
						ФИО, должность	Подпись	
1	2	3	4	5	6	7	8	9

ПРИЛОЖЕНИЕ С

№_____
заполняется отправителем

Расписка
(составлена в двух экземплярах, по одному для каждой из сторон)

«___»_____ 201_ г. г. Челябинск

Настоящим подтверждаю получение электронного носителя информации (Регистрационный номер электронного носителя_____) с сопроводи тельным письмом (Исходящий номер сопроводительного письма _____) от ИП Суский Сергей Леонидович
Должность и ФИО представителя организации:
_____

Сведения о получателе:

Название организации:
_____
Должность и ФИО получателя:
_____
_____

«___»_____ 201_ г.
_____/_____/
подпись получателя расшифровка

ПРИЛОЖЕНИЕ Т

АКТ № ____
о затирании/уничтожении конфиденциальной информации и электронных носителей

«____»_____201_ г. г. Челябинск

Комиссия в составе:
Председатель:
– Ф.И.О. должностного лица
Члены комиссии:
– Ф.И.О. должностного лица

Ф.И.О. должностного лица составила настоящий Акт о том, что в ее присутствии уничтожены следующие электронные носители персональных данных и иной конфиденциальной информации/ информация на следующих электронных носителях

Регистрационный номер электронного носителя	Вид (тип, модель) электронного носителя	Характер информации, которая содержится на носителе	Причина	Способ уничтожения (физическое разрушение, форматирование, с использованием специальных программных средств (каких))
1	2	3	4	5

Председатель комиссии: Ф.И.О. должностного лица
Члены комиссии: Ф.И.О. должностного лица
Ф.И.О. должностного лица

Отметку в «Журнал регистрации и учета электронных носителей конфиденциальной информации и персональных данных» произвел ответственный за информационную безопасность

_____ (ФИО)_____.
подпись