

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт
Факультет приборостроения,
информационных технологий и
электроники

Кафедра
«Информационная безопасность
систем и технологий»

Специальность 100503 –

Специализация –

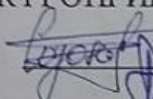
Информационная безопасность
автоматизированных систем
Защищенные автоматизированные
системы управления

ДИПЛОМНЫЙ ПРОЕКТ

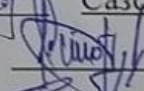
на тему

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В АО
«ПО «ЭЛЕКТРОПРИБОР»

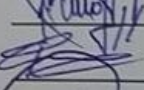
Студент

 Сазонов Геннадий Сергеевич

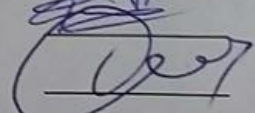
Руководитель

 Дубин Р.М.

Нормоконтролёр

 Фатеев А.Г.

Рецензент

 Дудко Н.Н.

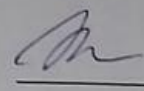
Работа допущена к защите (протокол заседания кафедры от 20.06.2016 № 14)

Заведующий кафедрой

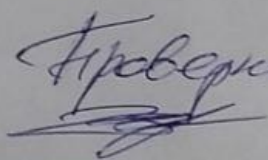
 С.Л. Зефирин

Работа защищена с отметкой отлично (протокол заседания ГЭК
от 24.06.16 № 17)

Секретарь ГЭК

 А.П. Иванов

Пенза 2016

 Проверка ВКР – Тобянов
С.Л. Зефирин

РЕФЕРАТ

Отчёт 175с., 17 рис., 23 табл., 14 источников.

ПОЛИТИКА, ИДЕНТИФИКАЦИЯ, КОНФИДЕНЦИАЛЬНАЯ ИНФОРМАЦИЯ, ПЕРСОНАЛЬНЫЕ ДАННЫЕ, КОММЕРЧЕСКАЯ ТАЙНА, ИНФОРМАЦИОННАЯ СИСТЕМА, УГРОЗА, УЯЗВИМОСТЬ, МОДЕЛЬ УГРОЗ, ЗАЩИТНЫЕ МЕРЫ, ЗАЩИТНЫЕ СРЕДСТВА, ДОКУМЕНТАЦИЯ.

Объектом исследования является защищённость конфиденциальной информации, обрабатываемой в АО «ПО «Электроприбор».

Цель работы – разработка политики по обеспечению защиты конфиденциальной информации в АО «ПО «Электроприбор».

В процессе работы было выполнено выявление конфиденциальной информации, обрабатываемой в АО «ПО «Электроприбор», определение значимости данной информации, произведена оценка исходной защищённости информационных систем, в которых производится обработка различных видов конфиденциальной информации, завершённая составлением моделей угроз безопасности, разработан перечень защитных мер, а также выбраны программные средства и разработана соответствующая документация для реализации данных мер.

В результате была разработана по обеспечению защиты конфиденциальной информации в АО «ПО «Электроприбор».

СОДЕРЖАНИЕ

Обозначения и сокращения.....	7
Введение.....	9
1 Идентификация организационной структуры АО «ПО «Электроприбор».....	11
2 Выявление конфиденциальной информации, обрабатываемой на предприятии.....	17
3 Определение значимости выявленной информации.....	25
4 Оценка исходной защищённости информационных систем АО «ПО «Электроприбор».....	28
4.1 Оценка исходной защищённости информационной системы персональных данных «Персонал» АО «ПО «Электроприбор».....	28
4.1.1 Определение масштабов ИС.....	28
4.1.2 Составление перечня угроз информационной безопасности.....	36
4.1.3 Идентификация актуальных угроз информационной безопасности.....	43
4.1.4 Разработка модели нарушителя.....	51
4.2 Оценка исходной защищённости информационной системы коммерческой тайны АО «ПО «Электроприбор».....	51
4.2.1 Определение масштабов информационной системы коммерческой тайны.....	51
4.2.1.1 Описание процессов обработки информации, составляющей коммерческую тайну «АО «ПО «Электроприбор» и структуры информационной системы коммерческой тайны.....	51
4.2.1.2 Определение условий использования информации, составляющей КТ.....	51

4.2.2 Составление перечня угроз информационной безопасности для информационной системы коммерческой тайны	66
4.2.3 Идентификация актуальных угроз безопасности для информации, составляющей коммерческую тайну АО «ПО «Электроприбор»	72
4.2.4 Разработка модели нарушителя.....	75
4.3 Оценка исходной защищённости информационной системы конфиденциальной информации АО «ПО «Электроприбор»	75
4.3.1 Определение масштабов информационной системы конфиденциальной информации.....	75
4.3.1.1 Описание процессов обработки иной конфиденциальной информации в АО «ПО «Электроприбор» и структуры информационной системы иной конфиденциальной информации.....	75
4.3.1.2 Определение условий использования информации, составляющей КТ	79
4.3.2 Составление перечня угроз информационной безопасности для информационной системы иной конфиденциальной информации.....	82
4.3.3 Идентификация актуальных угроз безопасности для иной конфиденциальной информации в АО «ПО «Электроприбор»	82
4.3.4 Разработка модели угроз безопасности для иной конфиденциальной информации.....	82
4.3.4 Разработка модели нарушителя.....	82
5 Выбор мер и средств защиты	84
5.1 Выбор мер и средств защиты для обеспечения безопасности персональных данных обрабатываемых в информационной системе персональных данных «Персонал»	84

5.1.1. Определение уровня защищённости информационной системы персональных данных «Персонал»..	84
5.1.2 Разработка перечня защитных мер для обеспечения безопасности персональных данных.....	86
5.1.3 выбор средств защиты для обеспечения безопасности персональных данных	90
5.2 Выбор мер и средств для обеспечения безопасности конфиденциальной информации, обрабатываемой в информационной системе коммерческой тайны	91
5.2.1 Разработка защитных мер для информации, составляющей коммерческую тайну	91
5.2.2 Выбор средств защиты для обеспечения безопасности информации, составляющей коммерческую тайну	93
5.3 Выбор мер и средств защиты для конфиденциальной информации, обрабатываемой в информационной системе конфиденциальной информации	93
6 Разработка документации.....	95
Заключение	96
Список использованных источников.....	97
Приложение А. Политика по защите конфиденциальной информации...	99
Приложение Б. Базовый набор защитных мер	123
Приложение В. Инструкция администратора безопасности	128
Приложение Г. Инструкция по соблюдению режима конфиденциальности.....	137
Приложение Д. Положение «О коммерческой тайне».....	141
Приложение Е. Положение «Об организации работы с персональными данными»	158
Приложение Ж. Проект приказа об утверждении об утверждении перечня лиц, доступ которых к персональным данным, обрабатываемым в информационной системе	173

Приложение И. Проект приказа о назначении ответственного за организацию обработки персональных данных в информационной системе персональных данных «Персонал»	175
---	-----

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

В настоящем отчете применяют следующие обозначения и сокращения:

- РФ – Российская Федерация;
- АО «ПО «Электроприбор» – Акционерное общество «Пензенское производственное объединение «Электроприбор»;
- ЧС – чрезвычайная ситуация;
- ПДн – персональные данные;
- КТ – коммерческая тайна;
- КИ – конфиденциальная информация;
- ФИО – фамилия, имя, отчество;
- ЧПУ – числовое программное управление;
- ОС – операционная система;
- БД – база данных;
- КЗ – контролируемая зона;
- ПО – программное обеспечение;
- АРМ – автоматизированное рабочее место;
- ТС – техническое средство;
- ИС – информационная система;
- ФСТЭК – Федеральная служба по техническому и экспортному контролю;
- ИСПДн – информационная система персональных данных;
- ВПО – вредоносное программное обеспечение;
- НСД – несанкционированный доступ;
- УБ – угроза безопасности;
- К – конфиденциальность;
- Ц – целостность;
- Д – доступность;
- ПЭВМ – персональная электронная вычислительная машина;
- ГО – гражданская оборона;

- ИС КТ – информация система информации, составляющей коммерческую тайну;
- ИБ – информационная безопасность;
- ИС КИ – информационная система иной конфиденциальной информации;
- СЗИ – средство защиты информации;
- ФЗ – федеральный закон.

ВВЕДЕНИЕ

В настоящее время в Российской Федерации свою деятельность ведёт множество предприятий и учреждений различных организационных форм, форм собственности и размеров, в информационных системах которых ведётся обработка персональных данных, а также информации, представляющей коммерческую ценность, позволяющая избегать неоправданных расходов, увеличивать прибыль, конкурентоспособность выпускаемой продукции и оказываемых услуг. Стоит отметить, что немалое количество таких организации обрабатывает информацию, не являющейся ни персональными данными, ни коммерческой тайной, но, тем не менее, распространение которой может нанести нежелательный ущерб предприятию.

Защита персональных данных – требование законодательства РФ, защита коммерческой тайны и иной конфиденциальной информации – процедура добровольная, однако для стабильного функционирования организации, избежания лишних финансовых, репутационных и иных потерь, а также поддержания статуса добросовестного исполнителя требований законодательства РФ, необходима защита всех 3-х видов конфиденциальной информации, что подтверждается. Необходимость защиты конфиденциальной информации в коммерческих организациях обусловлена также тем, что по данным всемирного исследования на 2015 год около 72,8% утечек происходит именно на подобных предприятиях и в 90,8% случаев это персональные данные, в 7,5 коммерческая тайна или иная конфиденциальная информация, а наша страна занимает второе место в мире по общему числу утечек.

Обеспечение безопасности конфиденциальной – ресурсоёмкий процесс, требующий, как значительных финансовых, так и временных затрат. Для построения наиболее эффективной системы защиты такой информации очень важно грамотно определить перечень информации, подлежащей защите, описать и определить защищённость информационных систем, в которых такая информация обрабатывается, определить перечни угроз безопасности для каждого вида информации, на основании которого разработать исчерпывающий

перечень защитных мер. Также большое значение имеет грамотный выбор средств, позволяющих реализовать выбранные защитные меры и разработка документации, которая, как определяет цели, задачи и методы обеспечения защиты конфиденциальной информации в целом, так и регламентирует процедуры и действия, реализация которых необходима для обеспечения безопасности отдельных видов информации.

1 Идентификация организационной структуры АО «ПО «Электроприбор»

АО «ПО «Электроприбор» является одним из ведущих предприятий России по изготовлению и поставке средств телекоммуникации и связи специального назначения, которые обеспечивают надежную криптографическую защиту конфиденциальной речевой, документальной, графической информации и применяются на стационарных и подвижных (на колесной и гусеничной базе, на вертолетах, самолетах, космических аппаратах, на надводных и подводных объектах морского базирования) пунктах управления различного назначения. В настоящее время предприятие серийно изготавливает и поставляет:

- комплексы технических средств криптографической защиты, повышения достоверности, передачи/приема и распределения данных;
- аппаратуру криптографической защиты речевой, документальной (от ПЭВМ) и факсимильной информации;
- коммутационное оборудование;
- устройства преобразования сигналов для передачи цифровой информации;
- модемы и мультиплексоры для передачи информации по каналам тональной частоты и основному цифровому каналу [1].

Для наибольшей наглядности было разработано графическое изображение организационной структуры АО «ПО «Электроприбор», представленное на рисунке 1.



Рисунок 1 – Организационная структура АО «ПО «Электроприбор»

Для более точного выявления конфиденциальной информации, обрабатываемой на предприятии, было произведено описание структурных подразделений, приведённых на рисунке 1, в части задач, возложенных на них. Описание цехов и производств не проводилось, так как задачи, решаемые данными структурными единицами, являются узко направленными и прямо вытекают из их названий. Результаты были сведены в таблицу 1.

Таблица 1 – Подразделения предприятия и задачи, решаемые ими

Подразделение	Задачи, решаемые подразделением
Конструкторский отдел	<ul style="list-style-type: none"> – реализация единой политики «АО «ПО Электроприбор» в сфере конструкторских разработок; – осуществление подготовительных мероприятий к производству новой продукции; – обеспечение высокой конкурентоспособности разрабатываемой продукции.
Технологический отдел	<ul style="list-style-type: none"> – модернизация выпускаемой продукции для улучшения ее потребительских свойств и спроса на неё; – разработка и реализация технических мероприятий по снижению всех видов затрат на единицу продукции. – разработка и реализация технических мероприятий по сокращению рабочих мест с вредными и опасными условиями труда.

Продолжение таблицы 1

Подразделение	Задачи, решаемые подразделением
Отдел технической документации	<ul style="list-style-type: none"> – обеспечение руководителей структурных подразделений предприятия необходимой информацией для принятия решений; – обеспечение отдельных структурных подразделений необходимой технической документацией; – обеспечение необходимых условий хранения и оперативного поиска технической информации; – организация обмена технической информацией между структурными подразделениями АО «ПО «Электроприбор».
Отдел маркетинга	<ul style="list-style-type: none"> – оценка конъюнктуры рынка, постоянный анализ результатов коммерческой деятельности предприятия и факторов, на них влияющих; разработка прогнозов продаж и рыночной доли предприятия, проведение ситуационного рыночного анализа; – выработка целей и стратегий рыночной деятельности предприятия на внутреннем и внешнем рынках в целом и в отношении отдельных видов выпускаемой продукции, относительно ценовой политики, выбора рациональных каналов товародвижения и методов продвижения продукции совместно с другими подразделениями предприятия и руководством предприятия; – разработка долгосрочных и текущих планов маркетинга в отношении отдельных видов выпускаемой продукции и всего предприятия в целом; – оперативное информационное обеспечение маркетинговой деятельности предприятия и его подразделений; – выработка рекомендаций по установлению контактов с внешними организациями, представление предприятия в его отношениях с другими организациями, предприятиями.
Отдел информационных технологий	<ul style="list-style-type: none"> – формирование и развитие единой политики в области применения информационных технологий, систем обработки данных, средств телекоммуникации и связи, участие в пределах своей компетенции в обеспечении информационной безопасности предприятия совместно с отделом информационной безопасности.

Продолжение таблицы 1

Подразделение	Задачи, решаемые подразделением
Отдел информационных технологий	<ul style="list-style-type: none"> – внедрение, конфигурирование и сопровождение системы автоматизации управленческой, производственной и учетной деятельности предприятия (информационная система предприятия); – развитие информационной системы предприятия согласно внутренним потребностям и их изменениям, а также внедрение технологических платформ новых поколений; – приведение эксплуатируемых автоматизированных и информационных систем предприятия в соответствие действующему законодательству Российской Федерации и его изменения.
Планово–экономический отдел	<ul style="list-style-type: none"> – формирование единой экономической политики предприятия на основе анализа состояния и тенденций развития отрасли; – экономическое планирование, направленное на эффективное использование ресурсов в процессе производства, реализации продукции и оказания услуг; – анализ экономического состояния предприятия; – формирование ценовой политики в отношении выпускаемой продукции и оказываемых услуг; – разработка перспективных и краткосрочных прогнозов экономического развития предприятия; – контроль за выполнением подразделениями предприятия законодательства в области экономики.
Отдел труда и зарплаты	<ul style="list-style-type: none"> – организация процессов труда и управления на предприятии; – нормирование труда; – организация оплаты и стимулирования труда; – управление затратами на персонал.
Бухгалтерия	<ul style="list-style-type: none"> – ведение достоверного бухгалтерского, налогового и управленческого учета финансово–хозяйственной деятельности предприятия. – формирование и сдача бухгалтерской, налоговой и управленческой отчетности финансово–хозяйственной деятельности предприятия. – взаимодействие с государственными налоговыми и иными органами в пределах своей компетенции. – взаимодействие с контрагентами и финансовыми организациями в пределах своей компетенции

Продолжение таблицы 1

Подразделение	Задачи, решаемые подразделением
Отдел гражданской обороны и чрезвычайных ситуаций	<ul style="list-style-type: none"> – осуществление управления в области гражданской обороны, предупреждения и ликвидации чрезвычайных ситуаций и пожарной безопасности, координации деятельности руководства предприятия в случае ЧС; – разработка и реализация мероприятий по организации и ведению гражданской обороны, защите сотрудников предприятия и его территории от ЧС и пожаров; – осуществление сбора, обработки и обмена информацией в области гражданской обороны, предупреждения и ликвидации чрезвычайных ситуаций природного и техногенного характера и пожарной безопасности; – организация своевременного оповещения и информирования руководства и сотрудников предприятия о проведении мероприятий гражданской обороны, об угрозе возникновения или о возникновении чрезвычайных ситуаций.
Служба охраны труда и экологии	<ul style="list-style-type: none"> – контроль за соблюдением работниками законов и иных нормативных правовых актов по охране труда, коллективного договора, соглашения по охране труда, других локальных нормативных правовых актов предприятия, инструкций по охране труда; организация профилактической работы по предупреждению производственного травматизма, профессиональных заболеваний и заболеваний, обусловленных производственными факторами, а также работы по улучшению условий труда; – информирование и консультирование работников предприятия, в том числе ее руководителя, по вопросам охраны труда; – реализация мероприятий по охране окружающей среды от факторов, возникающих в процессе деятельности предприятия.
Отдел кадров	<ul style="list-style-type: none"> – подбор и расстановка кадров; – учёт личного состава и ведение кадровой документации; – контроль соблюдения дисциплины труда; – формирование кадрового резерва; – контроль и соблюдение трудовых и социальных прав работника.

Продолжение таблицы 1

Подразделение	Задачи, решаемые подразделением
Юридический отдел	<ul style="list-style-type: none"> – контроль за исполнением документов, договоров, контрактов и подготовка к их передаче в архив; – проведение консультаций по вопросам юридического характера, возникающим в процессе деятельности предприятия и его отдельных подразделений; – участие, в пределах своей компетенции, в мероприятиях по подготовке и заключению договоров с другими организациями и предприятиями.
Канцелярия	<ul style="list-style-type: none"> – разработка, в пределах своей компетенции, мероприятий по совершенствованию и оптимизация системы документооборота в организации; – организационно–методическое руководство, координация и контроль деятельности структурных подразделений организации по вопросам делопроизводства и архивного дела; – подготовка и оформление документов в соответствии с действующими стандартами и правилами; – контроль над прохождением и исполнением документов в организации; – разработка предложений и мероприятий по внедрение новых методов организации делопроизводства, в том числе на основе использования современных информационных технологий.
Отдел снабжения	<ul style="list-style-type: none"> – обеспечение производственных подразделений предприятия материально–техническими ресурсами; участие, в пределах своей компетенции, в подготовке и заключении договоров на поставку материально–технических ресурсов; – организация рационального использования материально–технических ресурсов.
Отдел информационной безопасности	<ul style="list-style-type: none"> – разработка, планирование, реализация мероприятий, координация работ всех подразделений и служб по комплексной защите информации на предприятии; – контроль и оценка эффективности принятых мер и применяемых средств защиты информации на предприятии.

2 Выявление конфиденциальной информации, обрабатываемой на предприятии

В структурных подразделениях АО «ПО «Электроприбор» происходит обработка следующих видов конфиденциальной информации:

- ПДн работников предприятия (ПДн);
- информация, составляющая КТ АО «ПО «Электроприбор» (КТ);
- информация, не являющаяся ПДн и КТ, распространение которой ограничено нормативными актами АО «ПО «Электроприбор» и вышестоящих организаций (КИ).

В таблице 2 приведено соотношение структурных подразделений АО «ПО «Электроприбор», вида и содержания конфиденциальной информации в них обрабатываемой.

Таблица 2 – Конфиденциальная информация, обрабатываемая в подразделениях АО «ПО «Электроприбор»

Подразделение	Вид конфиденциальной информации	Содержание конфиденциальной информации
Бухгалтерия	ПДн	<ul style="list-style-type: none">– ФИО, дата и место рождения;– паспортные данные (серия, номер, дата выдачи и иные паспортные данные.);– сведения о заработной плате (номер счёта для расчета с работниками, данные зарплатных договоров с клиентами, в том числе номера их спецкартсчетов, данные по окладу, надбавкам, долгам);– сведения о номере и серии страхового свидетельства государственного пенсионного страхования;– сведения об идентификационном номере налогоплательщика;

Продолжение таблицы 2

Подразделение	Вид конфиденциальной информации	Содержание конфиденциальной информации
Бухгалтерия	ПДн	<ul style="list-style-type: none"> – сведения о соц. льготах и о социальном статусе (серия, номер, дата выдачи, наименование органа, выдающего документ, являющийся основанием для предоставления льгот и статус, и другие сведения); – сведения о временной нетрудоспособности работника.
Отдел кадров	ПДн	<ul style="list-style-type: none"> – ФИО, дата и место рождения; – паспортные данные (серия, номер, дата выдачи и т. д.); – номера телефонов (моб и дом), в случае их регистрации на работника или по адресу его места жительства (по паспорту); – сведения об образовании, квалификации, наличии спец. Знаний или спец. Подготовки (серия, номер, дата выдачи диплома, свидетельства, аттестата или другого документа об окончании образовательного учреждения, в том числе наименование и местоположение образовательного учреждения, дата начала и завершения обучения, факультет или отделение, квалификация и специальность по окончании образовательного учреждения, учёная степень, учёное звание, владение иностранным языком);

Продолжение таблицы 2

Подразделение	Вид конфиденциальной информации	Содержание конфиденциальной информации
Отдел кадров	ПДн	<ul style="list-style-type: none"> – сведения о повышении квалификации и переподготовке (серия, номер, дата выдачи документа о повышении квалификации или о переподготовке, наименовании и местоположение образовательного учреждения, дата начала и завершения обучения, квалификация и специальность по окончании образовательного учреждения); – сведения о трудовой деятельности (данные о трудовой занятости на текущее время с полным указанием должности, подразделения, организации и ее наименовании, ИНН, адрес и телефон, а также реквизитов других организаций с полным наименованием занимаемых ранее в них должностей и времени работы в этих организациях); сведения о номере, серии и дате выдачи трудовой книжки и записях в неё.
Отдел труда и зарплаты	ПДн	<ul style="list-style-type: none"> – ФИО, дата и место рождения; – сведения о трудовой деятельности (данные о трудовой занятости на текущее время с полным указанием должности, подразделения, организации и её наименования, ИНН, адрес и телефон, а также реквизитов других организаций с полными наименованиями занимаемых ранее в них должностей и времени работы в этих организациях, а также другие сведения.

Продолжение таблицы 2

Подразделение	Вид конфиденциальной информации	Содержание конфиденциальной информации
Отдел труда и зарплаты	ПДн	<ul style="list-style-type: none"> – сведения, указанные в оригинальных и копиях приказов по личному составу организации и материалах к ним; – сведения о заработной плате (данные по окладу, надбавкам, премиям); – табельный номер работника организации.
Конструкторский отдел	КТ	<ul style="list-style-type: none"> – схемы и чертежи, а также любые сведения о новых разработках; – алгоритмы (в т.ч. блок-схемы) разработанного и вновь разрабатываемого ПО; – исходные коды разработанного и вновь разрабатываемого ПО.
Технологический отдел	КТ	– сводные сведения о новых (перспективных) технологиях и конструктивных решениях, разработанных организацией и используемых при проектировании и изготовлении продукции.
	КИ	<ul style="list-style-type: none"> – архив технологических процессов – сведения о конфигурации ПО для фрезерных станков с ЧПУ; – сведения о конфигурации ПО для станков с ЧПУ по листообработке; – сведения о конфигурации ПО для гравировочных станков с ЧПУ; – сведения о конфигурации ПО для станков с ЧПУ токарной обработки.
Отдел технической документации	КТ	– техническая документация на изготавливаемые изделия.
	КИ	<ul style="list-style-type: none"> – архив технической документации; – информация на электронных носителях, хранящихся в архиве; – архив конструкторской документации.

Продолжение таблицы 2

Подразделение	Вид конфиденциальной информации	Содержание конфиденциальной информации
Юридический отдел	КТ	<ul style="list-style-type: none"> – сведения о заключаемых договорах (кроме подлежащих опубликованию в соответствии с положением о гос. закупках); – сведения об организациях и предприятиях, с которыми были заключены и планируется заключение договоров.
Канцелярия	КТ	– сведения о порядке, методах и средствах ведения делопроизводства на предприятии.
Отдел снабжения	КТ	<ul style="list-style-type: none"> – уровень запасов, материалов и комплектующих; – данные о резервах сырья на предприятии.
Бухгалтерия	КТ	<ul style="list-style-type: none"> – бухгалтерская отчётность до её официального опубликования в соответствии с законодательством РФ; – прибыль предприятия и направления её использования; – сведения о финансовых операциях предприятия; – размеры и условия банковских кредитов; – развёрнутые сведения стоимости, основных и оборотных фондов предприятия.
Планово–экономический отдел	КТ	<ul style="list-style-type: none"> – стратегические и тактические планы по развитию предприятия; – сведения о планах предприятия по расширению производства и другие коммерческие замыслы; – сведения, раскрывающие плановые и фактические показатели финансового плана, не содержащиеся в открытых источниках.

Продолжение таблицы 2

Подразделение	Вид конфиденциальной информации	Содержание конфиденциальной информации
Планово–экономический отдел	КТ	– плановая себестоимость, объемы производства; – прибыль предприятия и направления её использования.
Отдел гражданской обороны и ЧС	КТ	– схема систем пожаротушения и сигнализации.
	КИ	– сведения о состоянии ГО и ПБ.
Отдел маркетинга	КТ	– отчёты о собственных маркетинговых исследованиях рынка; – сведения о конкретных направлениях в торговой политике; – сведения об объемах реализации;
Отдел информационных технологий	КТ	– настройки и конфигурации серверного, сетевого и каналобразующего оборудования ЛВС организации; – стратегические и тактические планы развития сетевой инфраструктуры; – сведения о рисках и уязвимостях АС.
	КИ	– личные пароли пользователей и административные пароли доступа к ОС, прикладным системам, БД, сетевому и каналобразующему оборудованию; – положение о порядке пользования сетью интернет на предприятии; – положение о резервном копировании БД; – сведения о программах собственной разработки на базе 1С: предприятие.

Продолжение таблицы 2

Подразделение	Вид конфиденциальной информации	Содержание конфиденциальной информации
Отдел информационной безопасности	КТ	<ul style="list-style-type: none"> – регламенты, планы, задания подразделения обеспечения безопасности информации; – информация о состоянии систем защиты информации в организации; – сведения о структуре, принципах и технических решениях, используемых в системах обеспечения безопасности информации; – сведения о местах, порядке хранения документов, содержащих сведения, составляющие коммерческую тайну, а также их учёте; – секретные (закрытые) ключи электронной цифровой подписи и порядок их учёта, хранения.
	КИ	<ul style="list-style-type: none"> – личные пароли пользователей и административные пароли доступа к ОС, прикладным системам, БД, сетевому и каналообразующему оборудованию.
Производство энергетическое	КТ	<ul style="list-style-type: none"> – схемы систем отопления и кондиционирования (за исключением схем отопления для выделенных помещений (ВП), объектов информатизации (ОИ) и без привязки к схеме КЗ); – схема систем электропитания (для отдельных помещений и без привязки к схеме КЗ).
	КИ	<ul style="list-style-type: none"> – сведения об используемом оборудовании, его показателях и состоянии; – сведения о мощностях отдельных видов энергетического производства для нужд предприятия.

Продолжение таблицы 2

Подразделение	Вид конфиденциальной информации	Содержание конфиденциальной информации
Механо–сборочное производство	КТ	– сведения о производственных возможностях; – данные о типе и размещении оборудования.
Монтажно–сборочное производство	КТ	– сведения о производственных возможностях; – данные о типе и размещении оборудования.
	КИ	– сведения о конфигурации используемого ПО.
Производство мелких серий	КТ	– сведения о производственных возможностях; – данные о типе и размещении оборудования.
	КИ	– сведения по комплектованию изделий деталями и сборочными единицами; – сведения о трудоёмкости производства.
Цех ремонтно–строительный	КИ	– проекты на реконструкцию и техническое перевооружение предприятия.
Служба охраны труда и экологии	КИ	– сводные сведения об очистных сооружениях и оборудовании используемом при реализации мероприятий по охране окружающей среды; – планы по улучшению условий охраны труда; – сведения о требуемых для нужд предприятия средствах индивидуальной защиты и их количестве.

3 Определение значимости выявленной информации

Критерием определения значимости для ПДн, обрабатываемых в подразделениях АО «ПО «Электроприбор» является их категория в соответствии с ФЗ № 152 «О персональных данных». Выделяются следующие категории ПДн:

- ПДн, включаемые с согласия их субъекта в общедоступные источники персональных данных (ПДн–О);
- ПДн специальной категории – ПДн, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни (ПДн–С);
- биометрические ПДн – сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных (ПДн–Б);
- иные категории ПДн – ПДн не являющиеся биометрическими, специальных категорий и, не входящие в общедоступные источники ПДн (ПДн–И).

Для определения значимости (ценности) информации, составляющей коммерческую тайну АО «ПО «Электроприбор» в организации принято делить такую информацию на 2 группы:

- 1 группа – сведения, разглашение которых влечет за собой существенный экономический ущерб во всех сферах и направлениях деятельности организации;
- 2 группа – сведения, разглашение которых приводит к экономическому ущербу в отдельной сфере (нескольких сферах) или направлениях деятельности организации.

Для определения значимости конфиденциальной информации, являющейся собственностью АО «ПО «Электроприбор», в организации принято, делить данный вид информации, также, как и КТ на 2 группы:

– 1 группа – сведения, разглашение которых влечет за собой существенный ущерб любого характера (материального и не материального) во всех сферах и направлениях деятельности организации;

– 2 группа – сведения, разглашение которых приводит к ущербу любого характера (материального и не материального) в отдельной сфере (нескольких сферах) или направлениях деятельности организации.

С учётом приведенных выше критериев для каждого вида конфиденциальной информации было проведено сопоставление уровня значимости конкретных пунктов такой информации. В таблице А.1 приложения А приведено категорирование персональных данных, обрабатываемых в некоторых подразделениях АО «ПО «Электроприбор».

По результатам определения уровней значимости ПДн был сделан вывод, что в АО «ПО «Электроприбор» практически все ПДн имеют категорию иные. Безопасность данной категории конфиденциальной информации должна быть обеспечена в соответствии с требованиями законодательства РФ.

Результаты определения уровней значимости информации, составляющей коммерческую тайну АО «ПО «Электроприбор» приведены в таблице А.2 приложения А.

По результатам определения уровня значимости (ценности) информации, составляющей коммерческую тайну АО «ПО «Электроприбор», был сделан вывод, что более 50% сведений данного характера относятся к 1 группе значимости, таким образом необходимо уделить особое внимание обеспечению информационной безопасности таких сведений ввиду их высокой коммерческой ценности.

Результаты определения уровней значимости информации, не являющейся ПДн и КТ, распространение которой ограничено нормативными актами АО «ПО «Электроприбор» и вышестоящих организаций приведены в таблице А.3 приложения А.

По результатам определения уровня значимости конфиденциальной информации АО «ПО «Электроприбор» был сделан вывод, что практически все сведения данного характера относятся ко 2 группе значимости, таким образом безопасность данной информации должна быть обеспечена на приемлемом уровне.

4 Оценка исходной защищённости информационных систем АО «ПО «Электроприбор»

4.1 Оценка исходной защищённости информационной системы персональных данных «Персонал» АО «ПО «Электроприбор»

4.1.1 Определение масштабов ИС

4.1.1.1 Описание процесса обработки персональных данных и структуры информационной системы персональных данных «Персонал»

Для описания процесса обработки персональных данных в АО «ПО «Электроприбор» была разработана модель IDF0, диаграмма которой представлена на рисунке 2.



Рисунок 2 – Описание процесса обработки ПДн сотрудников предприятия

При приеме сотрудника на работу осуществляется сбор его ПДн, который производится в соответствии с ФЗ – 152 РФ «О персональных данных» и главой 14 ТК РФ. Дальнейшее хранение осуществляется в соответствии с ФЗ – 152 РФ «О персональных данных». Сотрудник отдела кадров со своего АРМ с использованием программы «1С: Кадры» заносит ПДн в базу данных сотрудников предприятия. Информация циркулирует по ИС только в

электронном виде, разрывы автоматизированной обработки информации отсутствуют.

Для учёта часов, отработанных в течение месяца работниками АО «ПО «Электроприбор» и начисления за эти часы зарплаты сотрудники подразделения «Отдел труда и зарплаты» с использованием программ «1С: Зарплата» и «1С: Учёт рабочего времени» вносят необходимые данные в соответствующие базы данных. Информация циркулирует по ИС только в электронном виде, разрывы автоматизированной обработки информации отсутствуют.

Для выплаты работникам АО «ПО «Электроприбор» заработной платы сотрудники Бухгалтерии с использованием программы «1С: Зарплата» получают сведения о конкретном работнике и его заработной плате, начисленной по итогам месяца, а также осуществляют печать платёжного документа. Информация циркулирует по ИС в электронном виде, при осуществлении печати платёжного документа возникает разрыв автоматизированной обработки информации.

Далее было разработано графическое изображение структуры ИСПДн «Персонал» АО «ПО «Электроприбор» с отображением технических средств обработки информации и телекоммуникационного оборудования, входящих в состав ИСПДн, а также физических связей между ними, приведена на рисунке 3.

Далее была произведена описание технических средств, используемого системного и прикладного программного обеспечения, а также определение ответственных за конкретное ТС, а также полномочий пользователей подразделения в отношении описываемых ТС. АРМ сотрудников отдела кадров, АРМ сотрудников бухгалтерии и АРМ сотрудников отдела труда и зарплаты имеют идентичную конфигурацию, поэтому производилось описание только 1 ТС на подразделение. Результаты приведены в таблице 3.

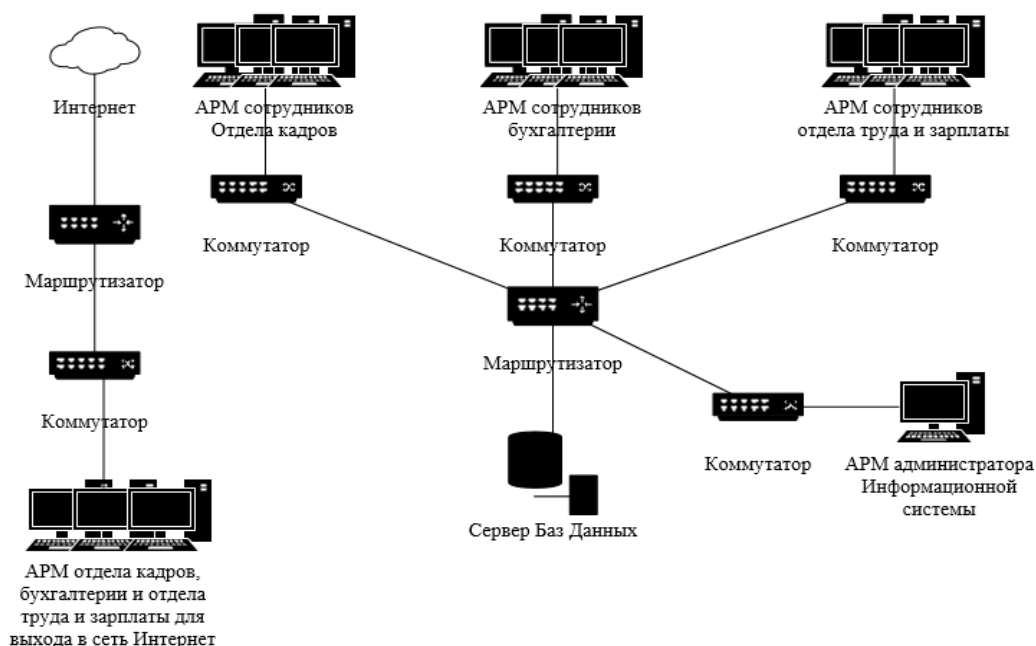


Рисунок 3 – Структура ИСПДн «Персонал»

Таблица 3 – Перечень ТС, ПО и ответственных лиц

Техническое средство (ТС)	Установленное ПО	Ответственный за ТС	Пользователь (полномочия)
АРМ сотрудника бухгалтерии	Microsoft Windows 7 Service Pack, Microsoft SQL Server 2012, Антивирус Касперского 8.0 для Windows, «1С: Зарплата», пакет Microsoft Office 2007	сотрудник, использующий данное АРМ в повседневной деятельности	разрешено использовать АРМ в объемах, необходимых для выполнения должностных обязанностей (использование в служебных целях), запрещено изменять конфигурацию АРМ
АРМ сотрудника отдела кадров	Microsoft Windows 7 Service Pack, Microsoft SQL Server 2012, Антивирус Касперского 8.0 для Windows, «1С: Кадры», пакет Microsoft Office 2007	сотрудник, использующий данное АРМ в повседневной деятельности	разрешено использовать АРМ в объемах, необходимых для выполнения должностных обязанностей (использование в служебных целях), запрещено изменять конфигурацию АРМ

Продолжение таблицы 3

Техническое средство (ТС)	Установленное ПО	Ответственный за ТС	Пользователь (полномочия)
АРМ сотрудника отдела труда и зарплаты	Microsoft Windows 7 Service Pack, Microsoft SQL Server 2012, Антивирус Касперского 8.0 для Windows, «1С: Зарплата», «1С: Учёт рабочего времени», пакет Microsoft Office 2007	сотрудник, использующий данное АРМ в повседневной деятельности	разрешено использовать АРМ в объёмах, необходимых для выполнения должностных обязанностей (использование в служебных целях), запрещено изменять конфигурацию АРМ
Цифровой Коммутатор Cisco IE- 3000- 8ТС- E	–	администратор ИС	–
АРМ Администратора ИС	Microsoft Windows Server 2008 Standard Edition (SP2), Microsoft SQL Server 2012, Антивирус Касперского 8.0 для Windows Servers Enterprise Edition, пакет Microsoft Office 2007	администратор АС	разрешено изменять конфигурацию и состав всех ТС ИС
АРМ для доступа в сеть интернет	Microsoft Windows 7 Service Pack, Kaspersky Internet Security 2016, пакет Microsoft Office 2007	руководитель соответствующего подразделения	разрешено использовать АРМ в объёмах, необходимых для выполнения должностных обязанностей (использование в служебных целях), запрещено изменять конфигурацию АРМ
Маршрутизатор Cisco 1841	–	администратор ИС	–

Затем была разработана структура информационных потоков в ИСПДн «Персонал» АО «ПО «Электроприбор». Для большей наглядности графического изображения, которое представлено на рисунке 4. На нем не отображалось телекоммуникационное оборудование и физические связи между ТС. АРМ для доступа в сеть интернет является вспомогательным техническим средством описываемой ИС, на данном АРМ не осуществляется обработка ПДн

сотрудников АО «ПО «Электроприбор», таким образом ИСПДн «Персонал» не имеет подключения к сетям общего пользования.

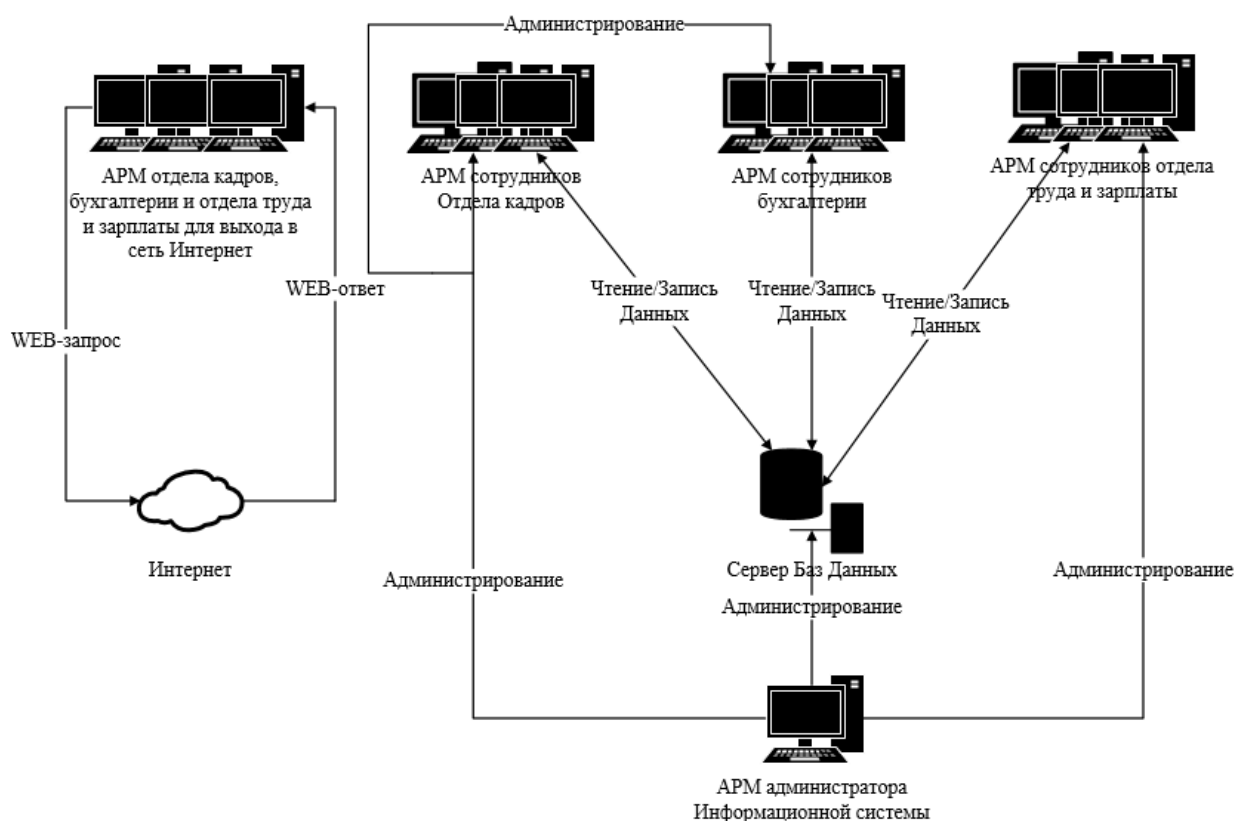


Рисунок 4 – Структура информационных потоков в ИС подразделений, ведущих обработку ПДн в АО «ПО «Электроприбор»

4.1.1.2 Определение условий создания и использования персональных данных

В соответствии с частью 3 статьи 5 главы 2 ФЗ №152 «О персональных данных» не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой. Для проверки отсутствия данного факта в ИСПДн «Персонал» на основании модели IDF0 процесса обработки ПДн сотрудников предприятия были определены цели и основания обработки персональных данных работников предприятия. Результаты представлены в таблице 4.

Таблица 4 – Цели и основания обработки ПДн в АО «ПО «Электроприбор»

Содержание ПДн	Цель обработки ПДн	Основание для обработки ПДн	Вид обработки
<ul style="list-style-type: none"> – ФИО, дата и место рождения; – паспортные данные (серия, номер, дата выдачи и т. д.); – номера телефонов (моб и дом), в случае их регистрации на работника или по адресу его места жительства (по паспорту); – сведения об образовании, квалификации, наличии спец. Знаний или спец. Подготовки (серия, номер, дата выдачи диплома, свидетельства, аттестата или другого документа об окончании образовательного учреждения, в том числе наименование и местоположение образовательного учреждения, дата начала и завершения обучения, факультет или отделение, квалификация и специальность по окончании образовательного учреждения, учёная степень, учёное звание, владение иностранным языком). 	ведение кадрового делопроизводства.	трудовые отношения между работником и АО «ПО «Электроприбор» (ст. 16 ТК РФ).	смешанная
<ul style="list-style-type: none"> – ФИО, дата и место рождения; – паспортные данные (серия, номер, дата выдачи и иные паспортные данные.); – сведения о заработной плате (номер счёта для расчета с работниками, данные зарплатных договоров с клиентами, в том числе номера их спецкартсчетов, данные по окладу, надбавкам, долгам); – сведения о номере и серии страхового свидетельства государственного пенсионного страхования; – сведения об идентификационном номере налогоплательщика; 	выплата заработной платы, осуществление налоговых и пенсионных отчислений, начисление льгот.		

Продолжение таблицы 4

Содержание ПДн	Цель обработки ПДн	Основание для обработки ПДн	Вид обработки
<ul style="list-style-type: none"> – сведения о соц. льготах и о социальном статусе (серия, номер, дата выдачи, наименование органа, выдающего документ, являющийся основанием для предоставления льгот и статус, и другие сведения); – сведения о временной нетрудоспособности работника. 	выплата заработной платы, осуществление налоговых и пенсионных отчислений, начисление льгот.	трудовые отношения между работником и АО «ПО «Электроприбор» (ст. 16 ТК РФ).	смешанная
<ul style="list-style-type: none"> – ФИО, дата и место рождения; сведения о трудовой деятельности (данные о трудовой занятости на текущее время с полным указанием должности, подразделения, организации и её наименования, ИНН, адрес и телефон, а также реквизитов других организаций с полными наименованиями занимаемых ранее в них должностей и времени работы в этих организациях, а также другие сведения; – сведения, указанные в оригинальных и копиях приказов по личному составу организации и материалах к ним; – сведения о заработной плате (данные по окладу, надбавкам, премиям); табельный номер работника организации. 	учёт рабочего времени, начисление заработной платы, премий, надбавок.		

На основании структуры и категории ПДн, целей и оснований их обработки была разработана матрица доступа к ПДн АО «ПО «Электроприбор», то есть были определены лица, допущенные к ПДн на законном основании, а также перечень действий с ПДн, разрешённых им. Это обусловлено тем, что ПДн сотрудников предприятия являются неотъемлемой частью ИСПДн, следовательно, перечень групп и лиц, а также их количества, допущенных к ПДн влияет на масштабы ИСПДн. С целью обеспечения конфиденциальности ПДн

сотрудников АО «ПО «Электроприбор» их фамилия, имя и отчество были заменены на цифровые идентификаторы. Результат представлен в таблице 5.

Таблица 5 – Матрица доступа к ПДн АО «ПО «Электроприбор»

Группа	Уровень доступа к ПДн	Разрешённые действия	Сотрудники
Администраторы ИСПДн	<ul style="list-style-type: none"> – обладает полной информацией о системном и прикладном программном обеспечении ИСПДн; – обладает полной информацией о технических средствах и конфигурации ИСПДн; – имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн; – обладает правами конфигурирования и административной настройки технических средств ИСПДн; – обладает правами конфигурирования и административной настройки системного и прикладного программного обеспечения ИСПДн. 	<ul style="list-style-type: none"> – сбор; – систематизация; – накопление; – хранение; – использование; – уничтожение. 	администратор: №1221, №1222 №1223
Операторы ИСПДн с правами чтения и записи	обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ к ПДн сотрудников организации.	<ul style="list-style-type: none"> – сбор; – систематизация; – накопление; – хранение; – уточнение; – использование. 	оператор отдела кадров: №1081, №1082, №1083, №1084, №1805, №1806, №1807, №1808, №1809, №1810
			сотрудники бухгалтерии: №1371, №1372, №1373, №1374, №1375
			сотрудники отдела труда и зарплаты: №1181, №1182, №1183, №1184, №1185, №1186, №1187

Продолжение таблицы 5

Группа	Уровень доступа к ПДн	Разрешённые действия	Сотрудники
Сотрудники прокуратуры	обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ к ПДн сотрудников и клиентов, для осуществления прокурорского надзора (отрасли прокурорского надзора сформулированы в ч.2 ст.1 Закона о прокуратуре РФ, а также общего надзора.	– сбор; – систематизация; – накопление; – хранение; – использование; – уточнение.	
Сотрудники Роскомнадзора	обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ к ПДн сотрудников и клиентов, для осуществления защиты прав субъектов ПДн в соответствии со ст.22– 23 Закона о персональных данных	– сбор; – систематизация; – уточнение; – хранение; – уничтожение.	
Сотрудники ФСБ	обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ к ПДн сотрудников и клиентов, для осуществления оперативно–разыскной деятельности.	– сбор; – систематизация; – накопление; – хранение; – использование; – уточнение.	

4.1.2 Составление перечня угроз информационной безопасности

Составление перечня угроз информационной безопасности для ИСПДн «Персонал» производилось на основании документа ФСТЭК от 15.02.2008 «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» [2]. ИСПДн была определена как локальная ИС, не имеющая подключения к сетям общего пользования и международного обмена. Согласно упомянутой выше модели, в данной ИСПДн возможна реализация следующих УБ ПДн:

- угроз утечки информации по техническим каналам;
- угроз НСД к ПДн, обрабатываемым в автоматизированном рабочем месте.

Угрозы утечки информации по техническим каналам включают в себя:

- угрозы утечки акустической (речевой) информации;
- угрозы утечки видовой информации;
- угрозы утечки информации по каналу ПЭМИН.

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

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

Угрозы утечки информации по каналу ПЭМИН возможны из–за наличия электромагнитных излучений, в основном, монитора и системного блока компьютера. Основную опасность представляют угрозы утечки из–за наличия электромагнитных излучений монитора.

Угрозы НСД в автономном АРМ связаны с действиями нарушителей, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующих угрозы непосредственно в ИСПДн. Кроме этого, источниками угроз НСД к информации в АРМ могут быть аппаратные закладки и отчуждаемые носители вредоносных программ.

В ИСПДн на базе автономного АРМ возможны все виды уязвимостей ИСПДн, за исключением уязвимостей, связанных с реализацией протоколов сетевого взаимодействия и каналов передачи данных. В таких ИСПДн возможны:

- угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой;

– угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) операционной системы или какой-либо прикладной программы (например, системы управления базами данных), с применением специально созданных для выполнения НСД программ (программ просмотра и модификации реестра, поиска текстов в текстовых файлах и т.п.);

– угрозы внедрения вредоносных программ.

Из типовой модели угроз были исключены угрозы утечки по каналу ПЭМИН, так как все ТС обработки ПДн и каналы их соединяющие расположены на территории АО «ПО «Электроприбор», на предприятии действует пропускной режим, препятствующий внешнему нарушителю – источнику данной угрозы получить доступ к ТС и каналам, их соединяющим. Также исключение данного типа угроз обусловлено тем, что для их реализации необходимы существенные материальные затраты на приобретение соответствующего оборудования, а также высококвалифицированные специалисты.

Также были исключены угрозы реализуемые в ходе загрузки ОС, так как для их реализации необходим физический доступ к АРМ, а источников угрозы является внешний нарушитель. На предприятии реализован контрольно-пропускной режим, посторонним лицам проход запрещён.

На основе Типовой модели угроз было произведено описание факторов угроз безопасности ПДн с добавлением и описанием угроз, возможных в данной ИСПДн, но не описанных в Типовой модели. Результаты представлены в таблице 6.

Таблица 6 – Описание факторов угроз

№ п/п	Описание угрозы	Источник угрозы	Нарушаемые свойства	Объекты воздействия	Уязвимость
1	Утечка видовой информации	внутренние (персонал, не имеющий доступа к защищаемой информации)	К	ПДн, обрабатываемые на АРМ ИСПДн	–не выключение экрана монитора при оставлении рабочего места; –расположение мониторов, позволяющее осуществить несанкционированный просмотр информации.
2	Кража носителей информации	внутренние (персонал, имеющий доступ к защищаемой информации) внутренние (персонал, имеющий доступ в КЗ, но не имеющий доступ к защищаемой информации)	К, Ц, Д	ПДн, содержащиеся на электронном и бумажном носителе информации	–слабость мер учёта и хранения носителей информации; –халатность персонала, ответственного за те или иные носители информации; –отсутствие механизмов резервного копирования информации.
3	Уничтожение информации и её носителей	внутренние (персонал, имеющий доступ к защищаемой информации; персонал, осуществляющий администрирование ИСПДн).	Ц, Д	ПДн, обрабатываемые на АРМ и сервере БД; ПДн, содержащиеся на электронном и бумажном носителе информации	– слабость мер учёта и хранения носителей информации; – отсутствие механизмов резервного копирования информации;

Продолжение таблицы 6

№ п/п	Описание угрозы	Источник угрозы	Нарушаемые свойства	Объекты воздействия	Уязвимость
3	Уничтожение информации и её носителей	внутренние (персонал, имеющий доступ к КЗ, но не имеющий доступ к защищаемой информации)	Ц, Д	ПДн, обрабатываемые на АРМ и сервере БД; ПДн, содержащиеся на электронном и бумажном носителе информации.	– наличие у пользователя прав доступа, позволяющих реализовать данную угрозу; отсутствие механизма контроля целостности.
4	Вывод из строя узлов ПЭВМ, каналов связи, телекоммуникационного оборудования	внутренние (персонал, имеющий доступ к защищаемой информации; персонал, осуществляющий администрирование ИСПДн)	Ц, Д	ПДн, обрабатываемые на АРМ и сервере БД; информация, циркулирующая по внутренним коммуникациям ЛВС ИСПДн	– отсутствие мер по предотвращению бесконтрольного доступа к системным блокам ПЭВМ и другим устройствам; – небрежная прокладка каналов связи; – отсутствие аппаратного резервирования критически важных узлов и средств
		внутренние (персонал, имеющий доступ к КЗ, но не имеющий доступ к защищаемой информации)			
5	Несанкционированное отключение средств защиты	внутренние (персонал, осуществляющий администрирование ИСПДн)	К, Ц	ПДн, обрабатываемые на АРМ и сервере БД	–недостаточность контроля за действиями администратора; –чрезмерное сосредоточение привилегий у одного лица.
6	Угроза внедрения кода или данных	внутренние	Ц, Д	ПДн, обрабатываемые на АРМ и сервере БД	–недостаточный уровень осведомлённости персонала; –неактуальные базы данных признаков ВПО.

Продолжение таблицы 6

№ п/п	Описание угрозы	Источник угрозы	Нарушаемые свойства	Объекты воздействия	Уязвимость
7	Установка ПО, не связанного с использованием в целях выполнения должностных обязанностей	внутренние	Ц, Д	ПДн, обрабатываемые на АРМ и сервере БД	–недостаточный уровень осведомленности и квалификации; –наличие прав доступа, позволяющих устанавливать ПО.
8	Утрата ключей и атрибутов доступа	внутренние	Д	ПДн, обрабатываемые на АРМ и сервере БД	недостаточный уровень осведомления, квалификации.
9	Непреднамеренная модификация (уничтожение) данных	внутренние (персонал, имеющий доступ к защищаемой информации; персонал, осуществляющий администрирование ИСПДн)	Ц	ПДн, обрабатываемые на АРМ и сервере БД	–недостаточный уровень обучения или квалификации; –отсутствие механизмов резервного копирования данных; –отсутствие механизма контроля целостности.
10	Непреднамеренное отключение средств защиты	внутренние (персонал, осуществляющий администрирование ИСПДн)	Ц, Д	ПДн, обрабатываемые на АРМ и сервере БД	–недостаточный уровень обучения или квалификации; –наличие соответствующих привилегий.
11	Выход из строя аппаратных и программных средств	внутренние (персонал, осуществляющий администрирование ИСПДн)	Д, Ц	ПДн, обрабатываемые на АРМ и сервере БД	–несвоевременное или халатное обслуживание аппаратно–программных средств;

Продолжение таблицы 6

№ п/п	Описание угрозы	Источник угрозы	Нарушаемые свойства	Объекты воздействия	Уязвимость
11	Выход из строя аппаратных и программных средств	внутренние (персонал, осуществляющий администрирование ИСПДн)	Д, Ц	ПДн, обрабатываемые на АРМ и сервере БД	–отсутствие аппаратного резервирования критических узлов системы; –отсутствие процедур резервирования программного обеспечения.
12	Разглашение ПДн	внутренние (персонал, имеющий доступ к защищаемой информации)	К	ПДн, обрабатываемые на АРМ и сервере БД	–недостаточный уровень осведомлённости, обучения.
13	Утрата носителей информации и содержащейся на них информации	внутренние (персонал, имеющий доступ к защищаемой информации)	К, Ц, Д	ПДн, содержащиеся на электронном и бумажном носителе информации	–слабость мер учёта и хранения носителей информации; –отсутствие механизмов резервного копирования.
14	Несанкционированное копирование БД ПДн или её частей	внутренние (персонал, имеющий доступ к защищаемой информации)	К	ПДн, обрабатываемые на АРМ и сервере БД	отсутствие механизмов, препятствующих несанкционированному копированию данных
		внутренние (персонал, осуществляющий администрирование ИСПДн)	К	ПДн, обрабатываемые на АРМ и сервере БД	
15	Обход некорректно настроенных механизмов аутентификации	внутренние (персонал, не имеющий доступ к защищаемой информации)	К, Ц, Д	ПДн, обрабатываемые на АРМ и сервере БД	отсутствие или слабость паролей для входа в систему.

Продолжение таблицы 6

№ п/п	Описание угрозы	Источник угрозы	Нарушаемые свойства	Объекты воздействия	Уязвимость
16	Модификация данных	внутренние (персонал, имеющий доступ к защищаемой информации)	Ц	ПДн, обрабатываемые на АРМ и сервере БД	отсутствие механизмов контроля целостности и резервного копирования.

4.1.3 Идентификация актуальных угроз информационной безопасности

Определение актуальности угроз, описанных в п. 4.1.2 настоящего отчёта, проводилось на основании документа ФСТЭК от 14.02.2008 «Методика определения актуальных безопасности персональных данных при их обработке в информационных системах персональных данных» [3]. Первоначально на основании технических и эксплуатационных характеристик ИСПДн был определён уровень её исходной защищённости, результат приведён в таблице 7. Таблица 7 – Показатели исходной защищённости

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности
1. По территориальному размещению: локальная ИСПДн, развернутая в пределах одного здания	высокий
2. По наличию соединения с сетями общего пользования: ИСПДн, физически отделенная от сети общего пользования	высокий
3. По встроенным (легальным) операциям с записями баз персональных данных: запись, удаление, сортировка;	средний
4. По разграничению доступа к персональным данным: ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн;	средний
5. По наличию соединений с другими базами ПДн иных ИСПДн: ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн	высокий

Продолжение таблицы 7

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности
6. По уровню обобщения (обезличивания) ПДн: ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)	низкий
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки: ИСПДн, не предоставляющая никакой информации;	высокий

Исходная защищённость ИСПДн определялась следующим образом:

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

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

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

ИСПДн – «Персонал» был присвоен «Средний» уровень исходной защищённости, так как 71% показателей соответствуют уровню «высокий», и оставшиеся 2 показателя имеют уровни «Средний» и «Низкий», что не позволяет присвоен «высокий» уровень исходной защищённости. Показатель Y_1 равен 5.

Далее для каждой угрозы были определены коэффициенты Y_2 , отражающие вероятность проявления угрозы. Определение коэффициентов проводилось экспертным методом на основе принципа «разумного пессимизма»,

то есть при оценке брался во внимание наихудший вариант развития событий, потенциально способствующий проявлению УБ ПДн.

Угрозе № 1 был присвоен показатель средняя вероятность и, соответствующий ему, численный коэффициент Y_2 равный 5, так как в течение рабочего дня сотрудник может несколько раз покидать своё рабочее по служебной необходимости, а также отлучаться на обед, следовательно, другие работники могут осуществить «подсматривание» информации с монитора ПЭВМ.

Угрозе №2 был присвоен показатель низкая вероятность и, соответствующий ему, численный коэффициент Y_2 равный 2, так как допуск лиц на территорию предприятия ограничен, бумажные и съёмные носители информации хранятся в специальных сейфах, однако кражу таких носителей сотрудниками, например, вследствие подкупа следует принимать во внимание.

Угрозе №3 был присвоен показатель низкая вероятность и соответствующий ему показатель Y_2 равный 2, так как допуск лиц на территорию предприятия ограничен, а сотруднику предприятия осуществить уничтожение носителей информации оставшись незамеченным затруднительно.

Угрозе № 4 был присвоен показатель низкая вероятность и соответствующий ему показатель Y_2 равный 2, так как допуск лиц на территорию предприятия ограничен, а сотруднику, осуществившему вывод из строя узлов ПЭВМ или внутренний каналов связи затруднительно остаться незамеченным, однако реализация данной угрозы возможна вследствие неосторожности или халатности сотрудников.

Угрозе № 5 был присвоен показатель маловероятно и соответствующий ему показатель Y_2 равный 0, так как администраторы ИСПДн при приёме на работу проходят тщательную проверку, обладают высоким уровнем профессионализма, однако, так же значение данного показателя было выбрано на основе статистических данных подобного инцидента.

Угрозе № 6 был присвоен показатель высокая вероятность и соответствующий ему показатель Y_2 равный 10, так как существующие на сегодняшний день антивирусные программы не в состоянии отследить проникновение всех, без исключения, вирусов, тем более, что вирус может быть специально разработан для точечной атаки и антивирусная программа просто «не умеет» его распознавать и эффективно устранять. вирус может быть перемещён на атакуемый ПЭВМ с отчуждаемых носителей, используемых сотрудниками подразделения.

Угрозе № 7 был присвоен показатель маловероятно и соответствующий ему показатель Y_2 равный 0, так как все сотрудники, кроме администраторов ИСПДн не обладают привилегиями, позволяющими им устанавливать любое ПО, а администраторы ИСПДн при приёме на работу проходят тщательную проверку и обладают высоким уровнем профессионализма.

Угрозе № 8 был присвоен показатель низкая вероятность и соответствующий ему показатель Y_2 равный 2, так как утрата ключей и атрибутов доступа возможна в силу человеческого фактора – рассеянность, халатность.

Угрозе № 9 был присвоен показатель низкая вероятность и соответствующий ему показатель Y_2 равный 2, так как непреднамеренная модификация информации возможна в силу человеческого фактора – невнимательность, халатность.

Угрозе № 10 был присвоен показатель маловероятно и соответствующий ему показатель Y_2 равный 0 администраторы ИСПДн при приёме на работу проходят тщательную проверку и обладают высоким уровнем профессионализма.

Угрозе № 11 был присвоен показатель низкая вероятность и соответствующий ему показатель Y_2 равный 2, так как администраторы ИСПДн, обслуживающие программно – аппаратные средства обладают высокой квалификацией, однако выход из таких средств возможен в силу обстоятельств, не зависящий от действий администраторов.

Угрозе № 12 был присвоен показатель средняя вероятность и соответствующий ему показатель Y_2 равный 5, так как нельзя быть уверенными в полной благонадёжности каждого сотрудника. возможно разглашение вследствие как подкупа, так и неосторожности, халатности.

Угрозе №13 был присвоен показатель маловероятно и соответствующий ему показатель Y_2 равный 0, так как бумажные и съёмные носители информации хранятся в специальных сейфах, однако утерю в следствие неосторожности или халатности стоит брать во внимание.

Угрозе №14 был присвоен показатель низкая вероятность и соответствующий ему показатель Y_2 равный 2, так как копирование ПДн сотрудников возможно с целью передачи 3-м лицам за вознаграждение.

Угрозе № 15 был присвоен показатель маловероятно и соответствующий ему показатель Y_2 равный 0, так как всем пользователям при создании учётной записи назначается пароль, соответствующий заданному уровню его сложности.

Угрозе №16 был присвоен показатель низкая вероятность и соответствующий ему показатель Y_2 равный 2.

Для каждой угрозы были рассчитаны показатели Y , отражающие степень реализуемости угрозы:

- №1: $Y=(5+5)/20=0,5$ – средняя возможность реализации;
- №2: $Y=(5+2)/20=0,35$ – средняя возможность реализации;
- №3: $Y=(5+2)/20=0,35$ – средняя возможность реализации;
- №4: $Y=(5+2)/20=0,35$ – средняя возможность реализации;
- №5: $Y=(5+0)/20=0,25$ – низкая возможность реализации;
- №6: $Y=(5+10)/20=0,75$ – высокая возможность реализации;
- №7: $Y=(5+0)/20=0,25$ – низкая возможность реализации;
- №8: $Y=(5+2)/20=0,35$ – средняя возможность реализации;
- №9: $Y=(5+2)/20=0,35$ – средняя возможность реализации;
- №10: $Y=(5+0)/20=0,35$ – низкая возможность реализации;
- №11: $Y=(5+2)/20=0,35$ – средняя возможность реализации;

- №12: $Y=(5+5)/20=0,5$ – средняя возможность реализации;
- №13: $Y=(5+0)/20=0,25$ – низкая возможность реализации;
- №14: $Y=(5+2)/20=0,35$ – средняя возможность реализации;
- №15: $Y=(5+0)/20=0,25$ – низкая возможность реализации;
- №16: $Y=(5+2)/20=0,35$ – средняя возможность реализации.

Далее была произведена оценка опасности каждой угрозы, с учётом того, что при оценке последствий от реализации угроз необходимо быть «разумным пессимистом».

Угрозе №1 был присвоен показатель средний, так как возможно нарушение конфиденциальности ПДн, которое повлечёт за собой нанесение различного рода ущерба для их субъекта, в следствие чего на организацию могут быть наложены административные штрафы.

Угрозе №2 был присвоен показатель высокий, так как при реализации данной угрозы возможно нарушение конфиденциальности ПДн достаточно большого числа субъектов, что может повлечь ущерб гражданам, чьи ПДн обрабатывались и наложение крупных административных штрафов на организацию, а также ущерб репутации АО «ПО «Электроприбор».

Угрозе №3 был присвоен показатель высокий, так как уничтожение носителей ПДн может причинить ущерб значительному числу субъектов, а также нанести существенный ущерб АО «ПО «Электроприбор».

Угрозе №4 был присвоен показатель средний, так как нарушения конфиденциальности при реализации данной угрозы не произойдёт, однако будет оказано влияние на доступность ПДн, что в некоторых случаях может быть серьёзной проблемой.

Угрозе №5 был присвоен показатель высокий, так создаётся возможность для оказания практически всех возможных в данной системе деструктивных воздействий на защищаемую информацию.

Угрозе №6 был присвоен показатель высокий, так как создаётся возможность нарушения целостности ПДн сотрудников, что может оказать

деструктивное воздействие на цели их обработки, а также в некоторых случаях антивирус может не обнаружить вредоносный код.

Угрозе №7 был присвоен показатель средний, так как установка ПО, не связанного с использованием служебных обязанностей в некоторых случаях является безобидной, а в некоторых может оказать деструктивное воздействие на ПДн, обрабатываемые в ИСПДн.

Угрозе №8 был присвоен показатель низкий, так как сама по себе утрата ключей и атрибутов доступа не несёт прямого ущерба ПДн, в случае нахождения такой информации посторонним лицом, оно не сможет воспользоваться этими атрибутами, оставшись незамеченным.

Угрозе №9 был присвоен показатель низкий, так как не будет осуществлено нарушение конфиденциальности, а также будет затронуто незначительное число ПДн.

Угрозе №10 был присвоен показатель средний, так как случайная ошибка не затронет большое число средств защиты, тем более всю систему защиты информации.

Угрозе №11 был присвоен показатель средний, так как нарушения конфиденциальности при реализации данной угрозы не произойдёт, однако будет оказано влияние на доступность ПДн, что в некоторых случаях может быть серьёзной проблемой.

Угрозе №12 был присвоен показатель высокий, так как возможно нарушение конфиденциальности Пдн достаточно большого числа субъектов, вследствие чего они понесут ущерб различного рода, а также на АО «ПЮ «Электроприбор» могут быть наложены административные штрафы.

Угрозе №13 был присвоен показатель высокий, так как создаётся возможность нарушения конфиденциальности достаточно большого числа ПДн.

Угрозе №14 был присвоен показатель высокий, так как создаётся возможность нарушения конфиденциальности достаточно большого числа ПДн.

Угрозе №15 был присвоен показатель средний, так как создаётся возможность нарушения конфиденциальности ПДн посредством ознакомления с ними лица, не допущенного к данным сведениям.

Угрозе №16 был присвоен показатель высокий, может быть нарушена целостность достаточно большого числа ПДн.

На основе коэффициентов реализуемости угроз и опасности каждой угрозы была произведена оценка их актуальности:

- Угроза №1 – средняя возм. + средняя опасность=актуальная;
- Угроза №2 – средняя возм. + высокая опасность=актуальная;
- Угроза №3 – средняя возм. + высокая опасность=актуальная;
- Угроза №4 – средняя возм. + средняя опасность=актуальная;
- Угроза №5 – средняя возм. + высокая опасность=актуальная;
- Угроза №6 – высокая возм. + высокая опасность=актуальная;
- Угроза №7 – низкая возм. + средняя опасность=неактуальная;
- Угроза №8 – средняя возм. + низкая опасность=неактуальная;
- Угроза №9 – средняя возм. + низкая опасность=неактуальная;
- Угроза №10 – низкая возм. + средняя опасность=неактуальная;
- Угроза №11 – средняя возм. + средняя опасность=актуальная;
- Угроза №12 – средняя возм. + высокая опасность=актуальная;
- Угроза №13 – низкая возм. + высокая опасность=актуальная;
- Угроза №14 – средняя возм. + высокая опасность=актуальная;
- Угроза №15 – низкая возм. + средняя опасность=неактуальная.
- Угроза №16 – средняя возм. + высокая опасность=актуальная.

Далее было произведено отнесение угроз к конкретному типу. все угрозы, кроме «действия вредоносного ПО», «установка ПО, не связанного с использованием служебных обязанностей» были отнесены к 3 типу, так как они не связаны с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемым в ИСПДн. Угрозы «действия вредоносного ПО», «установка ПО,

не связанного с использованием служебных обязанностей» были отнесены ко 2 типу, так как в обоих случаях предполагается установка постороннего прикладного ПО.

в завершении была разработана модель угроз безопасности ПДн в ИСПДн «Персонал», результаты приведены в таблице А.4 приложения А.

4.1.4 Разработка модели нарушителя

Законодательство о персональных данных, а также нормативно-методические документы ФСТЭК не требуют разработки модели нарушителя, однако данная модель была разработана с целью описания возможностей и мотивации источников угроз, сведения о которых приводились в модели угроз. Разработка модели нарушителя производилась на основе проекта методического документа ФСТЭК «Методика определения угроз безопасности в информационных системах». Результат представлен в таблице А.5 приложения А.

4.2 Оценка исходной защищённости информационной системы коммерческой тайны АО «ПО «Электроприбор»

4.2.1 Определение масштабов информационной системы коммерческой тайны

4.2.1.1 Описание процессов обработки информации, составляющей коммерческую тайну «АО «ПО «Электроприбор» и структуры информационной системы коммерческой тайны

Для описания процесса обработки информации, составляющей КТ АО «ПО «Электроприбор», была разработана модель IDf0, диаграмма которой представлена на рисунке 5. Графическое изображение информационного процесса обработки информации, составляющей КТ даёт общее представление о принципах функционирования ИС КТ, а также позволяет более точно описать структуру ИС и информационные потоки, в ней циркулирующие.

Данный информационный процесс является общим для всех подразделений предприятия, имеющих информацию, составляющую КТ и не учитывает специфику конкретного подразделения.

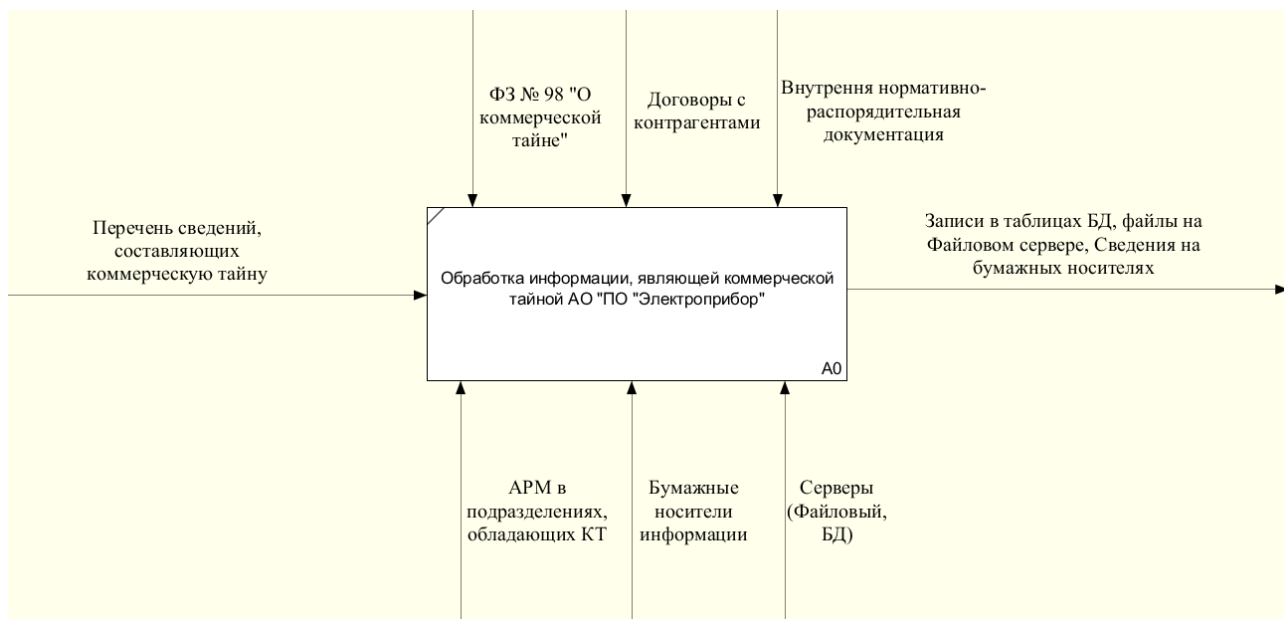


Рисунок 5 – Информационный процесс обработки информации, составляющей КТ АО «ПО «Электроприбор»

Далее было разработано графическое изображение структуры ИС КТ, которое представлено на рисунке 6, отображающее ТС обработки информации и телекоммуникационное оборудование, входящее в состав ИС КТ, а также физические связи между ними.

Как видно из графического изображения, приведённого на рисунке 6, практически в каждом подразделении имеется АРМ для выхода в сеть интернет. взаимодействие данных АРМ с сетью Интернет приведено на этом же рисунке на примере Типового АРМ. А также можно сделать вывод, что структура ИС КТ представляет собой локальную вычислительную сеть, подключение к сетям общего пользования (Интернет) осуществляется с помощью отдельных АРМ, не входящих в общую сеть.

После разработки графического изображения структуры ИС КТ было произведено описание ТС и используемого системного и прикладного ПО, а также, были определены ответственные за конкретное ТС и полномочия пользователей в отношении описанных ТС. Результаты приведены в таблице 8.

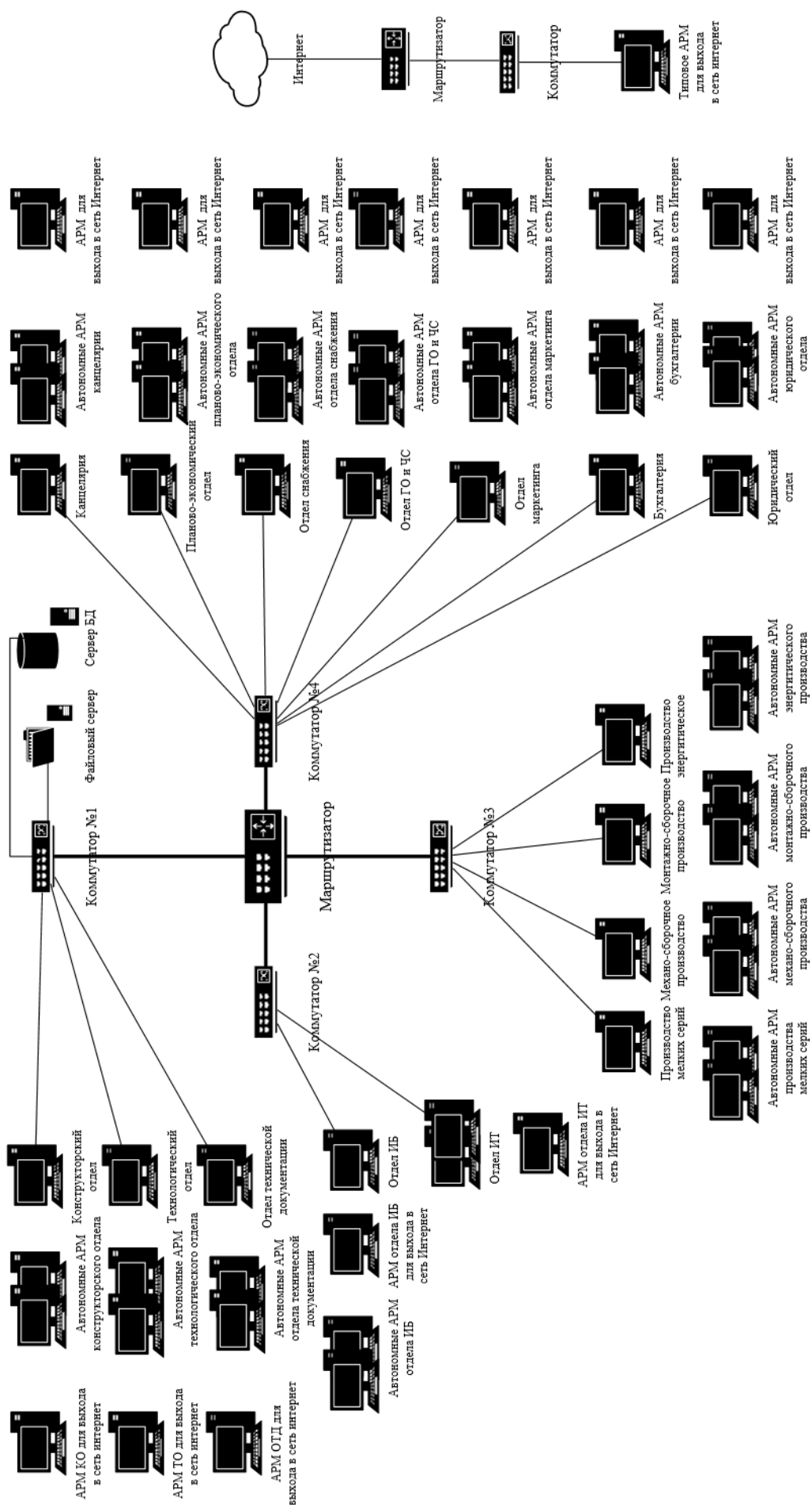


Рисунок 6 – Структура ИС КТ АО «ПО «Электроприбор»

Таблица 8 – Перечень ТС, ПО и ответственных лиц

Техническое средство (ТС)	Установленное ПО	Ответственный за ТС	Пользователь (полномочия)
АРМ сотрудника бухгалтерии	Microsoft Windows 7 Service Pack 1, Антивирус Касперского 8.0 для Windows, Microsoft SQL Server 2012, «1С: Зарплата», пакет Microsoft Office 2007	сотрудник, использующий данное АРМ в повседневной деятельности	разрешено использовать АРМ в объемах, необходимых для выполнения должностных обязанностей (использование в служебных целях), запрещено изменять конфигурацию АРМ
АРМ сотрудника конструкторского отдела	Microsoft Windows 7 Service Pack 1, пакет, Антивирус Касперского 8.0 для Windows, Microsoft Office 2007, Microsoft Visual Studio 2012, комплект программ от Texas Instruments.	сотрудник, использующий данное АРМ в повседневной деятельности	разрешено использовать АРМ в объемах, необходимых для выполнения должностных обязанностей (использование в служебных целях), запрещено изменять конфигурацию АРМ
АРМ сотрудника технологического отдела	Microsoft Windows 7 Service Pack 1, пакет, Антивирус Касперского 8.0 для Windows, Microsoft Office 2007, Microsoft, комплект программ T-FLEX для управления жизненным циклом изделий их совершенствования.	сотрудник, использующий данное АРМ в повседневной деятельности	разрешено использовать АРМ в объемах, необходимых для выполнения должностных обязанностей (использование в служебных целях), запрещено изменять конфигурацию АРМ
АРМ сотрудника отдела технической документации	Microsoft Windows 7 Service Pack 1, Антивирус Касперского 8.0 для Windows, пакет Microsoft Office	сотрудник, использующий данное АРМ в повседневной деятельности	разрешено использовать АРМ в объемах, необходимых для выполнения должностных обязанностей (использование в служебных целях), запрещено изменять конфигурацию АРМ

Продолжение таблицы 8

Техническое средство (ТС)	Установленное ПО	Ответственный за ТС	Пользователь (полномочия)
АРМ сотрудника отдела ИТ	Microsoft Windows Server 2008 Standard Edition (SP2), Microsoft SQL Server 2012, Антивирус Касперского 8.0 для Windows Servers Enterprise Edition, пакет Microsoft Office 2007	администратор АС	разрешено изменять конфигурацию и состав всех ТС ИС
АРМ сотрудников производств (мелких серий, механо–сборочного, монтажно–сборочного)	Microsoft Windows 7 Service Pack 1, Антивирус Касперского 8.0 для Windows, пакет Microsoft Office 2007, Microsoft Visual Studio 2012, комплект программ от Texas Instruments.	сотрудник, использующий данное АРМ в повседневной деятельности	разрешено использовать АРМ в объемах, необходимых для выполнения должностных обязанностей (использование в служебных целях), запрещено изменять конфигурацию АРМ
АРМ сотрудников Канцелярии	Microsoft Windows 7 Service Pack 1, Антивирус Касперского 8.0 для Windows, пакет Microsoft Office	сотрудник, использующий данное АРМ в повседневной деятельности	разрешено использовать АРМ в объемах, необходимых для выполнения должностных обязанностей (использование в служебных целях), запрещено изменять конфигурацию АРМ
АРМ сотрудника планово–экономического отдела	Microsoft Windows 7 Service Pack 1, Антивирус Касперского 8.0 для Windows, пакет Microsoft Office	сотрудник, использующий данное АРМ в повседневной деятельности	разрешено использовать АРМ в объемах, необходимых для выполнения должностных обязанностей (использование в служебных целях), запрещено изменять конфигурацию АРМ

Продолжение таблицы 8

Техническое средство (ТС)	Установленное ПО	Ответственный за ТС	Пользователь (полномочия)
АРМ сотрудника отдела снабжения	Microsoft Windows 7 Service Pack 1, Антивирус Касперского 8.0 для Windows, пакет Microsoft Office	сотрудник, использующий данное АРМ в повседневной деятельности	разрешено использовать АРМ в объемах, необходимых для выполнения должностных обязанностей (использование в служебных целях), запрещено изменять конфигурацию АРМ
АРМ сотрудника отдела ГО и ЧС	Microsoft Windows 7 Service Pack 1, Антивирус Касперского 8.0 для Windows, пакет Microsoft Office	сотрудник, использующий данное АРМ в повседневной деятельности	разрешено использовать АРМ в объемах, необходимых для выполнения должностных обязанностей (использование в служебных целях), запрещено изменять конфигурацию АРМ
АРМ сотрудника отдела маркетинга	Microsoft Windows 7 Service Pack 1, Антивирус Касперского 8.0 для Windows, пакет Microsoft Office	сотрудник, использующий данное АРМ в повседневной деятельности	разрешено использовать АРМ в объемах, необходимых для выполнения должностных обязанностей (использование в служебных целях), запрещено изменять конфигурацию АРМ
АРМ сотрудника юридического отдела	Microsoft Windows 7 Service Pack 1, Антивирус Касперского 8.0 для Windows, пакет Microsoft Office	сотрудник, использующий данное АРМ в повседневной деятельности	разрешено использовать АРМ в объемах, необходимых для выполнения должностных обязанностей (использование в служебных целях), запрещено изменять конфигурацию АРМ

Продолжение таблицы 8

Техническое средство (ТС)	Установленное ПО	Ответственный за ТС	Пользователь (полномочия)
АРМ сотрудника отдела ИБ	Microsoft Windows 7 Service Pack 1, Антивирус Касперского 8.0 для Windows, пакет Microsoft Office, Foxit Reader.	сотрудник, использующий данное АРМ в повседневной деятельности	разрешено использовать АРМ в объемах, необходимых для выполнения должностных обязанностей (использование в служебных целях), запрещено изменять конфигурацию АРМ
АРМ для доступа в сеть интернет	Microsoft Windows 7 Service Pack 1, Kaspersky Internet Security 2016, пакет Microsoft Office 2007	руководитель подразделения	Разрешено использовать АРМ в объемах, необходимых для выполнения должностных обязанностей (использование в служебных целях), запрещено изменять конфигурацию АРМ
Сетевое АРМ производств (производство мелких серий, механо–сборочное производство, монтажно–сборочное производство)	Microsoft Windows 7 Service Pack 1, Microsoft SQL Server 2012, Антивирус Касперского 8.0 для Windows, пакет Microsoft Office 2007, 1С: «Продукция», «Запасы», комплект программ T-FLEX для управления жизненным циклом изделий их совершенствования.	руководитель подразделения	разрешено использовать АРМ в объемах, необходимых для выполнения должностных обязанностей (использование в служебных целях), запрещено изменять конфигурацию АРМ
Сетевое АРМ отдела снабжения	Microsoft Windows 7 Service Pack 1, Microsoft SQL Server 2012, Антивирус Касперского 8.0 для Windows, пакет Microsoft Office 2007, 1С: «Запасы». 1С: «Документооборот»	руководитель подразделения	разрешено использовать АРМ в объемах, необходимых для выполнения должностных обязанностей (использование в служебных целях), запрещено изменять конфигурацию АРМ

Продолжение таблицы 8

Техническое средство (ТС)	Установленное ПО	Ответственный за ТС	Пользователь (полномочия)
Сетевое АРМ планово–экономического отдела	Microsoft Windows 7 Service Pack 1, Microsoft SQL Server 2012, Антивирус Касперского 8.0 для Windows, пакет Microsoft Office 2007, 1С: «Продукция », 1С: «Документооборот»	руководитель подразделения	разрешено использовать АРМ в объемах, необходимых для выполнения должностных обязанностей (использование в служебных целях), запрещено изменять конфигурацию АРМ
Сетевое АРМ отдела маркетинга	Microsoft Windows 7 Service Pack 1, Microsoft SQL Server 2012, Антивирус Касперского 8.0 для Windows, пакет Microsoft Office 2007, 1С: «Продукция », 1С: «Документооборот»	руководитель подразделения	разрешено использовать АРМ в объемах, необходимых для выполнения должностных обязанностей (использование в служебных целях), запрещено изменять конфигурацию АРМ
Сетевое АРМ отдела технической документации	Microsoft Windows 7 Service Pack 1, Microsoft SQL Server 2012, Антивирус Касперского 8.0 для Windows, пакет Microsoft Office 2007, 1С: «Запасы».	руководитель подразделения	разрешено использовать АРМ в объемах, необходимых для выполнения должностных обязанностей (использование в служебных целях), запрещено изменять конфигурацию АРМ
Сетевое АРМ конструкторского отдела	Microsoft Windows 7 Service Pack 1, Антивирус Касперского 8.0 для Windows, пакет Microsoft Office 2007.	руководитель подразделения	разрешено использовать АРМ в объемах, необходимых для выполнения должностных обязанностей (использование в служебных целях), запрещено изменять конфигурацию АРМ

Продолжение таблицы 8

Техническое средство (ТС)	Установленное ПО	Ответственный за ТС	Пользователь (полномочия)
Сетевое АРМ технологического отдела	Microsoft Windows 7 Service Pack 1, Microsoft SQL Server 2012, Антивирус Касперского 8.0 для Windows, пакет Microsoft Office 2007, 1С: «Продукция», «Запасы», комплект программ T-FLEX для управления жизненным циклом изделий их совершенствования.	руководитель подразделения	разрешено использовать АРМ в объемах, необходимых для выполнения должностных обязанностей (использование в служебных целях), запрещено изменять конфигурацию АРМ
Сетевое АРМ отдела ИБ	Microsoft Windows 7 Service Pack 1, Антивирус Касперского 8.0 для Windows, Microsoft SQL Server 2012, пакет Microsoft Office 2007, 1С «Документооборот»	руководитель подразделения	разрешено использовать АРМ в объемах, необходимых для выполнения должностных обязанностей (использование в служебных целях), запрещено изменять конфигурацию АРМ
Сетевое АРМ отдела ГО и ЧС	Microsoft Windows 7 Service Pack 1, Microsoft SQL Server 2012, Антивирус Касперского 8.0 для Windows, пакет Microsoft Office 2007, 1С «Документооборот»	руководитель подразделения	разрешено использовать АРМ в объемах, необходимых для выполнения должностных обязанностей (использование в служебных целях), запрещено изменять конфигурацию АРМ
Сетевое АРМ юридического отдела	Microsoft Windows 7 Service Pack 1, Microsoft SQL Server 2012, Антивирус Касперского 8.0 для Windows, пакет Microsoft Office 2007, 1С «Документооборот»	руководитель подразделения	разрешено использовать АРМ в объемах, необходимых для выполнения должностных обязанностей (использование в служебных целях), запрещено изменять конфигурацию АРМ

Продолжение таблицы 8

Техническое средство (ТС)	Установленное ПО	Ответственный за ТС	Пользователь (полномочия)
Сетевое АРМ энергетического производства	Microsoft Windows 7 Service Pack 1, Microsoft SQL Server 2012, Антивирус Касперского 8.0 для Windows, пакет Microsoft Office 2007, 1С «Документооборот»	руководитель подразделения	разрешено использовать АРМ в объёмах, необходимых для выполнения должностных обязанностей (использование в служебных целях), запрещено изменять конфигурацию АРМ
Типовой АРМ для выхода в сеть интернет	Microsoft Windows 7 Service Pack 1, Антивирус Kaspersky Internet Security 2016, пакет Microsoft Office 2007.	руководитель подразделения	разрешено использовать АРМ в объёмах, необходимых для выполнения должностных обязанностей (использование в служебных целях), запрещено изменять конфигурацию АРМ
Маршрутизатор Cisco 1841	–	администратор ИС	разрешено производить настройку данного оборудования
Цифровой Коммутатор Cisco IE– 3000– 8TC– E	–	администратор ИС	разрешено производить настройку данного оборудования

Далее на основании информационного процесса обработки информации, составляющей КТ, структуры сети, а также сведений о том, какие сведения обрабатываются в подразделениях АО «ПО «Электроприбор» была разработана структура информационных потоков в ИС КТ АО «ПО «Электроприбор». Для большей наглядности графического изображения, представленного на рисунке 7, на нём не отображалось телекоммуникационное оборудование и физические связи между ТС.

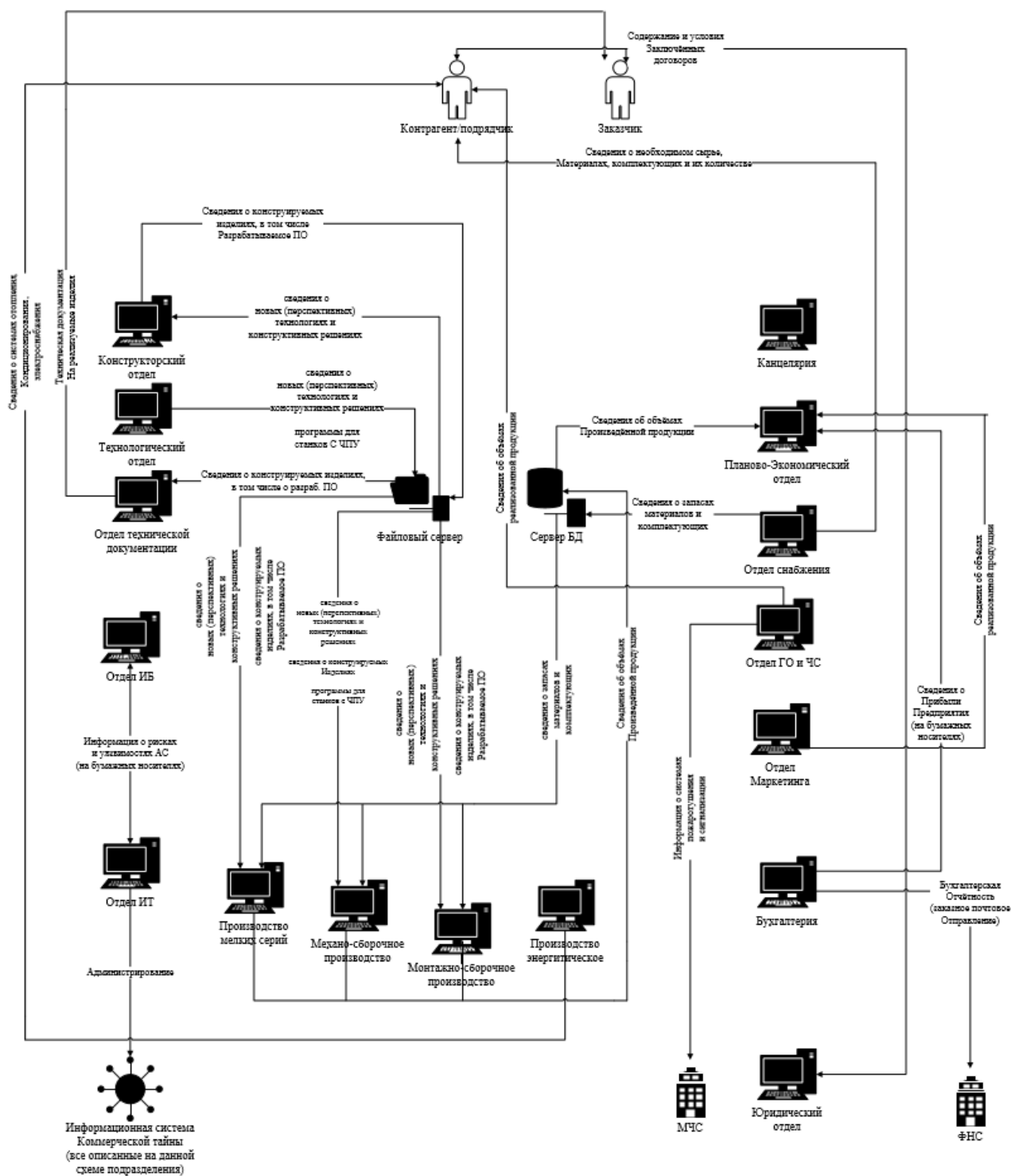


Рисунок 7 – Структура информационных потоков в ИС КТ АО «ПО «Электроприбор»

4.2.1.2 Определение условий использования информации, составляющей КТ

На основании разработанной схемы информационных потоков, а также разработанного на предыдущих этапах перечня информации, составляющей КТ

АО «ПО «Электроприбор» была разработана матрица доступа к такой информации. Целью разработки матрицы является определение групп лиц, допущенных к информации, составляющей КТ на законном основании, а также определить перечень разрешённых им действий в отношении данной информации. Матрица доступа представлена в таблице 9.

Таблица 9 – Матрица доступа к информации, составляющей коммерческую тайну АО «ПО «Электроприбор»

Подразделение с имеющейся в нём КТ	Группа доступа к КТ	Уровень доступа к КТ	Разрешённые действия
Конструкторский отдел	сотрудники конструкторского отдела	обладают всеми необходимыми атрибутами и правами, обеспечивающими доступ к КТ для выполнения должностных обязанностей	– создание; – хранение; – использование.
	сотрудники отдела технической документации	обладают необходимыми атрибутами и правами, обеспечивающими доступ к КТ для выполнения должностных обязанностей	использование
	сотрудники производств (мелких серий, монтажно–сборочное)	обладают необходимыми атрибутами и правами, обеспечивающими доступ к КТ для выполнения должностных обязанностей	использование
Технологический отдел	сотрудники технологического отдела	обладают всеми необходимыми атрибутами и правами, обеспечивающими доступ к КТ для выполнения должностных обязанностей	– создание; – хранение; – использование.
	сотрудники производств (мелких серий, монтажно–сборочное)	обладают необходимыми атрибутами и правами, обеспечивающими доступ к КТ для выполнения должностных обязанностей	использование

Продолжение таблицы 9

Подразделение с имеющейся в нём КТ	Группа доступа к КТ	Уровень доступа к КТ	Разрешённые действия
Технологический отдел	сотрудники конструкторского отдела	обладают необходимыми атрибутами и правами, обеспечивающими доступ к КТ для выполнения должностных обязанностей	использование
Отдел технической документации	сотрудники отдела технической документации	обладают всеми необходимыми атрибутами и правами, обеспечивающими доступ к КТ для выполнения должностных обязанностей	– создание; – хранение; – использование; – накопление.
	заказчики	обладают необходимыми правами, обеспечивающими доступ к КТ на условиях заключённых контрактов	– хранение; – использование.
Юридический отдел	сотрудники юридического отдела	обладают всеми необходимыми атрибутами и правами, обеспечивающими доступ к КТ для выполнения должностных обязанностей	– создание; – хранение; – использование.
	заказчики, контрагенты/поставщики	обладают необходимыми правами, обеспечивающими доступ к КТ на условиях заключённых контрактов	– хранение; – использование; – накопление.
Канцелярия	сотрудники канцелярии	обладают всеми необходимыми атрибутами и правами, обеспечивающими доступ к КТ для выполнения должностных обязанностей	– создание; – хранение; – использование.
Отдел снабжения	сотрудники отдела снабжения	обладают всеми необходимыми атрибутами и правами, обеспечивающими доступ к КТ для выполнения должностных обязанностей	– создание; – хранение; – использование.

Продолжение таблицы 9

Подразделение с имеющейся в нём КТ	Группа доступа к КТ	Уровень доступа к КТ	Разрешённые действия
Отдел снабжения	сотрудники производств (мелких серий, монтажно–сборочное, механо–сборочное)	обладают необходимыми атрибутами и правами, обеспечивающими доступ к КТ для выполнения должностных обязанностей	использование
	контрагенты, поставщики	обладают необходимыми правами, обеспечивающими доступ к КТ на условиях заключённых контрактов	использование
Бухгалтерия	сотрудники бухгалтерии	обладают всеми необходимыми атрибутами и правами, обеспечивающими доступ к КТ для выполнения должностных обязанностей	– создание; – хранение; – использование; – накопление.
	сотрудники планово–экономического отдела	обладают необходимыми атрибутами и правами, обеспечивающими доступ к КТ для выполнения должностных обязанностей	– хранение; – использование.
Планово–экономический отдел	сотрудники планово–экономического отдела	обладают необходимыми атрибутами и правами, обеспечивающими доступ к КТ для выполнения должностных обязанностей	– создание; – хранение; – использование; – накопление.
	руководители подразделений АО «ПО «Электроприбор»	обладают необходимыми атрибутами и правами, обеспечивающими доступ к КТ для выполнения должностных обязанностей	– использование, – хранение.
Отдел ГО и ЧС	сотрудники отдела ГО и ЧС	обладают необходимыми атрибутами и правами, обеспечивающими доступ к КТ для выполнения должностных обязанностей	– хранение; – использование; – накопление.

Продолжение таблицы 9

Подразделение с имеющейся в нём КТ	Группа доступа к КТ	Уровень доступа к КТ	Разрешённые действия
Отдел ГО и ЧС	контрагенты/подрядчики	обладают необходимыми правами, обеспечивающими доступ к КТ на условиях заключённых контрактов	– использование; – хранение.
	сотрудники МЧС	обладают необходимыми правами в соответствии с законодательством РФ, обеспечивающими доступ к КТ	использование
Отдел маркетинга	сотрудники отдела маркетинга	обладают всеми необходимыми атрибутами и правами, обеспечивающими доступ к КТ для выполнения должностных обязанностей	– создание; – хранение; – использование; – накопление.
	планово–экономический отдел	обладают необходимыми атрибутами и правами, обеспечивающими доступ к КТ для выполнения должностных обязанностей	– хранение; – использование; – накопление.
Отдел информационных технологий	сотрудники отдела информационных технологий	обладают всеми необходимыми атрибутами и правами, обеспечивающими доступ к КТ для выполнения должностных обязанностей	– создание; – хранение; – использование; – накопление.
	сотрудники отдела информационной безопасности	обладают всеми необходимыми атрибутами и правами, обеспечивающими доступ к КТ для выполнения должностных обязанностей	– использование; хранение.
Отдел информационно й безопасности	сотрудники отдела информационной безопасности	обладают всеми необходимыми атрибутами и правами, обеспечивающими доступ к КТ для выполнения должностных обязанностей	– создание; – использование; – хранение; – накопление.

Продолжение таблицы 9

Подразделение с имеющейся в нём КТ	Группа доступа к КТ	Уровень доступа к КТ	Разрешённые действия
Производство энергетическое	сотрудники энергетического производства	обладают всеми необходимыми атрибутами и правами, обеспечивающими доступ к КТ для выполнения должностных обязанностей	– использование; – хранение; – накопление.
	контрагенты/подрядчики	обладают необходимыми правами, обеспечивающими доступ к КТ на условиях заключённых контрактов	использование
Производства (механо–сборочное, монтажно–сборочное,	сотрудники производств	обладают всеми необходимыми атрибутами и правами, обеспечивающими доступ к КТ для выполнения должностных обязанностей	– использование; – хранение; – создание.
Все подразделения	руководители подразделений	обладают всеми необходимыми атрибутами и правами, обеспечивающими доступ к КТ для выполнения должностных обязанностей. вносят предложения по расширению или сужению перечня сведений, составляющих коммерческую тайну предприятия	– использование; – хранение; – создание; – уничтожение; – накопление.
	органы государственной власти, иных государственных органов, органов местного самоуправления	обладают необходимыми правами в соответствии с законодательством РФ, обеспечивающими доступ к КТ	– использование, – хранение.

4.2.2 Составление перечня угроз информационной безопасности для информационной системы коммерческой тайны

Так как для информации, составляющей КТ в настоящий момент не разработано документов, содержащих типовые модели угроз безопасности, за исходный перечень угроз ИБ был взят перечень угроз безопасности ПДн

разработанный ранее с последующим внесением некоторых изменений, он представлен в таблице 10.

Таблица 10 – Перечень угроз ИБ для информации, составляющей КТ АО «ПО «Электроприбор» и описание их факторов

№ п/п	Описание угрозы	Источник угрозы	Нарушаемые свойства	Объекты воздействия	Уязвимость
1	Утечка видовой информации	внутренние (персонал, не имеющий доступа к защищаемой информации)	К	информация, составляющая КТ: – обрабатываемая на АРМ пользователей; – находящаяся на бумажных носителях информации.	–не выключение экрана монитора при оставлении рабочего места; –расположение мониторов, позволяющее осуществить несанкционированный просмотр информации.
		внешние (персонал контрагента, не имеющий доступ к защищаемой информации)	К	информация, составляющая КТ, переданная или полученная на основании договорных обязательств	
2	Кража носителей информации	внутренние (персонал, имеющий доступ к защищаемой информации)	К	информация, составляющая КТ, содержащиеся на электронном и бумажном носителе информации	–слабость мер учёта и хранения носителей информации; –халатность персонала, ответственного за иные носители информации; –отсутствие механизмов резервного копирования информации
		внутренние (персонал, имеющий доступ в КЗ, но не имеющий доступ к защищаемой информации)			

Продолжение таблицы 10

№ п/п	Описание угрозы	Источник угрозы	Нарушаемые свойства	Объекты воздействия	Уязвимость
2	Кража носителей информации	внешние (персонал контрагента)	К	Информация, составляющая КТ, содержащиеся на электронном и бумажном носителе информации (переданная или полученная на основании договорных обязательств	–слабость мер учёта и хранения носителей информации; –халатность персонала, ответственного за иные носители информации; – отсутствие механизмов резервного копирования информации.
3	Уничтожение информации и её носителей	внутренние (персонал, имеющий доступ к защищаемой информации; персонал, осуществляющий администрирование ИС КТ).	Ц, Д	информация, составляющая КТ: – обрабатываемая на АРМ, сервере БД и файловом сервере; – содержащиеся на электронном и бумажном носителе информации.	– слабость мер учёта и хранения носителей информации; – отсутствие механизмов резервного копирования информации; – наличие у пользователя прав доступа, позволяющих реализовать данную угрозу; – отсутствие механизма контроля целостности
		внутренние (персонал, имеющий доступ к КЗ, но не имеющий доступ к защищаемой информации)			
4	Вывод из строя узлов ПЭВМ, серверов, каналов связи	внутренние (персонал, имеющий доступ к защищаемой информации; персонал, осуществляющий администрирование ИС КТ)	Д	информация, составляющая КТ, обрабатываемая на АРМ, сервере БД и файловом сервере.	– небрежная прокладка каналов связи; – отсутствие аппаратного резервирования; – отсутствие мер по контролю за исправностью ТС

Продолжение таблицы 10

№ п/п	Описание угрозы	Источник угрозы	Нарушаемые свойства	Объекты воздействия	Уязвимость
4	Вывод из строя узлов ПЭВМ, серверов, каналов связи	внутренние (персонал, имеющий доступ к КЗ, но не имеющий доступ к защищаемой информации)	Д	информация, составляющая КТ, обрабатываемая на АРМ, сервере БД и файловом сервере.	отсутствие мер по предотвращению бесконтрольного доступа к системным блокам ПЭВМ.
5	Несанкционированное отключение средств защиты	внутренние (персонал, осуществляющий администрирование ИС КТ)	К, Ц	информация, составляющая КТ, обрабатываемая на АРМ, сервере БД и файловом сервере	недостаточность контроля за действиями пользователей
6	Угроза внедрения кода или данных	внутренние	Ц	информация, составляющая КТ, обрабатываемая на АРМ, сервере БД и файловом сервере	–недостаточный уровень осведомлённости персонала; –отсутствие и/или некорректная настройка антивирусных средств.
		внешние	Ц, К	информация, составляющая КТ, переданная или полученная в соответствии с договорными обязательствами	–недостаточный уровень осведомлённости персонала; –неактуальные базы данных признаков ВПО.
7	Непреднамеренная модификация (уничтожение) данных	внутренние (персонал, имеющий доступ к защищаемой информации; персонал, осуществляющий администрирование ИС КТ)	Ц	информация, составляющая КТ, обрабатываемая на АРМ, сервере БД и файловом сервере	–недостаточный уровень обучения или квалификации; –отсутствие механизмов резервного копирования данных; –отсутствие механизма контроля целостности.

Продолжение таблицы 10

№ п/п	Описание угрозы	Источник угрозы	Нарушаемые свойства	Объекты воздействия	Уязвимость
8	Установка ПО, не связанного с использованием в целях выполнения должностных обязанностей	внутренние	Ц, Д	информация, составляющая КТ, обрабатываемая на АРМ, сервере БД и файловом сервере	–недостаточный уровень осведомлённости и квалификации; –наличие прав доступа, позволяющих устанавливать ПО.
9	Непреднамеренное отключение средств защиты	внутренние (персонал, осуществляющий администрирование ИС КТ)	Ц, Д	информация, составляющая КТ, обрабатываемая на АРМ, сервере БД и файловом сервере	–недостаточный уровень обучения или квалификации; –наличие соответствующих привилегий.
10	Утрата ключей и атрибутов доступа	внутренние	Д	информация, составляющая КТ, обрабатываемая на АРМ, сервере БД и файловом сервере	недостаточный уровень осведомления, квалификации.
11	Разглашение информации, составляющей КТ	внутренние (персонал, имеющий доступ к защищаемой информации, персонал)	К	информация, составляющая КТ, содержащиеся на электронном и бумажном носителе информации.	недостаточный уровень осведомлённости или обучения.
		внешние (персонал контрагента, имеющий доступ к защищаемой информации)			

Продолжение таблицы 10

№ п/п	Описание угрозы	Источник угрозы	Нарушаемые свойства	Объекты воздействия	Уязвимость
12	Выход из строя аппаратных и программных средств	внутренние (персонал, осуществляющий администрирование ИС КТ)	Д, Ц	информация, составляющая КТ, обрабатываемая на АРМ, сервере БД и файловом сервере	– несвоевременное или халатное обслуживание аппаратно–программных средств; – отсутствие аппаратного резервирования критических узлов системы; – отсутствие процедур резервирования программного обеспечения.
13	Утрата носителей информации	внутренние (персонал, имеющий доступ к защищаемой информации)	К	информация, составляющая КТ, содержащиеся на электронном и бумажном носителе информации	–слабость мер учёта и хранения носителей информации; –отсутствие механизмов резервного копирования.
14	Несанкционированное копирование БД информации, составляющей КТ или её частей, а также информации с файлового сервера	внутренние (персонал, имеющий доступ к защищаемой информации)	К	информация, составляющая КТ, обрабатываемая на АРМ, сервере БД и файловом сервере	отсутствие механизмов, препятствующих их несанкционированному копированию данных
		внутренние (персонал, осуществляющий администрирование ИС КТ)	К	информация, составляющая КТ, обрабатываемая на АРМ, сервере БД и файловом сервере	

Продолжение таблицы 10

№ п/п	Описание угрозы	Источник угрозы	Нарушаемые свойства	Объекты воздействия	Уязвимость
14	Несанкционированное копирование БД информации, составляющей КТ или её частей, а также информации с файлового сервера	внешние (персонал контрагента, имеющий доступ к защищаемой информации)	К	информация, составляющая КТ, переданная или полученная в соответствии с договорными обязательствами, находящаяся на съёмных носителях информации или на АРМ.	отсутствие механизмов, препятствующих их несанкционированному копированию данных.
15	Обход некорректно настроенных механизмов аутентификации	внутренние (персонал, не имеющий доступ к защищаемой информации)	К, Ц, Д	информация, составляющая КТ, обрабатываемая на АРМ, сервере БД и файловом сервере	отсутствие или слабость паролей для входа в система
16	Модификация данных	внутренние (персонал, имеющий доступ к защищаемой информации)	Ц	информация, составляющая КТ, обрабатываемая на АРМ, сервере БД и файловом сервере	отсутствие механизмов, препятствующих их несанкционированной модификации данных

4.2.3 Идентификация актуальных угроз безопасности для информации, составляющей коммерческую тайну АО «ПО «Электроприбор»

Для информации, составляющей КТ, не определены методики отнесения угроз к актуальным, поэтому отнесение угроз из разработанного перечня к актуальным производилось экспертным методом с обоснованием принятого решения.

Угроза №1 была признана актуальной, так как в повседневной деятельности могут неоднократно возникать обстоятельства, при которых сотрудник, не допущенный к определённому виду информации, составляющей КТ, может случайно или преднамеренно посредством наблюдения или «подсматривания» ознакомиться с такими сведениями, и, впоследствии,

создаётся вероятность, что эти сведения будут переданы 3–м лицам, что, в свою очередь, повлечёт финансовые потери или упущение коммерческой выгоды для организации.

Угроза №2 была признана актуальной, так как в случае кражи носителей информации, составляющей КТ и последующей их передаче третьим лицам, создаётся угроза финансовых потерь и/или упущения коммерческой выгоды.

Угроза №3 была признана актуальной, так как её реализации создаётся опасность нарушения отдельных видов деятельности предприятия, направленных на получение прибыли, следовательно, организация понесёт финансовые потери, также возможны репутационные потери.

Угроза №4 была признана неактуальной, так как информация, составляющая КТ, не обладает высоким уровнем оперативности, сотрудники отдела ИТ оперативно реагируют на случившиеся поломки, приостановления отдельных видов деятельности также не возникнет, так как данная угроза может быть реализована только точечно, как правильно случайно.

Угроза №5 была признана актуальной, так как при отключении средств защиты возникает возможность возникновения событий, которые повлекут за собой нарушение конфиденциальности и целостности защищаемой информации, что в свою очередь может приостановить или существенно затруднить деятельность некоторых подразделений АО «ПО «Электроприбор», следовательно, возникнут финансовые потери, возникнут непредвиденные затраты времени.

Угроза №6 была признана актуальной, так как при её реализации создаётся возможность утери защищаемых сведений, что, в свою очередь, может стать причиной финансовых потерь для организации, а также при реализации данной угрозы на стороне контрагента создаётся угроза нарушения конфиденциальности информации, составляющей КТ АО «ПО «Электроприбор», что в свою очередь влечёт финансовые потери и вероятное упущение коммерческой выгоды.

Угроза № 7 была признана неактуальной, так как действие угрозы случайное, и, как правило, точечное, следовательно, большие объёмы информации затронуты не будут, деятельность предприятия и подразделений не будет подвергнута затруднениям или приостановке, следовательно, финансовых потерь и упущения коммерческой выгоды не предвидится.

Угрозе №8 был признана неактуальной, так как пользователи ИС не имеют прав для инсталляции ПО, администраторы ИС проходят тщательный обор при приёме на работу.

Угрозе №9 была признана неактуальной, так как администраторы ИС, при приёме на работу проходят тщательный отбор и обладают высокой квалификацией.

Угроза №10 была признана неактуальной так как её реализация не влияет на конфиденциальность и целостность защищаемых сведений, следовательно, предприятию не будет нанесён ущерб.

Угроза № 11 была признана актуальной, так как её реализация может нанести существенный финансовый ущерб организации, а также повлечь за собой упущение коммерческой выгоды.

Угроза №12 была признана неактуальной, так как в случае её реализации организация не понесёт крупных финансовых потерь и/или не упустит коммерческую выгоду. Сотрудники отдела информационных технологий оперативно реагируют на возникающие неисправности.

Угроза №13 была признана неактуальной в случае, так как носители информации, составляющей КТ, хранятся в специальных шкафах.

Угроза №14 была признана актуальной, так как в случае её реализации и последующей передаче скопированной информации третьим лицам, АО «ПО «Электроприбор» может понести существенные финансовые потери и/или упустить значительную финансовую выгоду.

Угроза №15 была признана неактуальной, так как всем пользователям при создании учётной записи назначается пароль, соответствующий заданному уровню его сложности.

Угроза № 16 была признана актуальной, так как в некоторых случаях её реализация может повлечь за собой крупные финансовые потери и/или упущение коммерческой выгоды.

На основании перечня угроз безопасности информации, составляющей КТ, и определения их актуальности была разработана модель угроз безопасности, приведённая в таблице А.6 приложения А. Данная модель содержит сочетание угроз ИБ, источника угрозы, а также нарушаемые свойства защищаемой информации, ущерб, наносимый в результате реализации угрозы, и степень актуальности угрозы.

4.2.4 Разработка модели нарушителя

После разработки модели угроз информации, составляющей КТ АО «ПО «Электроприбор», была разработана модель нарушителя с целью описания возможностей и мотивации источников угроз, сведения о которых были приведены в модели угроз и частично были раскрыты. Разработка модели нарушителя производилась на основе проекта методического документа ФСТЭК «Методика определения угроз безопасности в информационных системах». Результат представлен в таблице А.7 приложения А.

4.3 Оценка исходной защищённости информационной системы конфиденциальной информации АО «ПО «Электроприбор»

4.3.1 Определение масштабов информационной системы конфиденциальной информации

4.3.1.1 Описание процессов обработки иной конфиденциальной информации в АО «ПО «Электроприбор» и структуры информационной системы иной конфиденциальной информации

Для описания процесса обработки конфиденциальной информации, не являющейся персональными данными или информацией, составляющей КТ АО «ПО «Электроприбор», была разработана модель IDF0, диаграмма которой представлена на рисунке 8. Графическое изображение информационного процесса обработки иной конфиденциальной информации даёт общее

представление о принципах функционирования ИС КИ, а также позволяет более точно описать структуру ИС и информационные потоки, в ней циркулирующие.

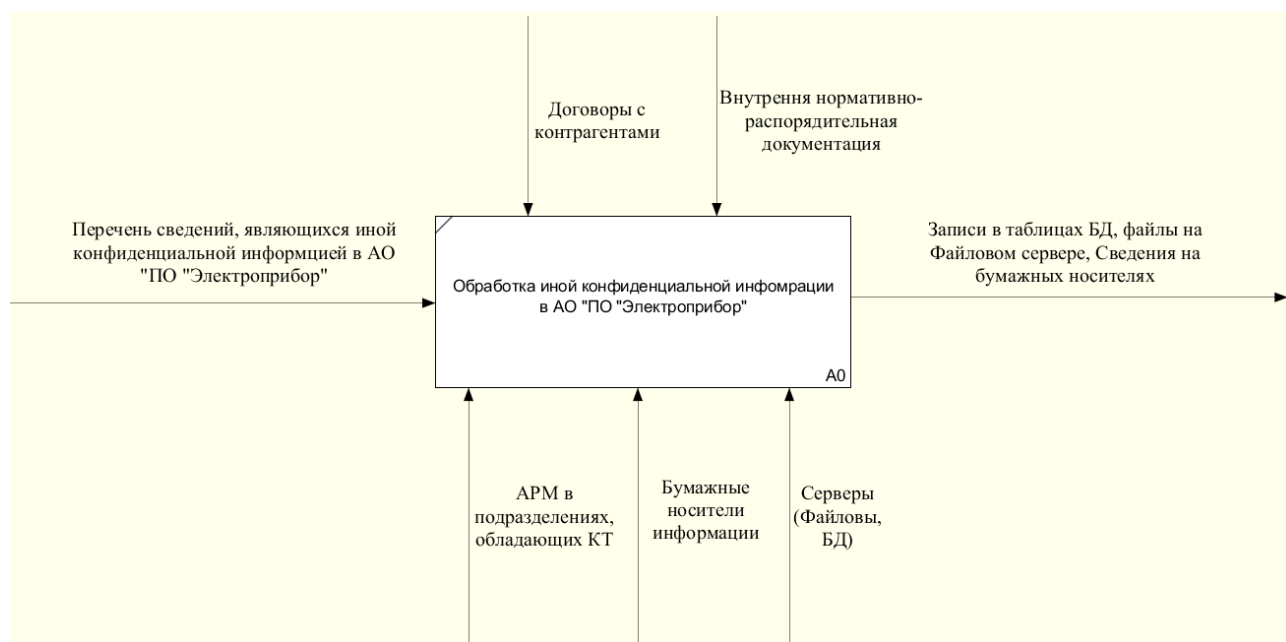


Рисунок 8 – Информационный процесс обработки иной конфиденциальной информации в АО «ПО «Электроприбор»

Данный информационный процесс является общим для всех подразделений предприятия, имеющих информацию, составляющую КТ и не учитывает специфику конкретного подразделения. Информационные процессы протекающие в каждом подразделении не приводились из соображений конфиденциальности.

Далее было разработано графическое изображение структуры ИС КИ, которое представлено на рисунке 9 и отображающее ТС обработки информации и телекоммуникационное оборудование, входящее в состав ИС КИ, а также физические связи между ними.

Как видно из графического изображения, приведённого на рисунке 9, практически в каждом подразделении имеется АРМ для выхода в сеть интернет. взаимодействие данных АРМ с сетью Интернет приведено на этом же рисунке на примере Типового АРМ. А также можно сделать вывод, что структура ИС КИ представляет собой локальную вычислительную сеть, подключение к сетям общего пользования (Интернет) осуществляется с помощью отдельных АРМ, не входящих в общую сеть.

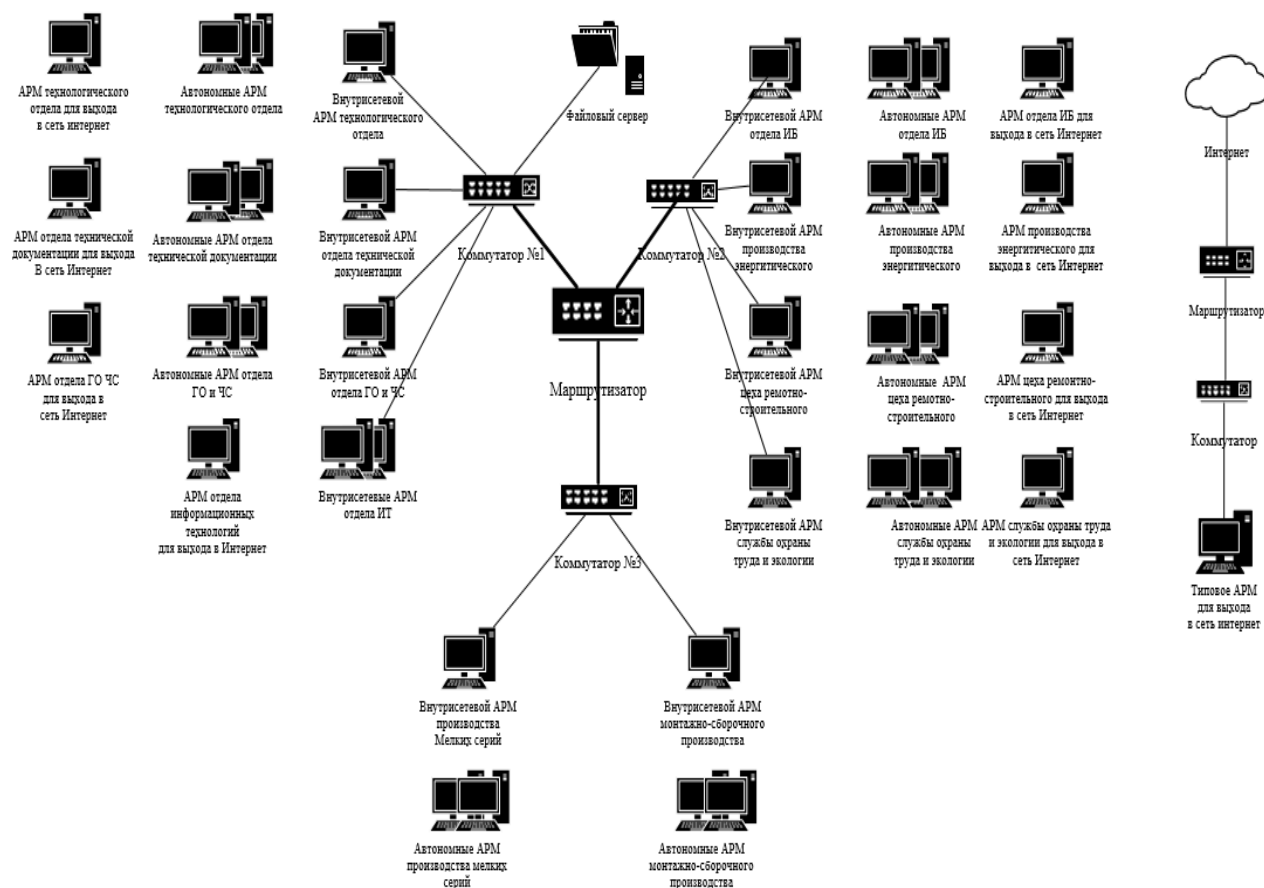


Рисунок 9 – Структура ИС КИ АО «ПО «Электроприбор»

Описание ТС и используемого системного и прикладного ПО, определение ответственных за конкретное ТС и полномочия пользователей в отношении них не проводилось, так как физически значительная часть ИС КИ входит в ИС КТ, в которой данное описание проводилось. Также стоит отметить, что АРМ, входящие в ИС КИ имеют идентичную конфигурацию системного и программного обеспечения.

На основании информационного процесса обработки информации, составляющей КТ, структуры сети и перечня КИ была разработана структура информационных потоков в ИС КТ АО «ПО «Электроприбор», представленная на рисунке 10.

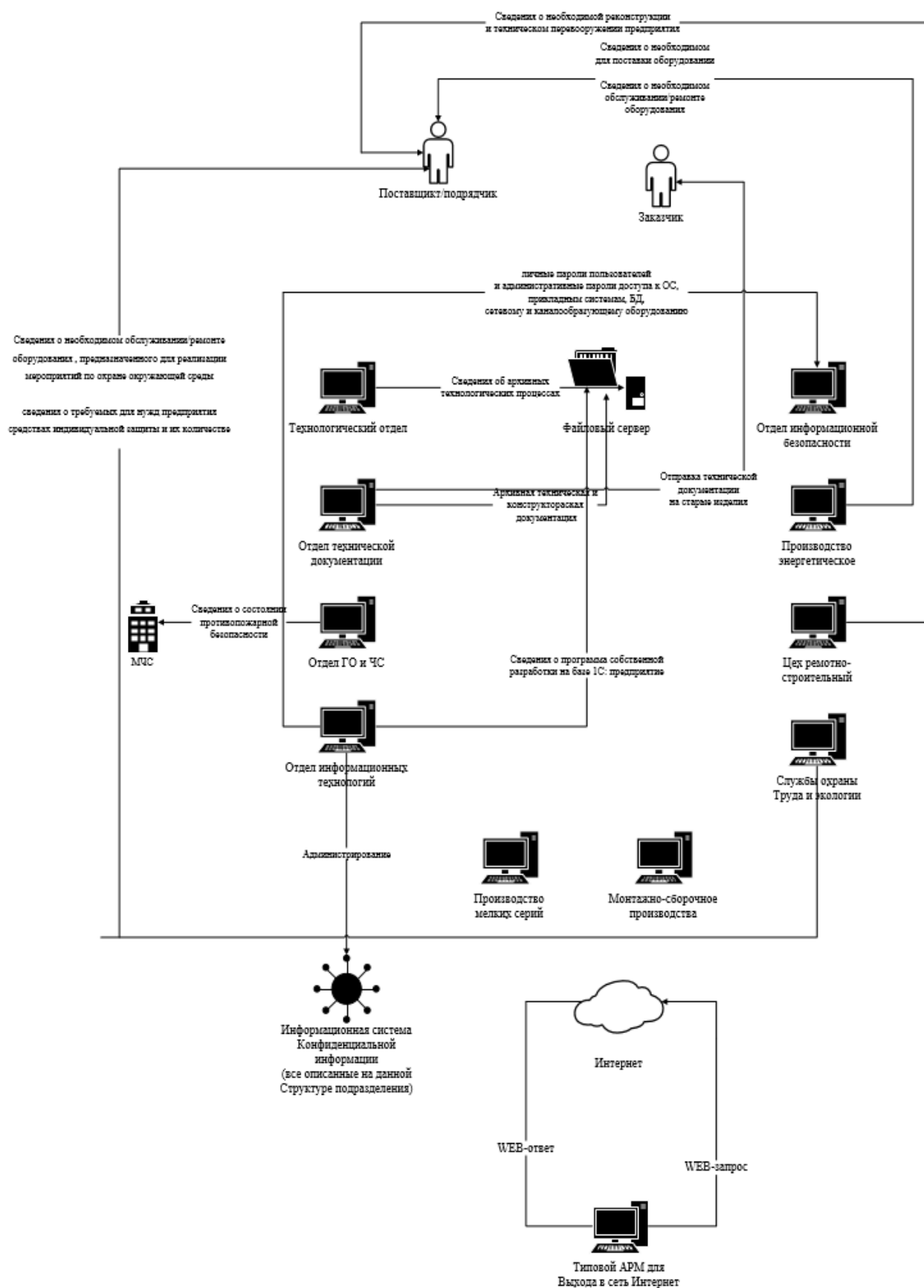


Рисунок 10 – Структура информационных потоков в ИС КИ АО «ПО «Электроприбор»

Для большей наглядности графического изображения, представленного на рисунке 10, на нём не отображалось телекоммуникационное оборудование и физические связи между ТС. Если какое-либо подразделение не имеет связи с другими элементами, то это означает, что обработка информации происходит лишь в пределах данного подразделения. Также на данной структуре приведена структура информационных потоков при взаимодействии выделенных АРМ с сетью Интернет.

4.3.1.2 Определение условий использования информации, составляющей КТ

На основании разработанной схемы информационных потоков, а также разработанного на предыдущих этапах перечня конфиденциальной информации, не являющейся КТ и ПДн АО «ПО «Электроприбор», была разработана матрица доступа к такой информации.

Целью разработки матрицы является определение групп лиц, допущенных к информации, составляющей КТ на законном основании, а также определить перечень разрешённых им действий в отношении данной информации. Разработанная матрица доступа представлена в таблице 11.

Таблица 11 – Матрица доступа к КИ АО «ПО «Электроприбор»

Подразделение с имеющейся в нём КИ	Группа доступа к КИ	Уровень доступа к КИ	Разрешённые действия
Технологический отдел	сотрудники технологического отдела	обладают всеми атрибутами и правами, обеспечивающими доступ к КИ для выполнения должностных обязанностей	хранение использование систематизация накопление
Отдел технической документации	сотрудники отдела технической документации	обладают всеми атрибутами и правами, обеспечивающими доступ к КИ для выполнения должностных обязанностей	хранение использование систематизация накопление

Продолжение таблицы 1 1

Подразделение с имеющейся в нём КИ	Группа доступа к КИ	Уровень доступа к КИ	Разрешённые действия
Отдел технической документации	заказчики	обладают необходимыми правами, обеспечивающими доступ к КИ на условиях заключённых контрактов	– использование; – хранение.
Отдел ГО ЧС	сотрудники отдела ГО ЧС	обладают всеми атрибутами и правами, обеспечивающими доступ к КИ для выполнения должностных обязанностей	– хранение; – использование; – накопление.
	сотрудники МЧС	обладают необходимыми правами в соответствии с законодательством РФ, обеспечивающими доступ к КИ	использование
Отдел информационных технологий	сотрудники отдела информационных технологий	обладают всеми необходимыми атрибутами и правами, обеспечивающими доступ к КИ для выполнения должностных обязанностей	– создание; – хранение; – использование; – накопление.
	сотрудники отдела информационной безопасности	обладают необходимыми атрибутами и правами, обеспечивающими доступ к КИ для выполнения должностных обязанностей	использование
Производство мелких серий	сотрудники производства мелких серий	обладают всеми атрибутами и правами, обеспечивающими доступ к КИ для выполнения должностных обязанностей	– использование; – хранение.
Монтажно–сборочное производство	сотрудники монтажно–сборочного производства	обладают всеми атрибутами и правами, обеспечивающими доступ к КИ для выполнения должностных обязанностей	– использование; – хранение.

Продолжение таблицы 1 1

Подразделение с имеющейся в нём КИ	Группа доступа к КИ	Уровень доступа к КИ	Разрешённые действия
Отдел информационной безопасности	сотрудники отдела информационной безопасности	обладают всеми атрибутами и правами, обеспечивающими доступ к КИ для выполнения должностных обязанностей	– использование; – хранение.
Производство энергетическое	сотрудники энергетического производства	обладают всеми атрибутами и правами, обеспечивающими доступ к КИ для выполнения должностных обязанностей	– использование; – хранение.
	поставщики/ подрядчики	обладают необходимыми правами, обеспечивающими доступ к КИ на условиях заключённых контрактов	использование
Цех ремонтно–строительный	сотрудники ремонтно–строительного цеха	обладают всеми атрибутами и правами, обеспечивающими доступ к КИ для выполнения должностных обязанностей	– использование; – хранение; – систематизация; – накопление.
	поставщики /подрядчики	обладают необходимыми правами, обеспечивающими доступ к КИ на условиях заключённых контрактов	– использование; – хранение.
Служба охраны труда и экологии	сотрудники службы охраны труда и экологии	обладают всеми атрибутами и правами, обеспечивающими доступ к КИ для выполнения должностных обязанностей	– использование; – хранение; – систематизация; – накопление.
	поставщики /подрядчики	обладают необходимыми правами, обеспечивающими доступ к КИ на условиях заключённых контрактов	– использование; – хранение.

4.3.2 Составление перечня угроз информационной безопасности для информационной системы иной конфиденциальной информации

Составление перечня угроз безопасности для конфиденциальной информации, не являющейся ПДн и КТ АО «ПО «Электроприбор», не проводилось, так как он идентичен перечню угроз ИБ для информации, составляющей КТ. в дальнейшем, при разработке модели угроз был использован именно этот перечень.

4.3.3 Идентификация актуальных угроз безопасности для иной конфиденциальной информации в АО «ПО «Электроприбор»

Так как информация, составляющая КТ, и иная КИ имеют общую структуру и схожую тематику, а также перечни угроз безопасности для обоих видов информации идентичны, угрозы актуальные для КТ были признаны актуальными и для КИ. Данное решение было принято экспертным методом, так как для рассматриваемого вида информации не разработано методического документа, определяющего порядок отнесения угроз безопасности к актуальным.

4.3.4 Разработка модели угроз безопасности для иной конфиденциальной информации

На основании принятого перечня угроз безопасности информации, и определения их актуальности была разработана модель угроз безопасности, приведённая в таблице А.8 приложения А. Данная модель содержит сочетание угроз ИБ, источника угрозы, а также нарушаемые свойства защищаемой информации, ущерб, наносимый в результате реализации угрозы, и степень актуальности угрозы.

4.3.4 Разработка модели нарушителя

После разработки модели угроз конфиденциальной информации, не являющейся ПДн и КТ АО «ПО «Электроприбор», была разработана модель нарушителя с целью описания возможностей и мотивации источников угроз, сведения о которых были приведены в модели угроз и частично были раскрыты. Разработка модели нарушителя производилась на основе проекта методического

документа ФСТЭК «Методика определения угроз безопасности в информационных системах». Результат представлен в таблице А.9 приложения А.

5 Выбор мер и средств защиты

5.1 Выбор мер и средств защиты для обеспечения безопасности персональных данных обрабатываемых в информационной системе персональных данных «Персонал»

5.1.1. Определение уровня защищённости информационной системы персональных данных «Персонал»

Степень защищённости ПДн, следовательно, и набор программных, программно–аппаратных и технических средств защиты зависит от требуемого уровня защищённости ПДн. Уровень их защищённости определяется на основании Постановления Правительства РФ от 01.11.2012 №1119 [4], при учитываются:

- категории обрабатываемых ПДн;
- категории субъектов ПДн и их количество;
- тип актуальных угроз безопасности.

в ИСПДн «Персонал» производится обработка специальных и иных категорий ПДн, категория субъектов ПДн – сотрудники, количество – менее 100 000, тип актуальных угроз – 3. На основании данных уровень защищённости ПДн в ИСПДн «Персонал» должен соответствовать **третьему** уровню. Также в соответствии с требованиями данного Постановления для ИСПДн такого уровня защищённости необходимо выполнение следующих требований:

- организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

- обеспечение сохранности носителей ПДн;
- утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к ПДн, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

- использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз;

- назначение должностного лица (работника), ответственного за обеспечение безопасности ПДн в информационной системе.

Приказ ФСТЭК №21 от 18.02.2013 «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [5] предъявляет следующие требования к сертифицированным по требованиям безопасности информации средствам защиты информации, применяемым для обеспечения третьего уровня защищённости персональных данных:

- средства вычислительной техники не ниже 5 класса;

- системы обнаружения вторжений и средства антивирусной защиты не ниже 4 класса защиты в случае актуальности угроз 2–го типа или взаимодействия информационной системы с информационно–телекоммуникационными сетями международного информационного обмена и системы обнаружения вторжений и средства антивирусной защиты не ниже 5 класса защиты в случае актуальности угроз 3–го типа и отсутствия взаимодействия информационной системы с информационно–телекоммуникационными сетями международного информационного обмена;

- межсетевые экраны не ниже 3 класса в случае актуальности угроз 2–го типа или взаимодействия информационной системы с информационно–телекоммуникационными сетями международного информационного обмена и межсетевые экраны не ниже 4 класса в случае актуальности угроз 3–го типа и отсутствия взаимодействия информационной системы с информационно–телекоммуникационными сетями международного информационного обмена.

Для ИСПДн «Персонал» актуальны требования по классу защищённости от НСД используемых СВТ, а также по классу защиты применяемых средств защиты.

Требование Постановления Правительства РФ №1119 о безопасности помещений, в которых проводится обработка ПДн в АО «ПО «Электроприбор» уже реализованы, так как на предприятии организована КЗ, данные помещения располагаются в её пределах, оборудованы сигнализациями и средства физической защиты (замки, прочные двери, решётки на окнах).

Меры по обеспечению сохранности носителей персональных данных описаны в «Об организации работы с персональными данными на АО «ПО «Электроприбор».

5.1.2 Разработка перечня защитных мер для обеспечения безопасности персональных данных

В соответствии с указанным выше приказом ФСТЭК №21 для обеспечения третьего уровня защищённости ПДн при их обработке в ИСПДн приводится базовых набор защитных мер, приведённый в таблице Б.1 приложения Б.

Далее для ИСПДн «Персонал» была проведена адаптация базового набора защитных мер на основе структурно–функциональных характеристик ИСПДн и уже имеющихся тех или иных защитных мер.

Был исключён набор защитных мер СОВ по обнаружению вторжений, так как ИСПДн не имеет подключения к сетям общего пользования, соответственно атаки, реализуемые из вне, для данной системы не актуальны.

Был исключен набор мер ЗСВ по защите среды виртуализации, так как средства виртуализации в рассматриваемой ИСПДн не используются.

Была исключена защитная мера ИАФ.6, так как наличие внешних пользователей в данной ИСПДн не предусмотрено.

Защитная мера УПД.1 была скорректирована таким образом, чтобы не включать в своей формулировке действия, направленные в отношении внешних пользователей, так как наличие таковых в данной ИСПДн не предусмотрено.

Были исключены защитные меры УПД.13–УПД.16, так как ИСПДн не имеет подключения к внешним сетям, в ней не предусмотрено использование технологии беспроводного доступа и мобильных технических средств, а также взаимодействие с информационными системами сторонних организаций.

Была исключена защитная мера ЗНИ.3, так как перемещение машинных носителей информации ПДн за пределы контролируемой зоны не предусмотрено.

Была исключена защитная мера ЗНИ.4, так как использование машинных носителей информации в иных ИС не предусмотрено.

Была исключена защитная мера АВЗ.1, так как антивирусная защита в ИСПДн уже реализована.

Были исключены защитные меры ОЦЛ.4 и ОЦЛ.5 так как ИСПДн не имеет подключения к внешним сетям.

Была исключена защитная мера ЗТС.2, так как на АО «ПО «Электроприбор» КЗ уже реализована.

Была исключена защитная мера ЗИС.3, так как ИСПДн «Персонал» не имеет каналов связи, выходящих за пределы КЗ.

Была исключена защитная мера ЗИС.5, так как на АРМ в ИСПДн «Персонал» не предусмотрено использование микрофонов, видеокамер, звукового оборудования.

Была исключена защитная мера ЗИС.7, так как использование технологии мобильного кода в рассматриваемой ИСПДн исключено.

Была исключена защитная мера ЗИС.4, так как все каналы связи находятся в пределах КЗ и автоматически удовлетворяют требованию доверенности.

Были исключены защитные меры ЗИС.8 и ЗИС.9, так как в ИСПДн «Персонал» не реализуются технологии передачи речи и видеоинформации.

Была исключена защитная мера ЗИС.20, так как в ИСПДн «Персонал» не используются беспроводные соединения.

Далее адаптированный базовый набор защитных мер был подвергнут уточнению, то есть были выбраны защитные меры, направленные на нейтрализацию уязвимостей актуальных угроз безопасности ПДн в ИСПДн «Персонал». Формулировки некоторых защитных мер были сопоставлены актуальным угрозам, уязвимостям, через которые они могут быть реализованы и защитным мер, нейтрализующих данные угрозы приведено в таблице 12.

Таблица 12 – Уточнённый набор защитных мер

Описание угрозы	Описание уязвимости	Описание защитной меры
Утечка видовой информации	не выключение экрана монитора при оставлении рабочего места	размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр
	расположение мониторов, позволяющее осуществить несанкционированный просмотр информации	
Кража носителей информации	слабость мер учёта и хранения носителей информации	учет машинных носителей персональных данных
		управление доступом к машинным носителям персональных данных
		организация надёжного хранения носителей информации
	халатность персонала, ответственного за те или иные носители информации	инструктирование персонала по вопросам обращения с носителями информации, содержащими ПДн
Уничтожение информации и её носителей	отсутствие механизмов резервного копирования информации	периодическое резервное копирование персональных данных
		учет машинных носителей персональных данных
		управление доступом к машинным носителям персональных данных
	отсутствие механизмов резервного копирования информации	организация надёжного хранения носителей информации
		периодическое резервное копирование персональных данных
	наличие у пользователя прав доступа, позволяющих реализовать данную угрозу	обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала
	отсутствие механизма контроля целостности	реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
		контроль целостности персональных данных,

Продолжение таблицы 12

Описание угрозы	Описание уязвимости	Описание защитной меры
Вывод из строя узлов ПЭВМ, каналов связи	отсутствие мер по предотвращению бесконтрольного доступа к системным блокам ПЭВМ	опечатывание системных блоков ПЭВМ размещение телекоммуникационного оборудования в специальных шкафах
	небрежная прокладка каналов связи	прокладка каналов связи, исключающая возможность их случайного «задевания»
	отсутствие аппаратного резервирования критически важных узлов и средств	резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования ИС
Несанкционированное отключение средств защиты	недостаточность контроля за действиями администратора	разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты персональных данных, функций по обработке персональных данных и иных функций информационной системы
	чрезмерное сосредоточение привилегий у одного лица	
Угроза внедрения кода или данных	недостаточный уровень осведомлённости персонала	осведомление пользователей о проблемах ВПО
	неактуальные базы данных признаков ВПО	обновление базы данных признаков вредоносных компьютерных программ (вирусов)
Выход из строя аппаратных и программных средств	несвоевременное или халатное обслуживание аппаратно– программных средств	контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование
	отсутствие аппаратного резервирования критических узлов системы	резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования ИС
	отсутствие процедур резервирования программного обеспечения	контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации
Разглашение ПДн	недостаточный уровень осведомлённости, обучения	осведомление сотрудников об ответственности за разглашение персональных данных
Утрата носителей информации и содержащейся на них информации	слабость мер учёта и хранения носителей информации	учет машинных носителей персональных данных
		организация надёжного хранения носителей информации
	отсутствие механизмов резервного копирования	периодическое резервное копирование персональных данных
Несанкционированное копирование БД ПДн или её частей	отсутствие механизмов, препятствующих несанкционированному копированию данных	контроль ввода (вывода) информации на машинные носители персональных данных
Модификация данных	отсутствие механизмов контроля целостности и резервного копирования	периодическое резервное копирование персональных данных на резервные машинные носители персональных данных
		обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала
		контроль целостности персональных данных, содержащихся в базах данных информационной системы

Для обеспечения реализации организационных защитных мер, а также иных мер из адаптированного перечня угроз была разработана инструкция администратора безопасности, представленная в приложении В.

5.1.3 Выбор средств защиты для обеспечения безопасности персональных данных

Для приведения ПЭВМ, входящих в состав ИСПДн «Персонал» к требуемому 5 классу защищённости, а также реализации части выбранных защитных мер рекомендуется использование СЗИ от НСД «Dallas Lock 8.0–К». Данное средство имеет сертификат ФСТЭК России № 2720 от 25.09.2012 г. и, действующий до 25.09.2018, на соответствие СЗИ НСД Dallas Lock 8.0–К 4 уровню контроля отсутствия НДВ, 5 классу защищенности от НСД, 3 классу защищенности МЭ, 4 классу защиты СКН. Также рекомендуется установка Сервера безопасности Dallas Lock 8.0–К для централизованного управления СЗИ, установленными на ПЭВМ пользователей. Также данный комплекс был выбран потому, что ориентирован на применение в ИСПДн и соответствует защитным мерам, описанным в 21 приказе ФСТЭК.

Антивирусная защита на ПЭВМ ИСПДн «Персонал» уже реализована. Антивирус Касперского 8.0 для Windows Servers Enterprise Edition имеет сертификат ФСТЭК № 2484, действующий до 18.11.2017, на соответствие ТУ и 2 уровню РД НДВ (может использоваться в ИСПДн до 1 класса). Антивирус Kaspersky Endpoint Security 8.0 для Windows имеет сертификат ФСТЭК № 2682, действующий до 26.07.2018 на соответствие ТУ и 2 уровню РД НДВ (может использоваться в ИСПДн до 1 класса).

Также выбранное средство Dallas Lock 8.0–К обеспечивает реализацию мер по идентификации и аутентификации, управлению доступа субъектов доступа к объектам доступа, регистрации событий безопасности.

5.2 Выбор мер и средств для обеспечения безопасности конфиденциальной информации, обрабатываемой в информационной системе коммерческой тайны

5.2.1 Разработка защитных мер для информации, составляющей коммерческую тайну

Аналогично с мероприятиями, проведённым для информационной системы персональных данных «Персонал» было реализовано сопоставление угроз безопасности, уязвимостей, через которые они могут быть реализованы и защитных мер, направленных на их нейтрализацию. Результат приведён в таблице 13. в качестве защитных мер, в частности, использовались меры, описанные для нейтрализации угроз безопасности персональных данных в ИСПДн «Персонал».

Таблица 13 – Сопоставление угроз, уязвимостей и защитных мер для информации, составляющей КТ

Описание угрозы	Описание уязвимости	Описание защитной меры
Утечка видовой информации	не выключение экрана монитора при оставлении рабочего места	размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр
	расположение мониторов, позволяющее осуществить несанкционированный просмотр информации	
Кража носителей информации	слабость мер учёта и хранения носителей информации	учет машинных носителей информации, составляющей КТ
		управление доступом к машинным носителям информации, составляющей КТ
		организация надёжного хранения носителей информации
		добавление в соглашения с контрагентами требований по организации режима защищённого хранения полученных носителей КТ
	халатность персонала, ответственного за те или иные носители информации	инструктирование персонала по вопросам обращения с носителями информации, содержащими информацию, составляющую КТ
	отсутствие механизмов резервного копирования информации	периодическое резервное копирование информации, составляющей КТ
Уничтожение информации и её носителей	слабость мер учёта и хранения носителей информации	учет машинных носителей информации, составляющей КТ
		управление доступом к машинным носителям информации, составляющей КТ

Продолжение таблицы 13

Описание угрозы	Описание уязвимости	Описание защитной меры
Уничтожение информации и её носителей	слабость мер учёта и хранения носителей информации	организация надёжного хранения носителей информации
	отсутствие механизмов резервного копирования информации	периодическое резервное копирование информации, составляющей КТ
		обеспечение возможности восстановления информации, составляющей КТ, с резервных машинных носителей КТ (резервных копий) в течение установленного временного интервала
	наличие у пользователя прав доступа, позволяющих реализовать данную угрозу	реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
Несанкционированное отключение средств защиты	отсутствие механизма контроля целостности	контроль целостности информации, составляющей КТ
	недостаточность контроля за действиями администратора	разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты КТ, функций по обработке КТ и иных функций информационной системы
Угроза внедрения кода или данных	чрезмерное сосредоточение привилегий у одного лица	разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты КТ, функций по обработке КТ и иных функций информационной системы
	недостаточный уровень осведомлённости персонала	осведомление пользователей о проблемах ВПО
	отсутствие средств антивирусной защиты и/или неактуальные базы данных признаков ВПО	обновление базы данных признаков вредоносных компьютерных программ (вирусов) рекомендации контрагентам по установке антивирусных средств или поддержанию в актуальном состоянии баз признаков ВПО
Выход из строя аппаратных и программных средств	несвоевременное или халатное обслуживание аппаратно – программных средств	контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование
	отсутствие аппаратного резервирования критических узлов системы	резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования ИС
	отсутствие процедур резервирования программного обеспечения	контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации
Разглашение информации, составляющей КТ	недостаточный уровень осведомлённости, обучения	осведомление сотрудников об ответственности за разглашение информации, составляющей КТ
		заключение с контрагентами соглашений о конфиденциальности и информирование их об ответственности за нарушение конфиденциальности информации, составляющей КТ
Несанкционированное копирование БД информации, составляющей КТ или её частей, а также информации с файлового сервера	отсутствие механизмов, препятствующих несанкционированному копированию данных	контроль ввода (вывода) информации на машинные носители КТ
		рекомендации контрагентам по использованию соответствующих средств защиты

Продолжение таблицы 13

Описание угрозы	Описание уязвимости	Описание защитной меры
Несанкционированное копирование БД информации, составляющей КТ или её частей, а также информации с файлового сервера	отсутствие механизмов, препятствующих несанкционированному копированию данных	заключение с контрагентами соглашений о конфиденциальности и информирование их об ответственности за нарушение конфиденциальности информации, составляющей КТ
Модификация данных	отсутствие механизмов контроля целостности и резервного копирования	периодическое резервное копирование информации, составляющей КТ, на резервные машинные носители КТ
		обеспечение возможности восстановления информации, составляющей КТ с резервных машинных носителей КТ (резервных копий) в течение установленного временного интервала
		контроль целостности информации, составляющей коммерческую, содержащихся в базах данных ИС и файловом сервере

5.2.2 Выбор средств защиты для обеспечения безопасности информации, составляющей коммерческую тайну

В соответствии с рекомендациями, описанными в документе «Специальные требования и рекомендации по технической защите конфиденциальной информации» было принято решение в ИС КТ реализовать защитные меры в соответствии с требованиями к классу защищённости АС 1Г, описанные в РД ФСТЭК «Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации» [6].

Для реализации данных требований, а также части описанных ранее защитных мер рекомендуется использование СЗИ от НСД Dallas Lock 8.0–К. Также рекомендуется установка Сервера безопасности Dallas Lock 8.0–К для централизованного управления СЗИ, установленными на ПЭВМ пользователей.

Антивирусная защита на ПЭВМ, входящих в ИС КТ реализована использованием сертифицированного антивируса Kaspersky Endpoint Security 8.0 для Windows.

Для ИС КТ также действительна инструкция администратора безопасности, разработанная для ИСПДн «Персонал».

5.3 Выбор мер и средств защиты для конфиденциальной информации, обрабатываемой в информационной системе конфиденциальной информации

Как было выявлено ранее, ИС КИ физически имеет общую часть с ИС КТ, иная конфиденциальная информация по своей структуре схожа с информацией, составляющей КТ, а также для данной информации составлена идентичная модель угроз, следовательно, рекомендуется применять те же защитные меры, средства и инструкции, их описывающие, применяемые для защиты информации, составляющей КТ в ИС КТ.

6 Разработка документации

На заключительном этапе помимо были разработаны документы, необходимые для выполнения требований законодательства, а также отражающие общие принципы по обеспечению безопасности конфиденциальной информации как в целом, так и по конкретному виду. Политика по защите конфиденциальной информации представлена в приложении А. Инструкция по соблюдению режима конфиденциальности представлена в приложении Г. Положение «О коммерческой тайне» представлено в приложении Д. Положение «Об организации работы с персональными данными», приведённое в приложении Е. На рисунках Ж.1 и Ж.2 приложения Ж приведён скан проекта приказа об утверждении перечня лиц, доступ которых к персональным данным, обрабатываемым в ИСПДн «Персонал», необходим для выполнения ими служебных (трудовых) обязанностей. На рисунке И.1 приложения И приведён скан проекта приказа о назначении ответственного за организацию обработки персональных данных в ИСПДн «Персонал».

ЗАКЛЮЧЕНИЕ

Разработанная политика по защите конфиденциальной информации устанавливает основные правила, требования и руководящие принципы в области обеспечения безопасности конфиденциальной информации в АО «ПО «Электроприбор». Положениями данной политики и сопровождающими её документами руководствуются все работники предприятия, в том числе ответственные за реализацию мероприятий по защите информации, а также звено управления.

В ходе выполнения дипломного проекта была идентифицирована организационная структура АО «ПО «Электроприбор», составлены перечни конфиденциальной информации, обрабатываемой на предприятии и определены уровни её значимости. Было произведена оценка исходной защищённости информационных систем, по итогам которой были разработаны модели угроз безопасности для каждого вида конфиденциальной информации. На основе перечня актуальных угроз были выбраны защитные меры, предложены средства для их реализации и разработаны проекты необходимых документов.

Таким образом, все пункты технического задания на выпускную квалификационную работу выполнены полностью.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 АО «ПО «Электроприбор». О предприятии. [Электронный ресурс] – URL: <http://www.electropribor-penza.ru>, свободный

2 Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: утверждена заместителем директора ФСТЭК России 15 фев. 2008г. URL: <http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/379-bazovaya-model-ugroz-h-vypiska-fstek-rossii-2008-god> (дата обращения: 12.04.2016)

3 Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: утверждена заместителем директора ФСТЭК России 14 фев. 2008г. URL: <http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380-metodika-opredeleniya-aktualnykh-ugroz-bezopasnosti-personalnykh-dannykh-fstek-rossii-2008-god> (дата обращения: 15.04.2016).

4 Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных (постановление Правительства РФ от 1 нояб. 2012г. № 1119). Доступ из справ. – правовой системы «КонсультантПлюс».

5 Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных (приказ ФСТЭК от 18 фев. 2013г. № 21). Доступ из справ. – правовой системы «КонсультантПлюс».

6 Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Руководящий документ [Электронный ресурс]: утвержден председателем Государственной технической комиссии при Президенте РФ 30 марта 1992г. URL: <http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/384->

rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g (дата обращения: 20.04.2016).

7 Российская Федерация. Законы. О персональных данных [Текст]: федер. закон [принят Гос. Думой 8 июля 2006г.: одобр. Советом Федерации 14 июля 2006г]. – М.: Российская газета, 2006. – 21с. – (Актуальный закон).

8 Российская Федерация. Законы. О коммерческой тайне [Текст]: федер. закон [принят Гос. Думой 9 июля 2004г.: одобр. Советом Федерации 15 июля 2004г]. – М.: Российская газета, 2004. – 7с. – (Актуальный закон).

9 Российская Федерация. Законы. Об информации, информационных технологиях и защите информации [Текст]: федер. закон [принят Гос. Думой 8 июля 2006г.: одобр. Советом Федерации 14 июля 2006г]. – М.: Российская газета, 2006 – 19с. – (Актуальный закон).

10 Специальные технические требования и рекомендации по технической защите конфиденциальной информации [Электронный ресурс]: Решение Коллегии Гостехкомиссии России от 2 марта 2001г. URL: http://www.rfcmd.ru/sphider/docs/InfoSec/RD_FSTEK_requirements.htm

11 Об утверждении перечня сведений конфиденциального характера (указ Президента Российской Федерации от 6 марта 1997г №188). Доступ из справ. – правовой системы «КонсультантПлюс».

12 Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации (постановление Правительства РФ от 15 сент. 2008г. № 687). Доступ из справ. – правовой системы «КонсультантПлюс».

13 Российская Федерация. Конституция (1993). Конституция Российской Федерации [Текст]: офиц. текст. – М.: Маркетинг, 2001. – 39с. – 10000 экз.

14 Российская Федерация. Законы. Трудовой кодекс Российской Федерации [Текст]: федер. закон [принят Гос. Думой 21 дек. 2001г.: одобр. Советом Федерации 26 дек. 2001г]. – [5-е изд.]. – М. Ось-89, [2001]. – 340 с. – (Актуальный закон).

ПРИЛОЖЕНИЕ А

(обязательное)

Политика по защите конфиденциальной информации

А.1 Общие положения

Настоящая политика определяет основные цели и принципы по обеспечению безопасности конфиденциальной информации в Акционерном обществе «Пензенское производственное объединение «Электроприбор» и устанавливает основные правила, требования и руководящие принципы в области обеспечения безопасности конфиденциальной информации, которыми руководствуются работники предприятия, имеющие доступ к такой информации.

А.2 Цели защиты конфиденциальной информации

Целью защиты конфиденциальной информации в АО «ПО «Электроприбор» является достижение и поддержание требуемого уровня безопасности такой информации в соответствии с требованиями законодательства, документов, разрабатываемых органами исполнительной власти, уполномоченными в области обеспечения безопасности информации, а также внутренних стандартов и стандартов вышестоящих организаций.

А.3 Область действия

Действие данной политики распространяется на следующие объекты:

- персональные данные работников АО «ПО «Электроприбор», обрабатываемых в ИСПДн «Персонал»;
- информацию, составляющую коммерческую тайну АО «ПО «Электроприбор», обрабатываемую в ИС КТ и передаваемую контрагентам с целью обеспечения выполнения договорных обязательств;
- иную конфиденциальную информацию, распространение которой ограничено нормативными актами АО «ПО «Электроприбор» и вышестоящих организаций, обрабатываемую в ИС КИ и передаваемую контрагентам с целью обеспечения выполнения договорных обязательств.

А.3.1 Критерии определения значимости объектов защиты

Критерием определения значимости для ПДн, обрабатываемых в подразделениях АО «ПО «Электроприбор» является их категория в соответствии с ФЗ № 152 «О персональных данных» [7]. Выделяются следующие категории ПДн:

- ПДн, включаемые с согласия их субъекта в общедоступные источники персональных данных (ПДн–О);
- ПДн специальной категории – ПДн, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни (ПДн–С);
- биометрические ПДн – сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных (ПДн–Б);
- иные категории ПДн – ПДн не являющиеся биометрическими, специальных категорий и, не входящие в общедоступные источники ПДн (ПДн–И).

Для определения значимости (ценности) информации, составляющей коммерческую тайну АО «ПО «Электроприбор» в организации принято делить такую информацию на 2 группы:

- 1 группа – сведения, разглашение которых влечет за собой существенный экономический ущерб во всех сферах и направлениях деятельности организации;
- 2 группа – сведения, разглашение которых приводит к экономическому ущербу в отдельной сфере (нескольких сферах) или направлениях деятельности организации.

Для определения значимости конфиденциальной информации, являющейся собственностью АО «ПО «Электроприбор», в организации принято, делить данный вид информации, также, как и КТ на 2 группы:

– 1 группа – сведения, разглашение которых влечет за собой существенный ущерб любого характера (материального и не материального) во всех сферах и направлениях деятельности организации;

– 2 группа – сведения, разглашение которых приводит к ущербу любого характера (материального и не материального) в отдельной сфере (нескольких сферах) или направлениях деятельности организации.

Перечень объектов защиты с определённым уровнем значимости (ценности) представлен в таблицах А.1 – А.3.

Таблица А.1 – Значимость ПДн

Подразделение	Пункт ПДн	Категория ПДн
Бухгалтерия	ФИО, дата и место рождения	ПДн–И
	паспортные данные(серия, номер, дата выдачи и иные паспортные данные)	ПДн–И
	сведения о заработной плате (номер счёта для расчёта с работниками, данные зарплатных договоров с клиентами, в том числе номера их спецкартсчетов, данные по окладу, надбавкам, долгам)	ПДн–И
	сведения о номере и серии страхового свидетельства государственного пенсионного страхования	ПДн–И
	сведения об идентификационном номере налогоплательщика	ПДн–И
	сведения о соц. льготах и о социальном статусе (серия, номер, дата выдачи, наименование органа, выдающего документ, являющийся основанием для предоставления льгот и статус, и другие сведения)	ПДн–И
	сведения о временной нетрудоспособности работника	ПДн–С
Отдел кадров	ФИО, дата и место рождения	ПДн–И
	паспортные данные (серия, номер, дата выдачи и т. д.)	ПДн–И
	номера телефонов (моб и дом), в случае их регистрации на работника или по адресу его места жительства (по паспорту)	ПДн–И

Продолжение таблицы А. 1

Подразделение	Пункт ПДн	Категория ПДн
Отдел кадров	сведения об образовании, квалификации, наличии спец. Знаний или спец. Подготовки (серия, номер, дата выдачи диплома, свидетельства, аттестата или другого документа об окончании образовательного учреждения, в том числе наименование и местоположение образовательного учреждения, дата начала и завершения обучения, факультет или отделение, квалификация и специальность по окончании образовательного учреждения, учёная степень, учёное звание, владение иностранным языком)	ПДн–И
	сведения о повышении квалификации и переподготовке (серия, номер, дата выдачи документа о повышении квалификации или о переподготовке, наименовании и местоположение образовательного учреждения, дата начала и завершения обучения, квалификация и специальность по окончании образовательного учреждения)	ПДн–И
	сведения о трудовой деятельности (данные о трудовой занятости на текущее время с полным указанием должности, подразделения, организации и ее наименовании, ИНН, адрес и телефон, а также реквизитов других организаций с полным наименованием занимаемых ранее в них должностей и времени работы в этих организациях)	ПДн–И
	сведения о номере, серии и дате выдачи трудовой книжки и записях в неё	ПДн–И
Отдел труда и зарплаты	ФИО, дата и место рождения	ПДн–И

Продолжение таблицы А. 1

Подразделение	Пункт ПДн	Категория ПДн
Отдел труда и зарплаты	сведения о трудовой деятельности (данные о трудовой занятости на текущее время с полным указанием должности, подразделения, организации и её наименования, ИНН, адрес и телефон, а также реквизитов других организаций с полными наименованиями занимаемых ранее в них должностей и времени работы в этих организациях, а также другие сведения	ПДн–И
	сведения, указанные в оригинальных и копиях приказов по личному составу организации и материалах к ним	ПДн–И
	сведения о заработной плате (данные по окладу, надбавкам, премиям)	ПДн–И
	табельный номер работника организации	ПДн–И

Таблица А.2 – Значимость информации, составляющей коммерческую тайну

Подразделение	Пункт КТ	Ценность КТ
Конструкторский отдел	схемы и чертежи, а также любые сведения о новых разработках	2гр
Конструкторский отдел	алгоритмы (в т.ч. блок–схемы) разработанного и вновь разрабатываемого ПО	2гр
	исходные коды разработанного и вновь разрабатываемого ПО	2гр
Технологический отдел	сводные сведения о новых (перспективных) технологиях и конструктивных решениях, разработанных организацией и используемых при проектировании и изготовлении продукции	2гр
Отдел технической документации	техническая документация на изготавливаемые изделия	1гр

Продолжение таблицы А.2

Подразделение	Пункт КТ	Ценность КТ
Юридический отдел	сведения о заключаемых договорах (кроме подлежащих опубликованию в соответствии с положением о гос. закупках)	2гр
	сведения об организациях и предприятиях, с которым были заключены и планируется заключение договоров	2гр
Канцелярия	сведения о порядке, методах и средствах ведения делопроизводства на предприятии	2гр
Отдел снабжения	уровень запасов, материалов и комплектующих	1гр
	данные о резервах сырья на предприятии	1гр
Бухгалтерия	бухгалтерская отчётность до её официального опубликования в соответствии с законодательством РФ	1гр
	прибыль предприятия и направления её использования	1гр
	сведения о финансовых операциях предприятия	1гр
	размеры и условия банковских кредитов	1гр
	развёрнутые сведения стоимости; основных и оборотных фондов предприятия	1гр
Планово– экономический отдел	стратегические и тактические планы по развитию предприятия	1гр
	сведения о планах предприятия по расширению производства и другие коммерческие замыслы	1гр
	сведения, раскрывающие плановые и фактические показатели финансового плана, не содержащиеся в открытых источниках	1гр
	плановая себестоимость, объёмы производства	1гр
	прибыль предприятия и направления её использования	1гр
Отдел ГО и ЧС	схема систем пожаротушения и сигнализации	1гр

Продолжение таблицы А.2

Подразделение	Пункт КТ	Ценность КТ
Отдел маркетинга	Отчёты о собственных маркетинговых исследованиях рынка	1гр
	сведения о конкретных направлениях в торговой политике	2гр
	сведения об объемах реализации	1гр
Отдел информационных технологий	настройки и конфигурации серверного, сетевого и каналобразующего оборудования ЛВС организации	1гр
	стратегические и тактические планы развития сетевой инфраструктуры	1гр
	сведения о рисках и уязвимостях АС	1гр
Отдел информационной безопасности	регламенты, планы, задания подразделения обеспечения безопасности информации	2гр
	информация о состоянии систем защиты информации в организации	1гр
Отдел информационной безопасности	сведения о структуре, принципах и технических решениях, используемых в системах обеспечения безопасности информации	1гр
	сведения о местах, порядке хранения документов, содержащих сведения, составляющие коммерческую тайну, а также их учёте	1гр
	секретные (закрытые) ключи электронной цифровой подписи и порядок их учёта, хранения	2гр
Производство энергетическое	схемы систем отопления и кондиционирования (за исключением схем отопления для вП, ОИ и без привязки к схеме КЗ)	1гр
	схема систем электропитания (для отдельных помещений и без привязки к схеме КЗ)	2гр
Механо–сборочное производство	сведения о производственных возможностях	2гр
	данные о типе и размещении оборудования	2гр
Производство мелких серий	сведения о производственных возможностях	2гр

Таблица А.3 – Значимость иной конфиденциальной информации

Подразделение	Пункт КИ	Ценность КИ
Производство мелких серий	данные о типе и размещении оборудования	2гр
Технологический отдел	архив технологических процессов	2гр
	сведения о конфигурации ПО для фрезерных станков с ЧПУ	2гр
	сведения о конфигурации ПО для станков с ЧПУ по листообработке	2гр
	сведения о конфигурации ПО для гравировочных станков с ЧПУ	2гр
	сведения о конфигурации ПО для станков с ЧПУ токарной обработки	2гр
Отдел технической документации	архив технической документации	2гр
	информация на электронным носителях, хранящихся в архиве	2гр
	архив конструкторской документации	2гр
Отдел ГО и ЧС	информация о состоянии ГО и ПБ	1гр
Отдел информационных технологий	личные пароли пользователей и административные пароли доступа к ОС, прикладным системам, БД, сетевому и каналобразующему оборудованию	2гр
	положение о порядке пользования сетью интернет на предприятии	2гр
	положение о резервном копировании БД	2гр
	сведения о программах собственной разработки на базе 1С: предприятие	2гр
Отдел информационной безопасности	личные пароли пользователей и административные пароли доступа к ОС, прикладным системам, БД, сетевому и каналобразующему оборудованию	2гр
Производство энергетическое	информация, хранящаяся на жёстком диске системного блока №1324 котельной	2гр
	информация, хранящаяся на жёстком диске системного блока №2741 участка эксплуатации	2гр
Монтажно–сборочное производство	сведения о конфигурации используемого ПО	2гр
Производство мелких серий	сведения по комплектованию изделий ДСЕ	2гр
	сведения о трудоёмкости производства	2гр

Продолжение таблицы А.3

Подразделение	Пункт КИ	Ценность КИ
Цех ремонтно–строительный	проекты на реконструкцию и техническое перевооружение предприятия	2гр

А.3.2 Информационные системы

Обработка конфиденциальной информации в АО «ПО «Электроприбор» производится в 3–х информационных системах:

- ИСПДн «Персонал» – обработка персональных данных;
- ИС КТ – обработка информации, составляющей коммерческую тайну АО «ПО «Электроприбор»;
- ИС КИ – обработка иной конфиденциальной информации.

Структуры процессов обработки информации в информационных системах приведены на рисунках А.1–А.3.



Рисунок А.1 –Процесса обработки ПДн сотрудников предприятия

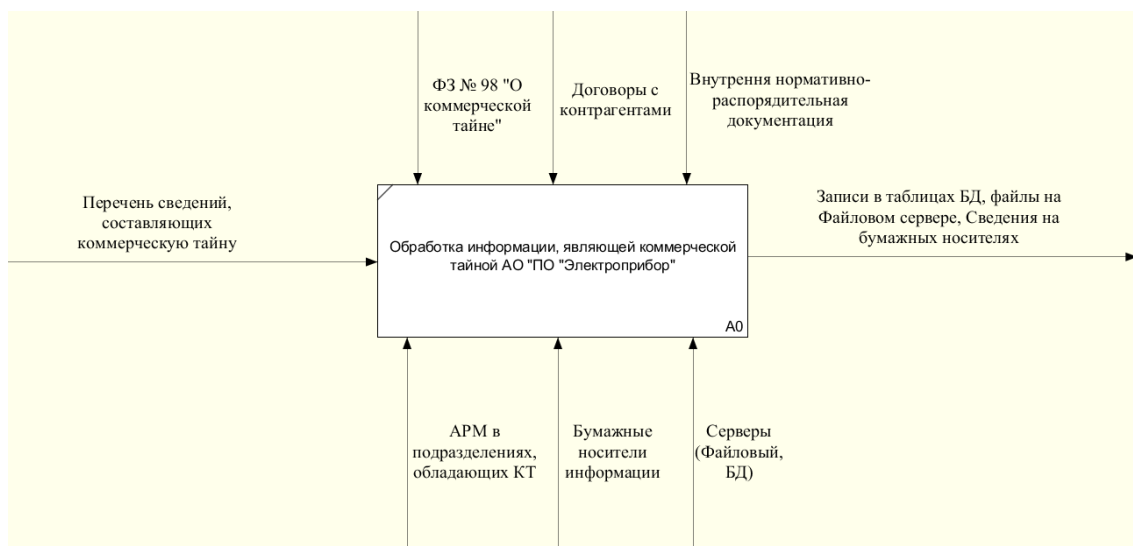


Рисунок А.3 – Информационный процесс обработки информации, составляющей коммерческую тайну АО «ПО «Электроприбор»

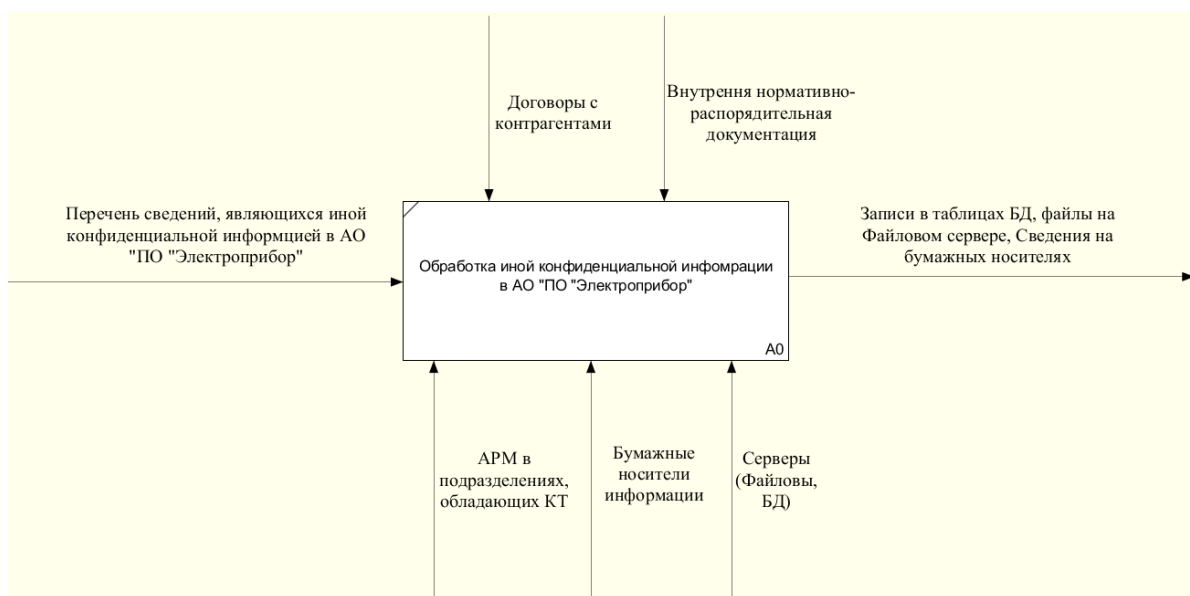


Рисунок А.3 – Информационный процесс обработки иной конфиденциальной информации в АО «ПО «Электроприбор»

4 Угрозы безопасности, связанные с объектами защиты

Модели угроз и нарушителя, связанные с объектами защиты, определёнными данной политикой приведены в таблицах А.4 – А.9.

Таблица А.4 – Модель угроз безопасности ПДн в ИСПДн «Персонал»

Описание угрозы	вероятность реализации угрозы (Y2)	Коэффициент реализуемости (возможность реализации) угрозы (Y)	Опасность угрозы	Актуальность угрозы	Последствия	Тип угрозы
Утечка видовой информации	средняя	средняя	средняя	актуальная	К	3
Кража носителей информации	низкая	средняя	высокая	актуальная	К, Ц	3
Уничтожение информации и её носителей	низкая	средняя	высокая	актуальная	Ц, Д	3
Вывод из строя узлов ПЭВМ, каналов связи	низкая	средняя	средняя	актуальная	Ц, Д	3
Несанкционированное отключение средств защиты	низкая	средняя	высокая	актуальная	К, Ц	3
Угроза внедрения кода или данных	высокая	высокая	высокая	актуальная	Ц, Д	3
Установка ПО, не связанного с использованием в целях выполнения должностных обязанностей	маловероятно	низкая	средняя	неактуальная	Ц, Д	2
Утрата ключей и атрибутов доступа	низкая	средняя	низкая	неактуальная	Д	3
Непреднамеренная модификация (уничтожение) данных	низкая	средняя	низкая	неактуальная	Ц	3
Непреднамеренное отключение средств защиты	маловероятно	низкая	средняя	неактуальная	Ц, Д	3
Выход из строя аппаратных и программных средств	низкая	средняя	средняя	актуальная	Д	3
Разглашение ПДн	средняя	средняя	высокая	актуальная	К	3
Утрата носителей информации и содержащейся на них информации	маловероятно	низкая	высокая	актуальная	К	3
Несанкционированное копирование БД ПДн или её частей	низкая	средняя	высокая	актуальная	К	3
Обхода некорректно настроенных механизмов аутентификации	маловероятно	низкая	средняя	неактуальная	К, Ц, Д	3
Модификация (уничтожение) данных	низкая	средняя	высокая	актуальная	Ц	3

Таблица А.5 – Модель нарушителя в ИСПДн «Персонал»

Описание угрозы	Вид нарушителя	Тип нарушителя	возможные цели, мотивация	Потенциал нарушителя
Утечка видовой информации	пользователи информационной системы	внутренний	– непреднамеренные неосторожные или неквалифицированные действия; – месть; – любопытство.	низкий
Кража носителей информации	пользователи информационной системы	внутренний	– действия вследствие подкупа; – месть; – действия в личных целях.	низкий
	сотрудники не являющиеся пользователями информационной системы			
Уничтожение информации и её носителей	пользователи информационной системы	внутренний	– действия вследствие подкупа; – месть.	низкий
	администраторы информационной системы и администраторы безопасности			средний
	сотрудники, не являющиеся пользователями информационной системы	внутренний	– действия вследствие подкупа; – месть.	низкий
Вывод из строя узлов ПЭВМ, каналов связи	пользователи информационной системы	внутренний	– непреднамеренные неосторожные или неквалифицированные действия; – месть.	низкий
	администраторы информационной системы и администраторы безопасности			средний
	сотрудники, не являющиеся пользователями информационной системы			низкий
	лица, обслуживающие инфраструктуру оператора (охрана, уборщики...)			низкий
Несанкционированное отключение средств защиты	администраторы информационной системы и администраторы безопасности	внутренний	– месть. – действия вследствие подкупа; – действия в личных целях.	средний
Угроза внедрения кода или данных	администраторы информационной системы и администраторы безопасности	внутренний	– непреднамеренные неосторожные или неквалифицированные действия; – месть; – действия вследствие подкупа.	средний
	пользователи информационной системы			низкий
Установка ПО, не связанного с использованием в целях выполнения должностных обязанностей	пользователи информационной системы	внутренний	неквалифицированные действия пользователей	низкий

Продолжение таблицы А.5

Описание угрозы	Вид нарушителя	Тип нарушителя	возможные цели, мотивация	Потенциал нарушителя
Утрата ключей и атрибутов доступа	пользователи информационной системы	внутренний	непреднамеренные неосторожные действия	низкий
	администраторы информационной системы и администраторы безопасности			средний
Непреднамеренная модификация (уничтожение) данных	пользователи информационной системы	внутренний	неосторожные или неквалифицированные действия	низкий
	администраторы информационной системы и администраторы безопасности		непреднамеренные неосторожные или неквалифицированные действия	средний
Непреднамеренное отключение средств защиты	администраторы информационной системы и администраторы безопасности	внутренний	непреднамеренные неосторожные или неквалифицированные действия	средний
Выход из строя аппаратных и программных средств	администраторы информационной системы и администраторы безопасности	внутренний	неквалифицированные действия	средний

Таблица А.6 – Модель угроз безопасности информации, составляющей коммерческую тайну

Описание угрозы	Источник угрозы	Нарушаемые свойства безопасности информации	Вероятный ущерб	Актуальность угрозы
Утечка видовой информации	внутренние (персонал, не имеющий доступа к защищаемой информации)	К	– финансовые потери; – упущение коммерческой выгоды.	актуальная
	внешние (персонал контрагента, не имеющий доступ к защищаемой информации)			
Кража носителей информации	внутренние (персонал, имеющий доступ к защищаемой информации)	К	– финансовые потери; – упущение коммерческой выгоды.	актуальная
	внутренние (персонал, имеющий доступ в КЗ, но не имеющий доступ к защищаемой информации)			
	внешние (персонал контрагента)			
Уничтожение информации и её носителей	внутренние (персонал, имеющий доступ к защищаемой информации; персонал, осуществляющий администрирование ИСПДн).	Ц	–приостановление или затруднение отдельных видов деятельности; –финансовые потери;	актуальная

Продолжение таблицы А.6

Описание угрозы	Источник угрозы	Нарушаемые свойства безопасности информации	Вероятный ущерб	Актуальность угрозы
Уничтожение информации и её носителей	внутренние (персонал, имеющий доступ к КЗ, но не имеющий доступ к защищаемой информации)	Ц	репутационные потери	актуальная
Вывод из строя узлов ПЭВМ, каналов связи	внутренние (персонал, имеющий доступ к защищаемой информации; персонал, осуществляющий администрирование ИСПДн)	Д	незначительные временные затраты сотрудников нескольких подразделений и время простоя	неактуальная
	внутренние (персонал, имеющий доступ к КЗ, но не имеющий доступ к защищаемой информации)			
Несанкционированное отключение средств защиты	внутренние (персонал, осуществляющий администрирование ИСПДн)	К, Ц	– финансовые потери; – непредвиденные временные затраты.	актуальная
Угроза внедрения кода или данных	внутренние	Ц	– финансовые потери; – упущение коммерческой выгоды.	актуальная
	внешние	Ц, К		
Непреднамеренная модификация (уничтожение) данных	внутренние (персонал, имеющий доступ к защищаемой информации);	Ц	незначительные временные затраты отдельных подразделений	неактуальная
	внутренние (персонал, осуществляющий администрирование ИСПДн)			
Установка ПО, не связанного с использованием в целях выполнения должностных обязанностей	внутренние	Ц, Д	незначительные временные затраты отдельных подразделений	неактуальная
Непреднамеренное отключение средств защиты	внутренние (персонал, осуществляющий администрирование ИСПДн)	Ц, Д	незначительные временные затраты отдельных подразделений	неактуальная
Утрата ключей и атрибутов доступа	внутренние	Д	незначительные временные затраты отдельных подразделений и незначительное время простоя	неактуальная
Разглашение информации, составляющей КТ	внутренние (персонал, имеющий доступ к защищаемой информации, персонал)	К	– финансовые потери – упущение коммерческой выгоды.	актуальная

Продолжение таблицы А.6

Описание угрозы	Источник угрозы	Нарушаемые свойства безопасности информации	Вероятный ущерб	Актуальность угрозы
Разглашение информации, составляющей КТ	внешние (персонал контрагента, имеющий доступ к защищаемой информации)	К	финансовые потери упущение коммерческой выгоды	актуальная
Выход из строя аппаратных и программных средств	внутренние (персонал, осуществляющий администрирование ИСПДн)	Д	незначительные временные затраты отдельных подразделений и незначительное время простоя.	неактуальная
Утрата носителей информации	внутренние (персонал, имеющий доступ к защищаемой информации)	К	То же	неактуальная
Несанкционированное копирование БД информации, составляющей КТ или её частей, а также информации с файлового сервера	внутренние (персонал, имеющий доступ к защищаемой информации)	К	– существенные финансовые потери; – утеря коммерческой выгоды.	актуальная
	внутренние (персонал, осуществляющий администрирование ИСПДн)			
	внешние (персонал контрагента, имеющий доступ к защищаемой информации)			
Обход некорректно настроенных механизмов аутентификации	внутренние (персонал, не имеющий доступ к защищаемой информации)	К, Ц, Д	–	неактуальная
Модификация данных	внутренние (персонал, имеющий доступ к защищаемой информации)	Ц	– финансовые потери; – упущение коммерческой выгоды.	актуальная

Таблица А.7 – Модель нарушителя для информации, составляющей КТ АО «ПЮ «Электроприбор»

Описание угрозы	Вид нарушителя	Тип нарушителя	Возможные цели, мотивация	Потенциал нарушителя
Утечка видовой информации	пользователи информационной системы	внутренний	– действия вследствие подкупа заинтересованными лицами или организаций; – действия с целью передачи заинтересованным лицам за вознаграждение.	низкий
Кража носителей информации	пользователи информационной системы	внутренний	– действия вследствие подкупа заинтересованными лицами или организаций;	низкий

Продолжение таблицы А.7

Описание угрозы	Вид нарушителя	Тип нарушителя	Возможные цели, мотивация	Потенциал нарушителя
Кража носителей информации	сотрудники, не являющиеся пользователями информационной системы	внутренний	действия с целью передачи заинтересованным лицам за вознаграждение.	низкий
	лица, обслуживающие инфраструктуру оператора (охрана, уборщики...)			
Уничтожение информации и её носителей	пользователи информационной системы	внутренний	– действия вследствие подкупа заинтересованными лицами или организаций; – месть.	низкий
	администраторы информационной системы и администраторы безопасности			средний
	лица, обслуживающие инфраструктуру оператора (охрана, уборщики...)			низкий
Вывод из строя узлов ПЭВМ, каналов связи	пользователи информационной системы	внутренний	– непреднамеренные неосторожные или неквалифицированные действия; – месть.	низкий
	администраторы информационной системы и администраторы безопасности			средний
	внутренние (персонал, имеющий доступ к КЗ, но не имеющий доступ к защищаемой информации)			низкий
Несанкционированное отключение средств защиты	администраторы информационной системы и администраторы безопасности	внутренний	– месть; – действия вследствие подкупа; – действия в личных целях.	средний
Угроза внедрения кода или данных	администраторы информационной системы и администраторы безопасности	внутренний	– непреднамеренные неосторожные или неквалифицированные действия; – месть; – действия вследствие подкупа.	средний
	пользователи информационной системы			низкий
	пользователи информационной контрагента/заказчика	внешний		низкий
Непреднамеренная модификация (уничтожение) данных	администраторы информационной системы и администраторы безопасности	внутренний	непреднамеренные неосторожные действия	средний
	пользователи информационной системы			низкий

Продолжение таблицы А.7

Описание угрозы	Вид нарушителя	Тип нарушителя	Возможные цели, мотивация	Потенциал нарушителя
Установка ПО, не связанного с использованием в целях выполнения должностных обязанностей	пользователи информационной системы	внутренний	непреднамеренные неосторожные или неквалифицированные действия	низкий
Непреднамеренное отключение средств защиты	администраторы информационной системы и администраторы безопасности	внутренний	непреднамеренные неосторожные действия	средний
Утрата ключей и атрибутов доступа	пользователи информационной системы	внутренний	непреднамеренные неосторожные действия.	низкий
	администраторы информационной системы и администраторы безопасности			средний
Разглашение информации, составляющей КТ	пользователи информационной системы	внутренний	– непреднамеренные неосторожные или неквалифицированные действия; – действия с целью передачи заинтересованным лицам за вознаграждение; – месть; – действия в личных целях.	низкий
	пользователи информационной системы заказчика/контрагента	внешний	– непреднамеренные неосторожные или неквалифицированные действия. – действия с целью передачи заинтересованным лицам за вознаграждение.	
Выход из строя аппаратных и программных средств	администраторы информационной системы и администраторы безопасности	внутренний	– неквалифицированные действия; – халатность.	средний
Утрата носителей информации	пользователи информационной системы	внутренний	– неосторожные неквалифицированные действия; – халатность.	низкий
Несанкционированное копирование БД информации, составляющей КТ или её частей, а также информации с файлового сервера	пользователи информационной системы	внутренний	– действия с целью передачи заинтересованным лицам за вознаграждение; – действия вследствие подкупа заинтересованными лицами. – действия в личных целях.	низкий
	администраторы информационной системы и администраторы безопасности			средний
	пользователи информационной системы заказчика/контрагента	внешний		низкий

Продолжение таблицы А.7

Описание угрозы	Вид нарушителя	Тип нарушителя	Возможные цели, мотивация	Потенциал нарушителя
Обход некорректно настроенных механизмов аутентификации	лица, обслуживающие инфраструктуру оператора (охрана, уборщики)	внутренний	– действия вследствие подкупа заинтересованными лицами; – месть; – действия в личных целях.	низкий
	пользователи информационной системы			
Модификация данных	пользователи информационной системы	внутренний	– действия вследствие подкупа заинтересованными лицами; – месть; – действие в личных целях.	низкий

Таблица А.8 – Модель угроз безопасности иной конфиденциальной информации

Описание угрозы	Источник угрозы	Нарушаемые свойства безопасности информации	Вероятный ущерб	Актуальность угрозы
Утечка видовой информации	внутренние (персонал, не имеющий доступа к защищаемой информации)	К	– затруднение отдельных видов деятельности; – потери времени; – материальные затраты.	актуальная
	внешние (персонал контрагента, не имеющий доступ к защищаемой информации)			
Кража носителей информации	внутренние (персонал, имеющий доступ к защищаемой информации)	К	– затруднение отдельных видов деятельности; – потери времени; – материальные затраты.	актуальная
	внутренние (персонал, имеющий доступ в КЗ, но не имеющий доступ к защищаемой информации)			
	внешние (персонал контрагента)			
Уничтожение информации и её носителей	внутренние (персонал, имеющий доступ к защищаемой информации; персонал, осуществляющий администрирование ИСПДн).	Ц	– затруднение отдельных видов деятельности; – потери времени; – материальные затраты.	актуальная
	внутренние (персонал, имеющий доступ к КЗ, но не имеющий доступ к защищаемой информации)			

Продолжение таблицы А.8

Описание угрозы	Источник угрозы	Нарушаемые свойства безопасности информации	Вероятный ущерб	Актуальность угрозы
Вывод из строя узлов ПЭВМ, каналов связи	внутренние (персонал, имеющий доступ к защищаемой информации; персонал, осуществляющий администрирование ИСПДн)	Д	незначительные временные затраты сотрудников нескольких подразделений и время простоя	неактуальная
	внутренние (персонал, имеющий доступ к КЗ, но не имеющий доступ к защищаемой информации)			
Несанкционированное отключение средств защиты	внутренние (персонал, осуществляющий администрирование ИСПДн)	К, Ц	– затруднение отдельных видов деятельности; – потери времени; – материальные затраты.	актуальная
Угроза внедрения кода или данных	внутренние	Ц	– затруднение; отдельных видов деятельности – потери времени; – материальные затраты.	актуальная
	внешние	Ц, К		
Непреднамеренная модификация (уничтожение) данных	внутренние (персонал, имеющий доступ к защищаемой информации);	Ц	незначительные временные затраты отдельных подразделений	неактуальная
	внутренние (персонал, осуществляющий администрирование ИСПДн)			
Установка ПО, не связанного с использованием в целях выполнения должностных обязанностей	внутренние	Ц, Д	незначительные временные затраты отдельных подразделений	неактуальная
Непреднамеренное отключение средств защиты	внутренние (персонал, осуществляющий администрирование ИСПДн)	Ц, Д	незначительные временные затраты отдельных подразделений	неактуальная
Утрата ключей и атрибутов доступа	внутренние	Д	незначительные временные затраты отдельных подразделений и незначительное время простоя	неактуальная
Разглашение иной конфиденциальной информации	внутренние (персонал, имеющий доступ к защищаемой информации, персонал)	К	– затруднение отдельных видов деятельности; – потери времени; – материальные затраты.	актуальная

Продолжение таблицы А.8

Описание угрозы	Источник угрозы	Нарушаемые свойства безопасности информации	Вероятный ущерб	Актуальность угрозы
Разглашение иной конфиденциальной информации	внешние (персонал контрагента, имеющий доступ к защищаемой информации)	К	– затруднение отдельных видов деятельности; – потери времени; – материальные затраты.	актуальная
Выход из строя аппаратных и программных средств	внутренние (персонал, осуществляющий администрирование ИСПДн)	Д	незначительные временные затраты отдельных подразделений и незначительное время простоя	неактуальная
Утрата носителей информации	внутренние (персонал, имеющий доступ к защищаемой информации)	К	незначительные временные затраты отдельных подразделений и незначительное время простоя	неактуальная
Несанкционированное копирование БД информации, составляющей КТ или её частей, а также информации с файлового сервера	внутренние (персонал, имеющий доступ к защищаемой информации)	К	– затруднение отдельных видов деятельности; – потери времени; – материальные затраты.	актуальная
	внутренние (персонал, осуществляющий администрирование ИСПДн)			
	внешние (персонал контрагента, имеющий доступ к защищаемой информации)			
Обход некорректно настроенных механизмов аутентификации	внутренние (персонал, не имеющий доступ к защищаемой информации)	К, Ц, Д	–	неактуальная
Модификация данных	внутренние (персонал, имеющий доступ к защищаемой информации)	Ц	– затруднение отдельных видов деятельности; – потери времени.	актуальная

Таблица А.9 – Модель нарушителя для иной конфиденциальной информации АО
«ПО «Электроприбор»

Описание угрозы	Вид нарушителя	Тип нарушителя	Возможные цели, мотивация	Потенциал нарушителя
Утечка видовой информации	пользователи информационной системы	внутренний	– действия вследствие подкупа заинтересованными лицами или организаций; – действия с целью передачи заинтересованным лицам за вознаграждение; – действия в личных целях.	низкий
Кража носителей информации	пользователи информационной системы	внутренний	– действия вследствие подкупа заинтересованными лицами или организаций; – действия с целью передачи заинтересованным лицам за вознаграждение; – действия в личных целях.	низкий
	сотрудники, не являющиеся пользователями информационной системы			
	лица, обслуживающие инфраструктуру оператора (охрана, уборщики...)			
Уничтожение информации и её носителей	пользователи информационной системы	внутренний	– действия вследствие подкупа заинтересованными лицами или организаций. – месть; – действие в личных целях.	низкий
	администраторы информационной системы и администраторы безопасности			средний
	лица, обслуживающие инфраструктуру оператора (охрана, уборщики...)			низкий
Вывод из строя узлов ПЭВМ, каналов связи	пользователи информационной системы	внутренний	– непреднамеренные неосторожные или неквалифицированные действия; – месть.	низкий
	администраторы информационной системы и администраторы безопасности			средний
	внутренние (персонал, имеющий доступ к КЗ, но не имеющий доступ к защищаемой информации)			низкий
Несанкционированное отключение средств защиты	администраторы информационной системы и администраторы безопасности	внутренний	– месть; – действия вследствие подкупа; – действия в личных целях.	средний
Угроза внедрения кода или данных	администраторы информационной системы и администраторы безопасности	внутренний	– непреднамеренные неосторожные или неквалифицированные действия; – месть; – действия вследствие подкупа.	средний

Продолжение таблицы А.9

Описание угрозы	Вид нарушителя	Тип нарушителя	Возможные цели, мотивация	Потенциал нарушителя
Угроза внедрения кода или данных	пользователи информационной системы	внутренний	– непреднамеренные неосторожные или неквалифицированные действия; – месть; – действия вследствие подкупа.	низкий
	пользователи информационной контрагента/заказчика	внешний		низкий
Непреднамеренная модификация (уничтожение) данных	администраторы информационной системы и администраторы безопасности	внутренний	непреднамеренные неосторожные действия	средний
	пользователи информационной системы			низкий
Установка ПО, не связанного с использованием в целях выполнения должностных обязанностей	пользователи информационной системы	внутренний	непреднамеренные неосторожные или неквалифицированные действия	низкий
Непреднамеренное отключение средств защиты	администраторы информационной системы и администраторы безопасности	внутренний	непреднамеренные неосторожные действия	средний
Утрата ключей и атрибутов доступа	пользователи информационной системы	внутренний	непреднамеренные неосторожные действия	низкий
	администраторы информационной системы и администраторы безопасности		непреднамеренные неосторожные действия	средний
Разглашение информации, составляющей КТ	пользователи информационной системы	внутренний	– непреднамеренные неосторожные или неквалифицированные действия; – действия с целью передачи заинтересованным лицам за вознаграждение; – месть; – действия в личных целях.	низкий
	пользователи информационной системы заказчика/контрагента	внешний	– непреднамеренные неосторожные или неквалифицированные действия; – действия с целью передачи заинтересованным лицам за вознаграждение.	
Выход из строя аппаратных и программных средств	администраторы информационной системы и администраторы безопасности	внутренний	– неквалифицированные действия; – халатность.	средний

Продолжение таблицы А.9

Описание угрозы	Вид нарушителя	Тип нарушителя	Возможные цели, мотивация	Потенциал нарушителя
Утрата носителей информации	пользователи информационной системы	внутренний	– неосторожные неквалифицированные действия; – халатность.	низкий
Несанкционированное копирование БД информации, составляющей КТ или её частей, а также информации с файлового сервера	пользователи информационной системы	внутренний	– действия с целью передачи заинтересованным лицам за вознаграждение; – действия вследствие подкупа заинтересованными лицами; – действия в личных целях.	низкий
	администраторы информационной системы и администраторы безопасности			средний
	пользователи информационной системы заказчика/контрагента	внешний		низкий
Обход некорректно настроенных механизмов аутентификации	лица, обслуживающие инфраструктуру оператора (охрана, уборщики)	внутренний	– действия вследствие подкупа заинтересованными лицами; – месть; – действия в личных целях.	низкий
	пользователи информационной системы			
Модификация данных	пользователи информационной системы	внутренний	– действия вследствие подкупа заинтересованными лицами; – месть; – действия в личных целях.	низкий

А.5 Субъекты и роли, на которые распространяется действие данной политики

Действие данной политики распространяется на всех работников «АО «ПО «Электроприбор», в том числе лиц звена управления.

Особое значение данная политика имеет для сотрудников подразделения информационных технологий, информационной безопасности, в частности, на администраторов информационных систем и администраторов безопасности информационных систем.

А.6 Требования по обеспечению безопасности конфиденциальной информации

Требования по обеспечению безопасности конфиденциальной информации для всех работников АО «ПО «Электроприбор» устанавливаются:

- ФЗ №152 от 27.07.2006 «О персональных данных» [7];

- ФЗ № 98 от 29.07.2004 «О коммерческой тайне» [8];
- инструкция по соблюдению режима конфиденциальности;
- положение «О коммерческой тайне»;
- положение «Об организации работы с персональными данными»;
- инструкция администратора безопасности.

А.7 Контроль реализации политики

Ответственными за реализацию настоящей политики назначаются руководители подразделения информационных технологий и подразделения информационной безопасности.

Для проверки реализации требований настоящей политики применяется внутренний аудит.

А.8 Ответственность за реализацию политики

Реализацию данной политики осуществляют администраторы безопасности информационных систем АО «ПО «Электроприбор» на основе инструкции администратора безопасности, приведённой в приложении В.

А.9 Условия пересмотра политики

Пересмотр настоящей политики ИБ осуществляется с составом следующих лиц:

- генеральный директор;
- директора по направлениям;
- руководитель подразделения ИБ;
- руководитель подразделения ИТ.

Случаи пересмотра:

- в случае выявления новых актуальных угроз безопасности или признании актуальных угроз неактуальными;
- при существенных изменениях в деятельности организации;
- при изменениях законодательства РФ в части информационной безопасности.

ПРИЛОЖЕНИЕ Б

(обязательное)

Базовый набор защитных мер

Таблица Б.1 – Базовый набор защитных мер для третьего уровня защищённости персональных данных

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

Продолжение таблицы Б.1

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)
УПД.17	Обеспечение доверенной загрузки средств вычислительной техники
III. Ограничение программной среды (ОПС)	
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов
ОПС.4	Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов
IV. Защита машинных носителей информации (ЗНИ)	
ЗНИ.1	Учет машинных носителей персональных данных
ЗНИ.2	Управление доступом к машинным носителям персональных данных
ЗНИ.3	Контроль перемещения машинных носителей персональных данных за пределы контролируемой зоны
ЗНИ.4	Исключение возможности несанкционированного ознакомления с содержанием персональных данных, хранящихся на машинных носителях, и (или) использования носителей персональных данных в иных информационных системах
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители персональных данных
ЗНИ.6	Контроль ввода (вывода) информации на машинные носители персональных данных
ЗНИ.7	Контроль подключения машинных носителей персональных данных
ЗНИ.8	Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания
V. Регистрация событий безопасности (РСБ)	
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения
РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе
РСБ.7	Защита информации о событиях безопасности
VI. Антивирусная защита (АВЗ)	
АВЗ.1	Реализация антивирусной защиты
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
VII. Обнаружение вторжений (СОВ)	
СОВ.1	Обнаружение вторжений
СОВ.2	Обновление базы решающих правил
VIII. Контроль (анализ) защищенности персональных данных	
АНЗ.1	выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей

Продолжение таблицы Б.1

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе
IX. Обеспечение целостности информационной системы персональных данных (ОЦЛ)	
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации
ОЦЛ.2	Контроль целостности персональных данных, содержащихся в базах данных информационной системы
ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций
ОЦЛ.4	Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама)
ОЦЛ.5	Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и (или) контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), методов, и исключение неправомерной передачи информации из информационной системы
ОЦЛ.6	Ограничение прав пользователей по вводу информации в информационную систему
ОЦЛ.7	Контроль точности, полноты и правильности данных, вводимых в информационную систему
ОЦЛ.8	Контроль ошибочных действий пользователей по вводу и (или) передаче персональных данных и предупреждение пользователей об ошибочных действиях
X. Обеспечение доступности персональных данных (ОДТ)	
ОДТ.1	Использование отказоустойчивых технических средств
ОДТ.2	Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования ИС
ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование
ОДТ.4	Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных
ОДТ.5	Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала
XI. Защита среды виртуализации (ЗСВ)	
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре
ЗСВ.4	Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры
ЗСВ.5	Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией

Продолжение таблицы Б.1

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных
ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных
ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций
ЗСВ. 8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей
XII. Защита технических средств (ЗТС)	
ЗТС.1	Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр
ЗТС.5	Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов)
XIII. Защита информационной системы, её средств, систем связи и передачи данных (ЗИС)	
ЗИС.1	Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты персональных данных, функций по обработке персональных данных и иных функций информационной системы
ЗИС.2	Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом
ЗИС.3	Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи
ЗИС.4	Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации
ЗИС. 5	Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств
ЗИС.6	Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с персональными данными, при обмене ими с иными информационными системами
ЗИС. 7	Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода
ЗИС. 8	Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи

Продолжение таблицы 14

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных
ЗИС.9	Контроль санкционированной и исключение несанкционированной передачи видеoinформации, в том числе регистрация событий, связанных с передачей видеoinформации, их анализ и реагирование на нарушения, связанные с передачей видеoinформации
ЗИС.10	Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам
ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов
ЗИС.12	Исключение возможности отрицания пользователем факта отправки персональных данных другому пользователю
ЗИС.13	Исключение возможности отрицания пользователем факта получения персональных данных от другого пользователя
ЗИС.14	Использование устройств терминального доступа для обработки персональных данных
ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных
ЗИС.16	выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер или внутри разрешенных сетевых протоколов
ЗИС.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы
ЗИС.18	Обеспечение загрузки и исполнения программного обеспечения с машинных носителей персональных данных, доступных только для чтения, и контроль целостности данного программного обеспечения
ЗИС.19	Изоляция процессов (выполнение программ) в выделенной области памяти
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе
XIV. выявление инцидентов и реагирование на них (ИНЦ)	
ИНЦ.1	Определение лиц, ответственных за выявление инцидентов и реагирование на них
ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов
ИНЦ.3	Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами
ИНЦ.4	Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий
ИНЦ. 5	Принятие мер по устранению последствий инцидентов
ИНЦ. 6	Планирование и принятие мер по предотвращению повторного возникновения инцидентов
XV. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)	
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных
УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты персональных данных
УКФ.3	Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных
УКФ.4	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных

ПРИЛОЖЕНИЕ В

(обязательное)

Инструкция администратора безопасности

В.1 Общие положения

Администратор безопасности ИСПДн (ИС КТ, ИС КИ) «Персонал» (ИС КТ, ИС КИ) в своей работе руководствуется настоящей инструкцией, требованиями законов и иных нормативных актов Российской Федерации по вопросам защиты персональных данных, руководящими и нормативными документами ФСТЭК России.

Администратор отвечает за поддержание необходимого уровня безопасности персональных данных в ИСПДн (ИС КТ, ИС КИ) «Персонал» (ИС КТ, ИС КИ).

Администратор безопасности является работником АО «ПО «Электроприбор», уполномоченным на проведение работ по технической защите информации и поддержанию достигнутого уровня защиты ИСПДн (ИС КТ, ИС КИ) «Персонал» (ИС КТ, ИС КИ) и ее ресурсов в процессе эксплуатации.

Администратор безопасности осуществляет методическое руководство Операторов ИСПДн «Персонал» (ИС КТ, ИС КИ), в вопросах обеспечения безопасности персональных данных.

Требования администратора информационной безопасности, связанные с выполнением им своих должностных обязанностей, обязательны для исполнения всеми пользователями ИСПДн (ИС КТ, ИС КИ).

Администратор безопасности несет персональную ответственность за качество проводимых им работ по контролю действий пользователей при работе в ИСПДн, состояние и поддержание установленного уровня защиты ИСПДн.

Д.2 Идентификации и аутентификации субъектов доступа и объектов доступа

Каждому пользователю должен быть присвоен пароль, отвечающий требованиям сложности

Пароли создаёт и присваивает Администратор безопасности ИСПДн.

Администратор безопасности ИСПДн (ИС КТ, ИС КИ) осуществляет разработку и ведение журнала учёта выданных персональных идентификаторов в формате: дата выдачи – ФИО сотрудника получившего идентификатор – учётный номер идентификатора – должность сотрудника.

Администратор настраивает максимальное число попыток ввода пароля в случае не корректной идентификации или в случае попыток входа в систему пользователей, подлинность идентификации которых при аутентификации не подтвердилась, осуществляется блокировка компьютера.

Администратор безопасности осуществляет разблокировку компьютеров.

Д.3 Управление доступом субъектов доступа к объектам доступа

Заведение, активация, блокирование и уничтожение учётных записей пользователей осуществляется администратором ИСПДн (ИС КТ, ИС КИ).

Управление доступом субъектов доступа к объектам доступа осуществляет Администратор безопасности ИСПДн (ИС КТ, ИС КИ).

Настраиваемый метод разграничения доступа субъектов доступа к объектам доступа – дискреционный.

Настройка системы разграничения доступа, реализуемой СЗИ от НСД «Dallas Lock 8.0–К» осуществляется администратором ИСПДн (ИС КТ, ИС КИ).

Администратор производит конфигурирование маршрутизатора таким образом, что передача/приём трафика АРМ сотрудников возможен только с АРМ администратора.

Обмен трафиком между АРМ сотрудников запрещён.

Администратор безопасности ИСПДн (ИС КТ, ИС КИ) осуществляет администрирование АРМ сотрудников со своего рабочего места, используя службу Active Directory, входящую в состав ОС Windows Server и интегрированную в неё систему управления СЗИ от НСД «Dallas Lock».

Администратор осуществляет плановое и внеплановое изменение конфигурации программных и технических средств компьютеров и серверов, входящих в состав ИСПДн (ИС КТ, ИС КИ), производит настройку

телекоммуникационного оборудования для корректного функционирования ИСПДн (ИС КТ, ИС КИ).

Число неуспешных попыток входа в систему = 5, после чего учётная запись блокируется. Разблокировка учётной записи осуществляется администратором ИСПДн (ИС КТ, ИС КИ).

Сеанс доступа в информационную систему блокируется после 20 минут бездействия пользователя. Разблокировка учётной записи осуществляется администратором ИСПДн (ИС КТ, ИС КИ).

Д.4 Ограничение программной среды

Администратор безопасности ИСПДн (ИС КТ, ИС КИ) проводит настройку ограничений программной среды.

Ограничение программной среды осуществляется посредством настройки соответствующего механизма СЗИ от НСД «Dallas Lock 8.0–К» установленной на компьютерах, входящих в состав ИСПДн «Персонал» (ИС КТ, ИС КИ).

Настройка ограничений программной среды проводится таким образом, чтобы каждый пользователь обладал правами на запуск минимального набора программ, необходимого ему для осуществления своих должностных обязанностей.

Запуск программ, права на доступ к которым пользователь не имеет, блокируются системой защиты, события о несанкционированной попытке запуска регистрируются в журнале «Dallas Lock 8.0–К» администратора СЗИ.

В.5 Защита машинных носителей

Администратор безопасности ИСПДн (ИС КТ, ИС КИ) обеспечивает учёт машинных носителей, используемых в ИСПДн (ИС КТ, КИ)

Каждому носителю присваивается регистрационный номер, который заносится в журнал учёта.

Администратор осуществляет разработку журнала учёта машинных носителей в формате.

Хранение машинных носителей осуществляется в специальных металлических шкафах, оборудованных замками.

На каждый носитель, помимо регистрационного номера наносится метка о невозможности использования носителей за пределами ИСПДн (ИС КИ, ИС КТ).

На каждый носитель, наносится маркер о возможности использования носителя для хранения и обработки информации соответствующей степени конфиденциальности.

В.6 Регистрации событий безопасности

Регистрация событий должна осуществляться в журнале «Безопасности» ОС и журнале «Dallas Lock 8.0–К».

Размер журналов регистрации принимать 2Гб и производить очистку журналов по мере необходимости.

Администратор безопасности ИСПДн (ИС КТ, ИС КИ) осуществляет копирование журналов безопасности и Secret Net не реже 1 раза в 30 дней и осуществляет их последующее архивирование.

Хранение архивированных копий журналов осуществляется администратором в течении 1 года, после чего они подлежат удалению.

Администратор безопасности ИСПДн (ИС КТ, ИС КИ) осуществляет просмотр журналов регистрации событий не реже 1 раза в 7 дней.

Защита информации о событиях безопасности осуществляется с помощью СЗИ от НСД «Dallas Lock 8.0–К».

В.7 Антивирусная защита

Администратор обязаны осуществлять централизованное автоматическое обновление баз данных признаков вредоносных программ для антивирусных программ по мере выхода актуальных доступных обновлений.

Настройка антивирусных программ осуществляется таким образом, что при установке нового ПО или подключении съёмного машинного носителя осуществляется его экспресс – проверка на наличие вредоносного ПО.

Администратор обязан разработать и вести журнал обновления

антивирусных программ в формате: учётный номер СВТ – дата обновления.

Экспресс – проверку СВТ, входящих в состав ИСПДн (ИС КТ, ИС КИ), на наличие вредоносного ПО осуществлять 1 раз в 7 дней.

Полную проверку СВТ (с использованием одной антивирусной программы), входящих в состав ИСПДн (ИС КТ, ИС КИ), на наличие вредоносного ПО осуществлять 1 раз в 30 дней.

Экспресс – проверку АРМ администратора ИСПДн (ИС КТ, ИС КИ) и серверов БД осуществлять 1 раз в 3 дня.

Полную проверку АРМ администратора ИСПДн (ИС КТ, ИС КИ), серверов БД осуществлять 1 раз в 15 дней.

Администратор безопасности ИСПДн (ИС КТ, ИС КИ) обязан разработать и вести журнал учёта полных и усиленных полных проверок СВТ, АРМ и серверов на наличие вредоносных программ в формате: учётный номер СВТ – вид проверки – дата проверки – результат проверки – предпринятые действия (в случае необходимости).

Администратор безопасности ИСПДн (ИС КТ, ИС КИ) обязан осуществлять полную проверку съёмных учётных носителей не реже 1 раза в 30 дней.

С целью предотвращения проникновения в ИСПДн (ИС КТ, ИС КИ) вредоносного ПО, запрещается использование неучётных носителей.

В.8 Контролю защищенности персональных данных

Администратор безопасности ИСПДн (ИС КТ, ИС КИ) осуществляет настройку и обеспечивает корректную работу средств защиты информации, технических средств и программного обеспечения.

Тестирование системы защиты на предмет выявления некорректной работы осуществляется администратором ИСПДн (ИС КТ, ИС КИ) не реже 1 раза в 30 дней.

Администратор безопасности ИСПДн (ИС КТ, ИС КИ) разрабатывает и ведёт журнал тестирования СЗИ в формате: дата – время начала тестирования – результат тестирования – предпринятые действия (в случае необходимости) –

время окончания тестирования.

Контроль установки обновлений общесистемного, прикладного и специального ПО осуществляется администратором ИСПДн (ИС КТ, ИС КИ) не реже 1 раза в 7 дней.

Администратором ИСПДн (ИС КТ, ИС КИ) осуществляется разработка и ведение журнала регистрации установки обновлений в формате: дата – наименование обновляемого ПО – суть обновления.

Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты осуществляется администратором ИСПДн (ИС КТ, ИС КИ) не реже 1 раза в 30 дней.

Администратором ИСПДн (ИС КТ, ИС КИ) разрабатывается и ведётся журнал контроля работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты в формате: дата проверки – результаты контроля – действия, предпринятые для устранения неполадок (в случае необходимости)

Контроль состава технических средств, программного обеспечения и средств защиты информации проводится администратором ИСПДн (ИС КТ, ИС КИ) не реже 1 раза в 30 дней.

В.9 Обеспечение целостности

Администратор осуществляет разработку перечня информационных ресурсов СВТ, в отношении которых необходимо вести контроль целостности.

Администратор осуществляет анализ журналов регистрации событий «Dallas Lock 8.0–К» с целью выявления событий нарушения контроля целостности.

Настройка механизма контроля целостности осуществляется администратором таким образом, что:

- проверка файлов на СВТ, входящих в состав ИСПДн, осуществляется не реже 1 раза в 7 дней;
- проверка файлов на АРМ администратора не реже 1 раза в 3 дня;

- проверка ПДн, обрабатываемых на серверах БД ИСПДн (ИС КТ, ИС КИ) не реже 1 раза в 2 дня;
- проверка программных компонентов средств защиты информации не реже 1 раза в 1 день;
- проверка программных компонентов ОС на всех СВТ и серверах, входящих в состав ИСПДн (ИС КТ, ИС КИ) не реже 1 раза в 1 день;
- пересчёт эталонов осуществлять не реже 1 раза в 7 дней.

Администратор безопасности ИСПДн (ИС КТ, ИС КИ) анализирует журнал регистрации событий «Dallas Lock 8.0–К» на выявление нарушений целостности информации не реже 1 раза в 5 дней.

Администратор безопасности ИСПДн (ИС КТ, ИС КИ) создаёт и ведёт журнал контроля целостности. в случае выявления нарушения целостности администратор делает запись следующего формата: дата – время – наименование ресурса, целостность которого было нарушена – имя учётной записи пользователя, осуществившего нарушение.

Настройка механизма контроля целостности осуществляется администратором ИСПДн (ИС КТ, ИС КИ) таким образом, чтобы при нарушении целостности файл восстанавливался из эталона.

Администратор безопасности ИСПДн (ИС КТ, ИС КИ) производит настройку ОС СВТ таким образом, что при нарушении целостности контролируемых ресурсов происходит блокировка СВТ.

Администратор осуществляет централизованное резервирование файлов, хранящихся на СВТ, входящих в состав ИСПДн (ИС КТ, ИС КИ) не реже 1 раза в 60 дней.

Администратор осуществляет резервное копирование БД, хранящихся на серверах БД и сохранение конфигураций основных программ и программ, входящих в состав средств защиты информации не реже 1 раза в 30 дней.

Пользователи имеют право вводить информацию, относящуюся к выполнению ими должностных обязанностей – ПДн клиентов и сотрудников.

В.10 Обеспечению доступности

Контроль корректного функционирования технических средств осуществляется администраторами ИСПДн (ИС КТ, ИС КИ) не реже 1 раза в 7.

в случае сбоя или выявленного факта некорректного функционирования технического средства Администратор безопасности ИСПДн (ИС КТ, ИС КИ) устраняет причину сбоя. При невозможности устранить поломку самостоятельно, Администратор безопасности ИСПДн (ИС КТ, ИС КИ) вызывает сотрудников организации, специализирующейся на ремонте данного вида технических средств.

Администратор осуществляет централизованное резервное копирование файлов, хранящихся на СВТ входящих в состав ИСПДн (ИС КТ, ИС КИ) на съёмные машинные носители информации не реже 1 раза в 60 дней.

Администратор осуществляет резервное копирование БД, хранящихся на серверах БД, на съёмные машинные носители информации не реже 1 раза в 30 дней.

Восстановление ПДн с резервных машинных носителей информации осуществляется в течение 30 минут, после потери доступности основных данных.

В.11 Выявление инцидентов и реагированию на них

Ответственным за выявления инцидентов и реагирование на них в Администратор безопасности ИСПДн.

Обнаружение и идентификация инцидентов осуществляется на основе анализа записей журналов безопасности ОС Microsoft Windows Server и СЗИ от НСД «Dallas Lock 8.0–К», а также оповещений СЗИ от НСД «Dallas Lock 8.0–К».

Инцидент может быть обнаружен сотрудником организации. в этом случае сотрудник заполняет форму, содержащую:

- свои ФИО и должности;
- дата и время обнаружения инцидента;
- описание событий.

После устранения инцидента Администратор безопасности ИСПДн (ИС КТ, ИС КИ) совместно с работниками подразделения ИБ и ИТ производят его анализ, определяя источник инцидента, причинённый ущерб и пути совершенствования системы безопасности для предотвращения данного инцидента в будущем.

Администратор безопасности ИСПДн (ИС КТ, ИС КИ) разрабатывает и ведёт журнал инцидентов следующей формы: дата время обнаружения инцидента – информация о лице, сообщившем об инциденте – описание событий – время устранения инцидента – нанесённый ущерб.

В.12 Управление конфигурацией ИСПДн (ИС КТ, ИС КИ) и ее системы защиты

Изменения в конфигурацию ИСПДн (ИС КТ, ИС КИ) и систему защиты разрешается вносить администраторам ИСПДн (ИС КТ, ИС КИ) с письменного разрешения генерального директора АО «ПО «Электроприбор» после предоставления в письменном виде оснований для такого изменения.

Администратор безопасности ИСПДн (ИС КТ, ИС КИ) разрабатывает и ведёт журнал учёта внесения конфигураций в формате: дата начала работ по внесению изменений в конфигурацию – причина проведения работ – перечень проведённых работ – дата окончания работ.

Конфигурирование СЗИ ИСПДн (ИС КТ, ИС КИ) осуществляют администраторы ИСПДн (ИС КТ, ИС КИ), при это делается запись в соответствующем журнале.

Администратор безопасности ИСПДн (ИС КТ, ИС КИ) осуществляет разработку и ведение журнала учёта внесения изменений в конфигурацию СЗИ ИСПДн (ИС КТ, ИС КИ) в формате: дата – время – причина внесения изменений – перечень изменений – дата окончания работ – время окончания работ.

Изменения допускаются в том случае, если при анализе потенциального воздействия планируемых изменений и СЗИ администраторами ИСПДн (ИС КТ, ИС КИ) и экспертами не было выявлено новых потенциальных угроз безопасности персональных данных.

ПРИЛОЖЕНИЕ Г

(обязательное)

Инструкция по соблюдению режима конфиденциальности

Г.1 Общие положения

Г.1.1 Настоящая инструкция разработана в дополнение к «Положению о коммерческой тайне Акционерного общества «Пензенское производственное объединение «Электроприбор».

Г.1.2 Инструкция направлена на обеспечение режима конфиденциальности информации, составляющей коммерческую тайну АО «ПО «Электроприбор» и информации, распространение которой ограничено нормативными актами АО «ПО «Электроприбор» и вышестоящих организаций, путём установления обязанностей и запретов необходимых для исполнения работниками и руководителями структурных подразделений АО «ПО «Электроприбор».

Г.2 Обязанности и запреты

Г.2.1 Руководитель структурного подразделения обязан:

- разрабатывать и осуществлять мероприятия по обеспечению режима коммерческой тайны в подразделении;
- участвовать в проведении служебного расследования в случае утраты либо хищения носителей сведений, составляющих коммерческую тайну Общества, других нарушений режима коммерческой тайны, а также фактах разглашения сведений, составляющих коммерческую тайну Общества;
- принимать меры по предотвращению разглашения и утечки сведений, составляющих коммерческую тайну, при проведении конфиденциальных работ;
- давать заместителю генерального директора по режиму и начальнику отдела № 135 объяснения по фактам нарушения режима коммерческой тайны в подразделении;
- организовывать защиту сведений, составляющих коммерческую тайну, при взаимодействии с контрагентами, в т.ч. подписать Соглашение о конфиденциальности;

- проводить проверки состояния работы по обеспечению режима коммерческой тайны в подразделении и на рабочих местах.

Г.2.2 Работники, допущенные к сведениям, составляющим коммерческую тайну Общества, несут ответственность за сохранность этих сведений и соблюдения установленного режима коммерческой тайны.

Г.2.3 Работники, получившие доступ к информации, составляющей коммерческую тайну Общества, обязаны:

- знать и выполнять в части его касающейся требования настоящего Положения, а также правовых актов Общества, регламентирующих вопросы защиты коммерческой тайны;

- хранить сведения, составляющие коммерческую тайну, ставшие им известными по работе, пресекать противоправные действия других работников, которые могут привести к разглашению этих сведений, немедленно информировать непосредственного руководителя и начальника отдела № 135 о таких фактах, а также о других причинах и условиях возможной утечки сведений, составляющих коммерческую тайну;

- при разработке конфиденциальных документов ограничиваться минимально необходимым объемом информации, составляющей коммерческую тайну, включаемой в документы, присваивать таким документам гриф конфиденциальности, определять необходимое количество экземпляров и оформлять указатель рассылки;

- хранить конфиденциальные документы в сейфах, запираемых шкафах (ящиках);

- незамедлительно сообщать в отдел № 135 об утрате или недостатке носителей информации и документов, содержащих коммерческую тайну, а также ключей от сейфов, в которых хранятся носители сведений, составляющих коммерческую тайну Общества;

- обеспечивать такое расположение носителей сведений, содержащих коммерческую тайну, при котором исключается возможность ознакомления с

ними других работников, в том числе и допущенных к сведениям, составляющим коммерческую тайну, но не имеющим к ним прямого отношения;

- по требованию лица, ответственного за конфиденциальное делопроизводство, а также сотрудников отдела № 135 предъявлять для проверки все полученные им под роспись конфиденциальные документы;

- представлять по требованию руководителя структурного подразделения, а также сотрудников отдела № 135 устные или письменные объяснения о нарушениях установленного режима коммерческой тайны, а также о фактах разглашения информации, составляющей коммерческую тайну, или утраты документов, содержащих эту информацию.

- в случае попытки третьих лиц, не имеющих доступ к информации, составляющей коммерческую тайну, получить от работника коммерческую тайну Общества незамедлительно сообщить об этом своему непосредственному начальнику и начальнику отдела № 135.

Г.2.4 Работникам, допущенным к информации, составляющей коммерческую тайну, запрещается:

- использовать информацию, составляющую коммерческую тайну Общества, при занятии другой деятельностью, в том числе при работе в иных организациях, а также в научной и педагогической деятельности, и в личных целях;

- в нарушение установленного порядка изготавливать дополнительные экземпляры (снимать копии) с документов и других носителей, содержащих информацию, составляющую коммерческую тайну Общества;

- накапливать ненужные для работы носители сведений, составляющие коммерческую тайну;

- сбор, хранение сведений составляющих коммерческую тайну не связанных с выполнением своих должностных обязанностей;

- выносить документы и другие носители информации (запоминающие устройства, USB-накопители и пр.), содержащие информацию, составляющую

коммерческую тайну, за пределы территории Общества без разрешения руководителя структурного подразделения;

- знакомить других работников Общества с документами, содержащими информацию, составляющую коммерческую тайну, без письменного разрешения руководителя структурного подразделения, в ведении которого находятся данные документы;

- использовать информацию, составляющую коммерческую тайну Общества, в публичных выступлениях или ссылаться на нее в средствах массовой информации, без согласования с отделом № 135;

- передавать информацию, составляющую коммерческую тайну Общества, по незащищенным каналам связи (с использованием факсимильной связи, сети Интернет). в исключительных случаях разрешается отправка по электронной почте, только после согласования с отделом №135 и применения мер по защите информации;

- обрабатывать конфиденциальную информацию с использованием личных портативных ПЭВМ (ноутбук), смартфонов, КПК и других личных средств вычислительной техники.

- обрабатывать конфиденциальную информацию на технических средствах (ПЭВМ, планшеты, телефоны), имеющих доступ к сети Интернет.

Г.2.5 При увольнении работник обязан сдать лицу, ответственному за ведение конфиденциального делопроизводства в структурном подразделении, все имеющиеся в его распоряжении материальные носители информации, содержащие сведения, составляющие коммерческую тайну Общества. в случае увольнения не разглашать и не использовать для личных целей или целей других лиц коммерческую тайну Общества в течение 3 лет с момента увольнения.

Г.3 Ответственность

За неисполнение или ненадлежащее исполнение положений настоящей инструкции работники (в том числе руководители структурных подразделений) несут ответственность, предусмотренную законодательством РФ в соответствии с п.12 «Положения о коммерческой тайне АО «ПО «Электроприбор».

ПРИЛОЖЕНИЕ Д

(обязательное)

Положение «О коммерческой тайне»

Д.1 Общие положения

Д.1.1 Настоящее Положение разработано в соответствии с Гражданским кодексом Российской Федерации, Федеральным законом "О коммерческой тайне" от 29 июля 2004 года N 98-ФЗ [8], Федеральным законом "Об информации, информационных технологиях и о защите информации" от 27 июля 2006 года N 149-ФЗ [9], другими нормативными правовыми актами Российской Федерации.

Положение устанавливает режим коммерческой тайны в Акционерном обществе «Пензенское производственное объединение «Электроприбор» (далее – Общество), определяет правовые, организационные и экономические механизмы по защите коммерческой тайны с целью предотвращения нанесения возможного экономического и имиджевого ущерба организации со стороны юридических и физических лиц, вызванного их неправомерными или неосторожными действиями путем несанкционированного присвоения или разглашения коммерческой тайны.

Требования настоящего Положения обязательны для исполнения всеми работниками Общества, получившими доступ к информации, составляющей коммерческую тайну Общества.

Д.1.2 Меры по охране информации, составляющей коммерческую тайну, включают:

- введение перечня информации, составляющей коммерческую тайну;
- ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и осуществление контроля за соблюдением такого порядка;
- учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;

- регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами – на основании гражданско–правовых договоров;

- нанесение на материальные носители (документы), содержащие информацию, составляющей коммерческую тайну, и (или) сопроводительную документацию к ним грифа «Коммерческая тайна» с указанием обладателя этой информации;

- выполнение требований по технической защите конфиденциальной информации на объектах информатизации в соответствии со Специальными требованиями и рекомендациями по технической защите конфиденциальной информации, утвержденными приказом Гостехкомиссии России от 30.08.2002 г. N 282 [10].

Режим коммерческой тайны считается установленным после реализации Обществом указанных мер.

Д.1.3 Координирует работы по реализации мер по защите информации, составляющей коммерческую тайну Общества, отдел № 135. Численность сотрудников отдела № 135, ведущих направление по защите коммерческой тайны Общества, определяется исходя из объема защищаемой информации и сложности проводимых мероприятий по их защите.

Д.2 Основные термины и определения

Для целей настоящего Положения используемые понятия означают следующее:

- "информация" – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;

- "документированная информация" – зафиксированная на материальном носителе путем документирования информации с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;

- "информационные процессы" – процессы сбора, обработки, накопления, хранения, поиска, предоставления и распространения информации;

– "информационные ресурсы" – отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах);

– "носители конфиденциальной информации" – материальные объекты, в которых конфиденциальная информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов;

– "гриф конфиденциальности" – реквизиты, свидетельствующие о конфиденциальности информации, содержащейся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него;

– "информация, составляющая коммерческую тайну (секрет производства)" – сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно–технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны;

– "обладатель информации, составляющей коммерческую тайну" – лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим коммерческой тайны;

– "коммерческая тайна" – режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду;

– "режим коммерческой тайны" – правовые, организационные, технические и иные меры, принимаемые обладателем информации,

составляющей коммерческую тайну, по ее охране;

- "перечень сведений, составляющих коммерческую тайну Акционерного общества «Пензенское производственное объединение «Электроприбор» – правовой акт Общества, утверждаемый генеральным директором и определяющий виды информации, относящейся к коммерческой тайне;

- "доступ к информации, составляющей коммерческую тайну" – ознакомление определенных лиц с информацией, составляющей коммерческую тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации;

- "передача информации, составляющей коммерческую тайну" – передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем контрагенту на основании договора в объеме и на условиях, которые предусмотрены договором, включая условие о принятии контрагентом установленных договором мер по охране ее конфиденциальности;

- "предоставление информации, составляющей коммерческую тайну" – передача информации, составляющей коммерческую тайну, зафиксированной на материальном носителе, ее обладателем органам государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функций;

- "разглашение информации, составляющей коммерческую тайну" – действие или бездействие, в результате которого информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной или иной, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору;

- "исполнитель документа" – работник, осуществляющий подготовку проекта документа.

Д.3 Порядок формирования перечня сведений, составляющих коммерческую тайну

Д.3.1 Право на отнесение научно–технической, технологической, финансово–экономической и иной информации, которой Общество владеет на законном основании, к информации, составляющей коммерческую тайну, формирование перечня и состава такой информации принадлежит Обществу.

Д.3.2 Общество является обладателем информации, составляющей коммерческую тайну, созданной работниками Общества в рамках трудовых отношений, а также контрагентами в рамках гражданско–правовых договоров. Положения настоящего абзаца применяются, если иное не предусмотрено законами, иными правовыми актами или договорами.

Д.3.3 Информация, составляющая коммерческую тайну, самостоятельно полученная Обществом 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.

Д.3.4 Информация, составляющая коммерческую тайну Общества, полученная от ее обладателя на основании договора или на другом законном основании, считается полученной законным способом.

Д.3.5 Перечень формируется отделом № 135 на основании предложений руководителей структурных подразделений Общества и утверждается генеральным директором Общества.

Д.3.6 Основным условием, позволяющим относить информацию (группу сведений) к информации, составляющей коммерческую тайну, является действительная или потенциальная коммерческая ценность в силу неизвестности ее третьим лицам.

Д.3.7 Разработка перечня должна осуществляться с учетом ограничений, установленных Федеральным законом от 29.07.2004 N 98–ФЗ "О

коммерческой тайне" [8] и иными Федеральными законами.

Д.3.8 Плановый пересмотр Перечня должен проводиться не реже одного раза в три года. Инициировать корректировку могут руководители подразделений или заместителя генерального директора по направлениям деятельности, написав письменное обоснование в отдел № 135.

Д.3.9 Руководители структурных подразделений и заместители генерального директора по направлениям деятельности несут персональную ответственность за обоснованность включения (не включения) информации, составляющей коммерческую тайну в Перечень.

Д.3.10 Для проведения оценки ценности документа, содержащего сведения, составляющие коммерческую тайну создается экспертная комиссия. в состав экспертной комиссии включается не менее трех квалифицированных работников Организации, которые могут корректно определить содержание документов, содержащих сведения, составляющие коммерческую тайну во всех сферах деятельности Организации.

Д.4 Порядок доступа к информации, составляющей коммерческую тайну

Д.4.1 Все сотрудники Общества должны быть ознакомлены с Перечнем, также со всеми работниками Общества в дополнение к трудовому договору заключается обязательство о неразглашении коммерческой тайны АО «ПО «Электроприбор».

Д.4.2 Отдел № 135 на основании предложений руководителей структурных подразделений Общества разрабатывает номенклатуру должностей работников АО «ПО «Электроприбор», допущенных к информации, составляющей коммерческую тайну (далее – номенклатура должностей). Номенклатура должностей утверждается генеральным директором Общества.

Д.4.3 Доступ работника структурного подразделения к информации, составляющей коммерческую тайну Общества, должность которого включена в номенклатуру должностей, допущенных к информации, составляющей коммерческую тайну Общества, осуществляется с письменного разрешения

руководителя структурного подразделения, в штате которого находится данный работник, после согласования с отделом № 135. Работник допускается к информации, составляющей коммерческую тайну Общества, в объеме, необходимом для выполнения своих должностных обязанностей.

Д.4.4 Сотруднику Общества может быть отказано в допуске к информации, составляющей коммерческую тайну в случае:

- признания его судом недееспособным или ограниченно дееспособным;
- выявления в результате проверок определенных обстоятельств и действий сотрудника, создающих угрозу экономической безопасности Общества;
- сообщения работником заведомо ложных анкетных данных и др.

Д.4.5 Допуск к коммерческой тайне Общества осуществляется только после подписания работником обязательства о неразглашении коммерческой тайны.

Д.4.6 При допуске работника к коммерческой тайне, на него возлагаются обязанности по неразглашению информации, составляющей коммерческую тайну Общества. При этом работник знакомится под роспись:

- с Перечнем сведений, составляющих коммерческую тайну АО «ПО «Электроприбор»;
- с другими правовыми актами Общества, определяющими режим коммерческой тайны и ответственность за его нарушение.

Д.4.7 Доступ к находящейся в ведении одного структурного подразделения информации, составляющей коммерческую тайну, работникам другого структурного подразделения осуществляется по письменному запросу руководителя структурного подразделения, заинтересованного в получении такой информации, и с разрешения руководителя структурного подразделения, в чьем ведении находится запрашиваемая информация.

Д.4.8 Прекращение доступа работника структурного подразделения к информации, составляющей коммерческую тайну Общества, осуществляется по решению генерального директора АО «ПО «Электроприбор» в случаях:

- нарушения работником установленного режима коммерческой тайны;
- освобождения работника от занимаемой должности.

Прекращение доступа к информации, составляющей коммерческую тайну Общества, не освобождает работника от взятых им обязательств по неразглашению указанных сведений.

Д.4.9 Соблюдение режима конфиденциальности информации, составляющей коммерческой тайны работниками АО «ПО «Электроприбор» регламентируется «Инструкцией по соблюдению режима конфиденциальности в АО «ПО «Электроприбор»

Д.5 Порядок обращения с документами, содержащими коммерческую тайну

Д.5.1 Организация конфиденциального делопроизводства возложена на подразделение № 121 «Канцелярия».

Д.5.2 Документированная информация, составляющая коммерческую тайну Общества, должна иметь соответствующие отличительные реквизиты. Такими реквизитами являются гриф конфиденциальности, отметка о количестве экземпляров, номер экземпляра, регистрационный номер, фамилия и инициалы исполнителя, номер телефона, дата разработки документа.

Д.5.3 На документах или других материальных носителях информации, содержащих информацию, составляющую коммерческую тайну Общества, должен быть проставлен гриф конфиденциальности, приведённый на рисунке Д.1

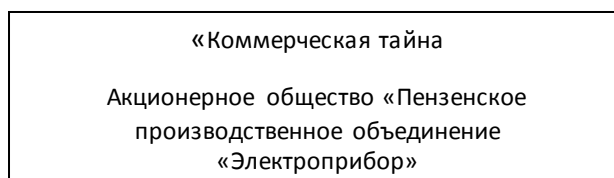


Рисунок Д.1 – Гриф «Коммерческая тайна»

Д.5.4 Разработанному в структурном подразделении Общества документу (проекту документа), содержащему информацию, составляющую коммерческую тайну, гриф конфиденциальности присваивает исполнитель документа, руководитель структурного подразделения или иное должностное лицо,

подписывающее (утверждающее) документ. Указанные лица несут дисциплинарную и иную ответственность, предусмотренную действующим законодательством, за невыполнение данного требования.

Д.5.5 Основанием для присвоения грифа конфиденциальности разрабатываемому документу (проекту документа) является включение в него информации, указанной в «Перечне...». Гриф конфиденциальности присваивается также выпискам из документов, содержащих информацию, составляющую коммерческую тайну, если в выписке содержится такая информация.

Д.5.6 Снятие грифа конфиденциальности с документов осуществляется:

- по истечении указанного в перечне срока действия ограничения доступа к информации, содержащейся в документе и составляющей коммерческую тайну Общества;

- в связи с исключением из перечня информации, составляющей коммерческую тайну Общества.

Д.5.7 Порядок регистрации, учета, оформления, тиражирования, хранения, использования и уничтожения конфиденциальных документов и других материальных носителей, содержащих информацию, составляющую коммерческую тайну, определяется «Инструкцией о порядке обращения с конфиденциальной документацией», утвержденной генеральным директором.

Д.5.8 Документы, содержащие информацию, составляющую коммерческую тайну Общества, должны храниться в сейфах или запираемых шкафах (ящиках).

Д.5.9 Осуществлять передачу конфиденциальной информации ценными (заказными) почтовыми отправлениями с уведомлением о вручении почтового сообщения адресату.

Д.5.10 Передача документов, содержащих информацию, составляющую коммерческую тайну Общества, по незащищенным каналам связи (с использованием факсимильной связи, сетей Интернет) запрещается. в исключительных случаях разрешается отправка по электронной почте, только

после согласования с отделом №135 и применения мер по защите информации.

Д.5.11 Использование информации, составляющей коммерческую тайну Общества, работниками, проходящими обучение, профессиональную подготовку и переподготовку в учебных заведениях, в том числе при написании ими курсовых или дипломных работ, запрещается.

Д.5.12 Обучение работников Общества правилам обращения с информацией, составляющей коммерческую тайну, осуществляется путем:

- проведения начальниками структурных подразделений инструктивных занятий с подчиненными работниками;
- самостоятельного изучения работником правовых актов Общества, регламентирующих вопросы режима коммерческой тайны.

Д.6 Учёт лиц, получивших доступ к информации, составляющей коммерческую тайну Общества

в структурных подразделениях Общества лицом, ответственным за конфиденциальное делопроизводство или уполномоченным по защите коммерческой тайны, ведется учет:

- работников структурных подразделений, получивших доступ к информации, составляющей коммерческую тайну Общества и ее контрагентов;
- органов государственной власти, иных государственных органов и органов местного самоуправления, которым была предоставлена в соответствии с их мотивированными требованиями (запросами) находящаяся в ведении структурного подразделения информация, составляющая коммерческую тайну, и переданных им материалов;
- контрагентов, которым в соответствии с заключенными соглашениями о конфиденциальности была передана информация или которым был предоставлен доступ к информации, составляющей коммерческую тайну Общества.

Д.7 Регулирование отношений с контрагентами и третьими лицами по использованию информации, составляющей коммерческую тайну Общества

Д.7.1 Для обеспечения охраны информации, составляющей коммерческую тайну, между АО «ПО «Электроприбор» и ее контрагентами при исполнении договорных обязательств, в ходе которых возможен доступ к информации, составляющей коммерческую тайну Общества со стороны контрагентов, заключаются соглашения о конфиденциальности.

Д.7.2 Ответственность за организацию оформления (подготовку) соглашения о конфиденциальности несет руководитель подразделения, заключающего договор. Соглашение о конфиденциальности подписывается Обществом и контрагентом в двух экземплярах, одновременно с договором.

Д.7.3 Срок действия соглашения о конфиденциальности устанавливается с учетом срока действия договора с контрагентом и срока действия ограничения доступа к получаемой информации, составляющей коммерческую тайну.

Д.7.4 Первый экземпляр заключенных соглашений о конфиденциальности должен быть передан исполнителем на хранение в отдел № 135.

Д.7.5 Доступ к информации, составляющей коммерческую тайну Общества, лицам, не являющимся контрагентами, или передача такой информации контрагентам без заключения соглашения о конфиденциальности запрещен.

Д.7.6 Физические лица, привлекаемые Обществом для проведения работы по гражданско-правовым договорам, допускаются к необходимой для выполнения работы информации, составляющей коммерческую тайну Общества, только если указанным гражданско-правовым договором предусмотрены обязанности по неразглашению конфиденциальной информации.

Д.7.7 В договоры о проведении научно-исследовательских, проектно-исследовательских и опытно-конструкторских работ, предусматривающие использование информации, составляющей коммерческую тайну Общества, или создание научно-технического продукта, содержащего такую информацию, а также в технические задания на выполнение указанных работ включается

требование соблюдения режима коммерческой тайны Общества в отношении такой информации.

Д.8 Контроль за соблюдением режима коммерческой тайны в обществе

Д.8.1 Контроль за соблюдением режима коммерческой тайны в Обществе, осуществляется в целях определения соответствия принятых мер по защите информации, составляющей коммерческую тайну, установленному режиму коммерческой тайны, выявления возможных каналов утечки и несанкционированного доступа к данной информации и принятия мер по их пресечению.

Д.8.2 Ежедневный контроль за соблюдением режима коммерческой тайны проводит начальник соответствующего структурного подразделения. Для осуществления принятых мер по защите коммерческой тайны в подразделениях назначается уполномоченный по защите коммерческой тайны. Его обязанности регламентируются «Инструкцией уполномоченному по защите коммерческой тайны в структурных подразделениях Общества, утвержденной генеральным директором Общества.

Д.8.3 Отдел № 135 осуществляет контроль за соблюдением режима коммерческой тайны путем проведения плановых проверок или проверок по указанию генерального директора.

Д.8.4 Основанием для проведения внеплановой проверки является информация о фактах нарушения режима коммерческой тайны, изложенных в служебных записках работников Общества.

Д.8.5 Отдел № 135 осуществляет периодический контроль исходящей корреспонденции подразделений Общества, путем выборочной проверки исходящих электронных документов в подразделениях на наличие в них сведений составляющих коммерческую тайну.

Д.8.6 В ходе контроля за соблюдением режима коммерческой тайны в Обществе проводится:

- оценка деятельности структурного подразделения Общества по

защите информации, составляющей коммерческую тайну;

- анализ состояния защищенности информационных ресурсов и технологий, подготовка предложений по совершенствованию их защиты;
- выявление каналов утечки информации и несанкционированного доступа к информации, составляющей коммерческую тайну;
- сверка документации, содержащей коммерческую тайну Общества (ежегодно);
- анализ причин нарушений и недостатков в организации и обеспечении защиты информации, составляющей коммерческую тайну, в структурных подразделениях, разработка рекомендаций по их устранению.

Д.8.7 Оперативный контроль за использованием информационных ресурсов Общества во время проведения выставок, конференций, семинаров, встреч с представителями СМИ осуществляется уполномоченными по защите коммерческой тайны или специалистами отдела № 135, включаемыми в состав участников данных мероприятий.

Д.8.8 При выявлении факта разглашения информации, составляющей коммерческую тайну, или утраты документов или иных носителей информации, содержащих указанную информацию, в установленном в Обществе порядке проводится служебное расследование, назначенное генеральным директором.

Д.8.9 В ходе служебного расследования устанавливаются:

- обстоятельства разглашения информации, составляющей коммерческую тайну, утраты документа или иного носителя информации, имеющего гриф конфиденциальности;
- лица, виновные в разглашении информации, составляющей коммерческую тайну, или утрате документа или иного носителя информации, имеющего гриф конфиденциальности;
- причины и условия, способствующие разглашению информации, составляющей коммерческую тайну, утрате документа или иного носителя информации, имеющего гриф конфиденциальности.

Д.8.10 При обнаружении в действиях работника признаков состава преступления Общества направляет соответствующее сообщение в правоохранительные органы.

Д.9 Технические меры обеспечения режима коммерческой тайны

Д.9.1 Уровень технической защиты информации, составляющей коммерческую тайну, а также перечень необходимых мер защиты определяются генеральным директором, дифференцировано, с учетом соотношения затрат на организацию защиты информации

Д.9.2 Технические меры обеспечения защиты информации, составляющей коммерческую тайну, при ее обработке техническими средствами устанавливаются Специальными требованиями и рекомендациями по технической защите конфиденциальной информации, утвержденными приказом Гостехкомиссии России от 30.08.2002 г. N 282 [10] и правовыми актами Общества, регламентирующими организацию технической защиты конфиденциальной информации в Обществе.

Д.9.3 Меры по охране конфиденциальности информации признаются разумно достаточными, если:

- исключается доступ к информации, составляющей коммерческую тайну, любых лиц без согласия ее обладателя;
- обеспечивается возможность использования информации, составляющей коммерческую тайну, работниками и передачи ее контрагентам без нарушения режима коммерческой тайны.

Д.9.4 Обработка сведений, составляющих коммерческую тайну Общества производить в автоматизированных системах с классом защищенности от НСД к информации не ниже 1Д.

Д.10 Предоставление информации, составляющей коммерческую тайну общества органам государственной власти

Д.10.1 Предоставление информации, составляющей коммерческую тайну Общества, органам государственной власти осуществляется в случаях, предусмотренных законодательством Российской Федерации.

Д.10.2 Информация, составляющая коммерческую тайну Общества, подлежит предоставлению органам государственной власти, иным государственным органам и органам местного самоуправления на основании мотивированного требования указанных органов. Мотивированное требование должно быть подписано уполномоченным должностным лицом, содержать указание цели, правовое основание затребования информации, составляющей коммерческую тайну Общества, и срок предоставления этой информации, если иное не установлено Федеральными законами.

Д.10.3 Информация, составляющая коммерческую тайну Общества, в обязательном порядке предоставляется судам, органам прокуратуры, органам предварительного следствия, органам дознания по делам, находящимся в их производстве, по их запросу в порядке и на основаниях, которые предусмотрены законодательством Российской Федерации.

Д.10.4 Решение о предоставлении указанной информации принимается генеральным директором или заместителями генерального директора Общества по направлениям деятельности.

Структурные подразделения, в ведении которых находится информация, составляющая коммерческую тайну Общества, подлежащая в соответствии с поступившим требованием (запросом) предоставлению органам государственной власти, обязаны:

- проверить основания требований (запросов) на получение соответствующей информации;
- представить генеральному директору или заместителю генерального директора по направлению деятельности, согласованную с отделом № 135, справку–обоснование для принятия решения о передаче информации.

Д.10.5 Доступ работников органов государственной власти к информации, составляющей коммерческую тайну Общества, осуществляется в пределах полномочий этих органов на основании предписаний, подписанных их руководителями или надлежащим образом уполномоченными лицами, по решению генерального директора или заместителей генерального директора

Общества по направлениям деятельности.

Д.10.6 в случае необходимости выемки документов, содержащих информацию, составляющую коммерческую тайну Общества должен быть оформлен протокол выемки, с указанием грифа конфиденциальности и учетного номера изымаемого документа.

Д.11 Ответственность за разглашение сведений, составляющих коммерческую тайну

Д.11.1 Руководитель структурного подразделения несет персональную ответственность за соблюдение режима коммерческой тайны в подразделении и выполнение работниками структурных подразделений требований правовых актов Общества, регламентирующих вопросы охраны информации, составляющей коммерческую тайну Общества.

Д.11.2 Ответственность за разглашение сведений, составляющих коммерческую тайну, несет персонально каждый сотрудник Общества, имеющий доступ к этим сведениям и допустивший их разглашение. Лица, разгласившие указанные сведения привлекаются к дисциплинарной, гражданско–правовой, административной или уголовной ответственности в порядке, установленном Федеральными законами, а также трудовым и гражданско–правовым договорами.

Д.11.3 Сотрудник, который в силу служебного положения получил доступ к коммерческой тайне, в случае умышленного разглашения или несанкционированной передачи третьей стороне такой информации несет ответственность в соответствии с законодательством Российской Федерации.

Д.11.4 Работник структурного подразделения, которому в силу трудовых отношений с Обществом стала известна информация, составляющая коммерческую тайну (в случае умышленного или неосторожного разглашения ее), при отсутствии в его действиях состава преступления несет дисциплинарную ответственность в соответствии с законодательством Российской Федерации, при наличии – несет уголовную ответственность в соответствии с законодательством Российской Федерации.

В случае если действия лица, разгласившего сведения, составляющие коммерческую тайну, причинили экономический вред, и при отказе добровольно возместить его, руководство Общества имеет право обратиться в суд для защиты своих интересов.

Д.11.5 Ответственность контрагента за неправомерное использование информации, составляющей коммерческую тайну Общества, устанавливается в соответствии с условиями заключенного между Обществом и контрагентом соглашения о конфиденциальности и положениями заключенного между Обществом и контрагентом договора.

Д.12 Особенности охраны иной конфиденциальной информации

Перечень иной конфиденциальной информации, не являющейся коммерческой тайной, определяется согласно Указу Президента Российской Федерации от 6 марта 1997 года №188 «Об утверждении перечня сведений конфиденциального характера» [11].

Охрана иной конфиденциальной информация, распространение которой ограничено нормативными актами АО «ПО «Электроприбор» и вышестоящих организаций осуществляется в соответствии с настоящим Положением.

На документах и других материальных носителях, содержащих иную конфиденциальную информацию, проставляется отметка "Конфиденциально".

ПРИЛОЖЕНИЕ Е

(обязательное)

Положение «Об организации работы с персональными данными»

Е.1 Общие положения

Е.1.1 Настоящим Положением определяется порядок получения, хранения, передачи и любого другого использования персональных данных граждан и работников в АО «ПО «Электроприбор» (далее – Организация).

Е.1.2 Настоящее Положение разработано в соответствии с:

- Конституцией РФ [13];
- Трудовым кодексом РФ [14];
- Федеральным законом от 27 июля 2006 г. № 152–ФЗ «О персональных данных» [7];
- Федеральным законом от 27 июля 2006 г. № 149–ФЗ «Об информации, информационных технологиях и о защите информации» [9];
- Федеральным законом от 29 июля 2004 г. № 98–ФЗ «О коммерческой тайне» [8];
- перечнем сведений конфиденциального характера, утвержденным Указом Президента РФ от 06 марта 1997 г. № 188 [11].

Е.1.3 Цель разработки Положения — определение порядка обработки персональных данных работников Организации; обеспечение защиты прав и свобод работников Организации при обработке их персональных данных.

Е.1.4 Для целей настоящего положения используются следующие основные понятия:

- **персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
- **оператор** – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав

персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

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

– **автоматизированная обработка персональных данных** – обработка персональных данных с помощью средств вычислительной техники;

– **распространение персональных данных** – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

– **предоставление персональных данных** – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

– **блокирование персональных данных** – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения 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;

– **обезличивание персональных данных** – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

– **информационная система персональных данных** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

– **трансграничная передача персональных данных** – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Е.2 Персональные данные работников

Е.2.1 Сбор и обработка персональных данных работников

Персональные данные работника Организации (далее – работник) относятся к конфиденциальной информации, то есть порядок работы с ними регламентирован трудовым законодательством РФ, Федеральным Законом от 27 июня 2006 г. № 152–ФЗ «О персональных данных» [7] и осуществляется с соблюдением строго определенных правил и условий. Данные требования установлены ст. 86 Трудового кодекса РФ [14] и не подлежат изменению, исключению, так как являются обязательными для сторон трудовых отношений.

В целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных работника обязуются соблюдать следующие требования:

- обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества работодателей, работников и третьих лиц;

- при определении объема и содержания обрабатываемых персональных данных работника работодатель должен руководствоваться Конституцией РФ, Трудовым кодексом РФ [14], Федеральным законом от 27 июня 2006 г. № 152–ФЗ «О персональных данных» [7] и иными Федеральными законами;

- отделом кадров берется согласие на обработку персональных данных у соискателя на кадровый резерв. при трудоустройстве начальник отдела кадров обязан ознакомить соискателя работы или его представителя с положением «об организации работы с персональными данными на АО «ПО «Электроприбор»

под личную подпись до подписания трудового договора, а также получить письменное согласие на обработку его персональных данных;

- письменное согласие на обработку персональных данных дают все работники организации с правом отзыва данного согласия по письменному заявлению. в случае отзыва согласия на обработку персональных данных работодатель должен довести до работника правовые последствия;

- все персональные данные работника следует получать лично у работника. если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, характере подлежащих получению персональных данных (например, оформление запроса на прежнее место работы работника в целях выяснения его профессиональных качеств, запроса в учебное заведение о подлинности документа об образовании и т.п.) и последствиях отказа работника дать письменное согласие на их получение;

- работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. в случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции РФ работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия;

- работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных Федеральным законом;

- при принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронно.

При поступлении на работу работник предоставляет персональные данные о себе в документированной форме, а именно:

- паспорт или иной документ, удостоверяющий личность;
- трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или работник поступает на работу на условиях совместительства;

- страховое свидетельство государственного пенсионного страхования;
- документы воинского учета – для военнообязанных и лиц, подлежащих призыву на военную службу;

- документ об образовании, о присвоении ученой степени, ученого звания, о квалификации или наличии специальных знаний при поступлении на работу, требующую специальных знаний или специальной подготовки;

- в отдельных случаях с учетом специфики работы в соответствии с действующим законодательством РФ может предусматриваться необходимость предъявления при заключении трудового договора дополнительных документов (например, медицинское заключение на монтажников, для лиц в возрасте до 18 лет; для лиц, занятых на тяжелых работах и работах с вредными и (или) опасными условиями труда, а также на работах, связанных с движением транспорта, при оформлении допуска к государственной тайне).

Запрещается требовать от лица, поступающего на работу, документы помимо предусмотренных Трудовым кодексом РФ [14], иными Федеральными законами, указами Президента РФ и постановлениями Правительства РФ.

При заключении трудового договора и в ходе трудовой деятельности может возникнуть необходимость о предоставлении работником документов:

- о возрасте детей;
- о беременности женщины;
- об инвалидности;
- о донорстве;
- о составе семьи, изменении семейного положения;
- о доходе с предыдущего места работы;

- о необходимости ухода за больным членом семьи;
- иные документы в соответствии с законодательством РФ.

После того, как будет принято решение о приеме работника на работу, а также впоследствии в процессе трудовой деятельности к документам, содержащим персональные данные работника, также будут относиться:

- трудовой договор и приказ о приеме работника на работу;
- приказы о поощрениях и взысканиях;
- дополнительные соглашения к трудовому договору и приказы об изменении условий трудового договора;
- анкета с фотографией;
- заключение предварительного медицинского осмотра;
- копии паспорта, страхового свидетельства государственного пенсионного страхования, свидетельства о постановке на учет в налоговом органе, документа об образовании, военного билета;
- заявления работника;
- характеристики–ходатайства;
- иные документы в соответствии с законодательством РФ.

Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом не менее чем за три рабочих дня и от него должно быть получено письменное согласие (либо письменный отказ), которое работник должен дать в течение пяти рабочих дней с момента получения от работодателя соответствующего уведомления.

Е.2.2 Защита персональных данных работников

В целях обеспечения защиты персональных данных, хранящихся у работодателя, работники имеют право на:

- полную информацию об их персональных данных и обработке этих данных, в частности работник имеет право знать перечень обрабатываемых персональных данных, кто и в каких целях использует или использовал его персональные данные;

- свободный и бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных Федеральным законом;

- определение представителей для защиты своих персональных данных;

- доступ к относящимся к ним медицинским данным;

- требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований трудового кодекса РФ [14] и Федеральным законом от 27 июня 2006 г. № 152–ФЗ «О персональных данных» [7]. При отказе работодателя исключить или исправить персональные данные работник имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия. персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения;

- требование об извещении работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;

- обжалование в суд любых неправомерных действий или бездействия работодателя при обработке и защите его персональных данных.

Лица, получающие персональные данные работника, обязаны соблюдать режим конфиденциальности. Данное положение не распространяется на обмен персональными данными работников в порядке, установленном законодательством РФ.

Защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном Трудовым кодексом РФ [14], иными Федеральными законами.

Работники, их представители должны быть ознакомлены под расписку с документами организации, устанавливающими порядок обработки

персональных данных работников, а также осведомлены об их правах и обязанностях в этой области.

Работники не должны отказываться от своих прав на сохранение и защиту тайны. Если в трудовом договоре будет содержаться норма об отказе работника от этого права, то в этой части трудовой договор будет считаться недействительным.

Работодатели, работники и их представители должны совместно вырабатывать меры защиты персональных данных работников.

Е.2.3 Хранение персональных данных работников

Персональные данные работника содержатся на бумажных носителях, в том числе в основном документе персонального учета работников – личном деле работника, в которое могут входить следующие документы:

- анкетно – биографические и характеризующие материалы, к которым относятся: анкета, автобиография (при необходимости), копии документов об образовании, результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей (в случаях, предусмотренных трудовым законодательством), заявление работника о приеме на работу, приказ о приеме на работу, трудовой договор, документы, связанные с переводом и перемещением работника (приказы, заявления работника и т.п.), выписки (копии) из документов о присвоении почетных званий, ученой степени, награждении государственными наградами, копии наградных листов, аттестационные листы, копии приказов о поощрениях, взысканиях, характеристики и рекомендательные письма, заявление работника об увольнении, приказ об увольнении и расторжении трудового договора, другие документы, нахождение которых в личном деле будет признано целесообразным;

- дополнительные материалы, к которым относятся: характеристики с прежнего места работы, фотографии, дополнение к личному делу – документ, в котором фиксируются сведения о перемещении работника по работе, другие документы, нахождение которых в личном деле будет признано целесообразным.

Сведения о работниках организации на бумажных носителях хранятся в помещении отдела кадров. Личные дела работников хранятся в отдельном помещении (архив) в алфавитном порядке с разбивкой по категории работников: рабочие, руководители, специалисты и служащие. Личные дела уволенных хранятся в архиве уволенных в алфавитном порядке.

Конкретные обязанности по хранению личных дел работников, заполнению, хранению и выдаче трудовых книжек (дубликатов трудовых книжек), иных документов, отражающих персональные данные работников, возлагаются на работников отдела кадров и закрепляются в должностных инструкциях.

В отношении некоторых документов действующим законодательством РФ могут быть установлены иные требования хранения, чем предусмотрено настоящим Положением. в таких случаях следует руководствоваться правилами, установленными соответствующим нормативным актом.

Обработка персональных данных в отделе кадров осуществляется как в автоматизированном, так и в неавтоматизированном режиме. Обеспечение безопасности персональных данных в неавтоматизированном режиме осуществляется в соответствии с «Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» утвержденном ППРФ 15 сентября 2008 г. №687 и настоящим Положением [12].

Информация, содержащая персональные данные работника, хранится в автоматизированной системе в электронном виде. в этом случае должны выполняться требования и рекомендации по защите персональных данных, обрабатываемых в автоматизированных системах.

Работодатель обеспечивает ограничение доступа к персональным данным работников лицам, не уполномоченным законом либо работодателем для получения соответствующих сведений.

Доступ к персональным данным имеют сотрудники:

- генеральный директор (доступ к ПДн работников, которые ему необходимы для исполнения своих служебных обязанностей);
- работники юридического отдела (доступ к сведениям, которые необходимы для подготовки к судебным заседаниям);
- работники бухгалтерии (доступ к ПДн работников, которые ему необходимы для исполнения своих служебных обязанностей);
- работники отдела кадров (доступ к ПДн работников, которые ему необходимы для исполнения своих служебных обязанностей);
- работники отдела труда и зарплаты (доступ к ПДн работников, которые ему необходимы для исполнения своих служебных обязанностей);
- работники отдела информационных технологий (доступ к ПДн работников, которые ему необходимы для исполнения своих служебных обязанностей);
- руководители в рамках своих подведомственных подразделений;
- работник (доступ к своим персональным данным);
- органы государственной власти, контрольные и надзорные органы (в рамках своих полномочий в соответствии с Федеральными законами).

При получении сведений, составляющих персональные данные работника, указанные лица имеют право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций, заданий.

Работник может отозвать свое согласие на обработку персональных данных по письменному заявлению.

В целях информационного обеспечения могут создаваться общедоступные источники персональных данных в виде справочников. В справочники могут включаться на основании данного Положения следующие персональные данные: фамилия, имя, отчество, день и месяц рождения (в случае юбилея 50, 60, 70 лет – год рождения), номер рабочего телефона (в том числе мобильного), занимаемая должность.

Сведения о субъекте персональных данных могут быть в любое время исключены из общедоступных источников персональных данных по требованию работника.

Е.2.4 Передача персональных данных работников

При передаче персональных данных работника работодатель должен соблюдать следующие требования:

- не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровья работника, а также в случаях, установленных Трудовым кодексом РФ [14] или иными федеральными законами;

- не сообщать персональные данные работника в коммерческих целях без его письменного согласия;

- предупреждать лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено;

- осуществлять передачу данных работника в пределах организации в соответствии с настоящим положением;

- разрешать доступ к персональным данным работника только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;

- не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции (например, допустимо обращение за информацией о состоянии здоровья беременной женщины при решении вопроса ее перевода на другую работу, исключаящую воздействие неблагоприятных техногенных факторов);

- передавать персональные данные работника представителю работника в порядке, установленном Трудовым кодексом РФ [14], иными Федеральными законами и настоящим положением, и ограничивать эту информацию только теми персональными данными, которые необходимы для выполнения указанными представителями их функций.

Данные требования установлены ст. 88 Трудового кодекса РФ [14] и не подлежат изменению, исключению, так как являются обязательными для сторон трудовых отношений.

Передача персональных данных работников Организации по запросу органов государственной власти, контрольных и надзорных органов оформляется работниками отдела кадров за подписью начальника отдела кадров или генерального директора.

Е.2.5 Обязанности работника и работодателя

В целях обеспечения достоверности персональных данных работник обязан:

- при приеме на работу предоставить работодателю полные и достоверные данные о себе;
- в случае изменения сведений, составляющих персональные данные работника, незамедлительно предоставить данную информацию работодателю.

Работодатель обязан:

- осуществлять защиту персональных данных работника;
- обеспечить хранение первичной учетной документации по учету труда и его оплаты, к которой, в частности, относятся документы по учету кадров, документы по учету использования рабочего времени и расчетов с работниками по оплате труда и др. При этом персональные данные не должны храниться дольше, чем это оправдано выполнением задач, для которых они собирались, или дольше, чем это требуется в интересах лиц, о которых собраны данные;
- заполнение документации, содержащей персональные данные работника, осуществлять в соответствии с унифицированными формами первичной учетной документации по учету труда и его оплаты, утвержденными

постановлением Госкомстата России от 05.01.04 № 1 «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты»;

- по письменному заявлению работника не позднее трех дней со дня подачи этого заявления выдавать последнему копии документов, связанных с работой (копии приказа о приеме на работу, приказов о переводах на другую работу, приказа об увольнении с работы; выписки из трудовой книжки или копии трудовой книжки; справки о заработной плате, периоде работы у данного работодателя и другое). Копии документов, связанных с работой, должны быть заверены надлежащим образом и предоставляться работнику безвозмездно;

- вести учет передачи персональных данных работника третьим лицам путем ведения соответствующего журнала, отражающего сведения о поступившем запросе (кто является отправителем запроса, дата его поступления работодателю), дату ответа на запрос, когда именно информация была передана либо отметку об отказе в ее предоставлении, либо ограничиваться помещением в личное дело работника выписок, копий документов и т.п., отражающих сведения о поступившем запросе и результатах его рассмотрения;

- в целях обеспечения сохранности документов по личному составу увольняемых работников в случае реорганизации или ликвидации организации, а также социальной защищенности граждан, выполняющих работу по трудовому договору, включать в свои учредительные документы правила учета и сохранности документов по личному составу, а также своевременной передачи их на государственное хранение при реорганизации или ликвидации юридического лица (Распоряжение Правительства РФ от 21.03.1994 № 358–Р «Об обеспечении учета и сохранности документов по личному составу, а также своевременной передачи их на государственное хранение при реорганизации или ликвидации юридического лица»[]);

- после увольнения работника хранить его личное дело в установленном порядке в течение 75 (семидесяти пяти) лет или до момента ликвидации Организации. в случае реорганизации или ликвидации организации, филиалов

учет и сохранность документов по личному составу, порядок передачи их на государственное хранение осуществлять в порядке, установленном действующим законодательством Российской Федерации.

Е.3 Ответственность за нарушение норм, регулирующих получение, обработку и защиту персональных данных граждан и работников организации

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных гражданина привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом РФ [14] и иными Федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном Федеральными законами.

За разглашение конфиденциальных сведений, содержащихся в базах, работники, уполномоченные на ведение и хранение баз данных ИСПДн Организации, могут привлекаться в соответствии с законодательством Российской Федерации к дисциплинарной ответственности.

Работники, уполномоченные на ведение и хранение баз данных ИСПДн Организации незаконно использовавшие или разгласившие указанную информацию без согласия работника из корыстной или иной личной заинтересованности и тем самым причинивший крупный ущерб, несет уголовную ответственность на основании ст. 173.2 Уголовного кодекса РФ.

Начальник отдела кадров несет персональную ответственность за сохранность документов, связанных с трудовой деятельностью сотрудников.

Неправомерный отказ работодателя исключить или исправить персональные данные гражданина, а также любое иное нарушение прав гражданина на защиту персональных данных влечет возникновение у гражданина права требовать устранения нарушения его прав и компенсации причиненного таким нарушением морального вреда.

Е.4 Заключительные положения

Настоящее Положение вступает в силу с момента его утверждения генеральным директором Организации.

В случае необходимости и с учетом действующего законодательства в настоящее Положение могут быть внесены изменения и дополнения на основании приказа генерального директора организации.

ПРИЛОЖЕНИЕ Ж

(обязательное)

Проект приказа об утверждении перечня лиц, допущенных к персональным данным, обрабатываемым в информационной системе персональных данных

«Персонал»

Акционерное общество «Пензенское производственное объединение
«Электроприбор»

ПРИКАЗ

«__» _____ 2016г.

№ _____

**Об утверждении перечня
лиц, доступ которых к
персональным данным,
обрабатываемым в
информационной системе,
необходим для
выполнения ими
служебных (трудовых)
обязанностей**

Во обеспечение требований подпункта в) пункта 13 Постановления
Правительства №1119 от 1 ноября 2012 г.

ПРИКАЗЫВАЮ:

Определить следующий перечень лиц, доступ которых к персональным данным в информационной системе необходим для выполнения ими служебных (трудовых обязанностей):

- генеральный директор (доступ к ПДн работников, которые ему необходимы для исполнения своих служебных обязанностей);
- работники юридического отдела (доступ к сведениям, которые необходимы для подготовки к судебным заседаниям);
- работники бухгалтерии (доступ к ПДн работников, которые ему необходимы для исполнения своих служебных обязанностей);
- работники отдела кадров (доступ к ПДн работников, которые ему необходимы для исполнения своих служебных обязанностей);
- работники отдела труда и зарплаты (доступ к ПДн работников, которые ему необходимы для исполнения своих служебных обязанностей);

- работники отдела информационных технологий (доступ к ПДн работников, которые ему необходимы для исполнения своих служебных обязанностей);
- руководители в рамках своих подведомственных подразделений;
- работник (доступ к своим персональным данным);
- органы государственной власти, контрольные и надзорные органы (в рамках своих полномочий в соответствии с федеральными законами).

Генеральный директор
АО «ПО «Электроприбор»

Почивалов Ю.С.

Рисунок Ж.2 – Проект приказа об утверждении матрицы доступа, часть №2

ПРИЛОЖЕНИЕ И

(обязательное)

Проект приказа о назначении ответственного за организацию обработки персональных данных в информационной системе персональных данных

«Персонал»

Акционерное общество «Пензенское производственное объединение
«Электроприбор»

ПРИКАЗ

«__» _____ 2016г.

№ _____

**О назначении
ответственного за
обработку
персональных данных**

Во исполнение подпункта г) пункта 13 постановления Правительства РФ от 1.11.2012 № 1119 «Требования к защите персональных данных при их обработке в информационных системах персональных данных»

ПРИКАЗЫВАЮ:

Назначить _____

(должность, подразделение, Ф.И.О.)

ответственным за организацию обработки персональных данных в ИСПДн – «Персонал».

Генеральный директор
АО «ПО «Электроприбор»

Почивалов Ю.С.

Рисунок И.1 – Проект приказа о назначении ответственного за обработку ПДн

МИНОБРАЗОВАНИЯ РОССИИ

Федеральное государственное бюджетное образовательное учреждение

высшего профессионального образования

«НИЖНИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УДК 004.056

Политехнический институт

Факультет приборостроения,

информационных технологий и

электроники

Выпускающая кафедра:

Информационная безопасность систем

и технологий

Учебная группа ИПИИ

УТВЕРЖДАЮ

Зав. кафедрой ИБСТ

к.т.н., доцент

С.Л. Зефирова

«27» 04 2016 г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ

студента группы ИПИИ Сазонова Геннадия Сергеевича

Специальность 100503 – Информационная безопасность

автоматизированных систем

Тема дипломного проекта: Обеспечение защиты конфиденциальной информации в АО «ПО «Электронприбор»

Руководитель ВКР

Начальник ОТЗИ и ПДТР АО «ПО «Электронприбор»

Нормоконтролер

к.т.н., доцент

Дубин Р.М.

Фатеев А.Г.

1 Цели и задачи ВКР

Цель работы – разработка политики по обеспечению защиты конфиденциальной информации в АО «ПО «Электроприбор».

Политика по обеспечению защиты конфиденциальной информации необходима для определения принципов обеспечения защиты конфиденциальной информации, методов их реализации, а также выбора механизмов обеспечения её безопасности.

2 Тактико-технические требования к выполнению ВКР

Технические требования.

Политика по обеспечению защиты конфиденциальной информации должна содержать результаты следующих процессов:

- идентификация организационной структуры АО «ПО «Электроприбор»;
- идентификация конфиденциальной информации, обрабатываемой на предприятии, и определение уровней её значимости;
- оценка исходной защищенности информационных систем АО «ПО «Электроприбор»;
- выбор мер и средств защиты для информационных систем АО «ПО «Электроприбор».

Выявление и определение уровней значимости информации должно содержать:

- определение категории обрабатываемых персональных данных;
- определение уровней значимости сведений, составляющих коммерческую тайну;
- определение уровней значимости иной конфиденциальной информации.

Оценка исходной защищённости должна содержать:

- определение масштабов информационных систем;
- составление перечня угроз информационной безопасности;

- идентификацию актуальных угроз информационной безопасности;
- разработку моделей угроз для информационных систем;
- разработку моделей нарушителя.

Выбор мер и средств защиты должен содержать:

- выбор защитных мер для обеспечения безопасности конфиденциальной информации в информационных системах;
- выбор программных, программно – аппаратных и (или) технических средств для реализации части выбранных защитных мер;
- разработку положения в отношении обработки персональных данных и иных документов в соответствии с законодательством о персональных данных;
- разработку положения о соблюдении режима коммерческой тайны в соответствии с федеральным законом №98-ФЗ «О коммерческой тайне»;
- разработку инструкции по соблюдению режима конфиденциальности;
- разработку инструкции администратора безопасности информационных систем.

3 Требования к разрабатываемой документации

Отчет по ВКР выполняется в соответствии с требованиями ГОСТ 7.32.

Перечень и содержание графической части ВКР:

- организационная структура АО «ПО «Электроприбор» – 1л., ф. А1 (плакат);
- структуры информационных систем АО «ПО «Электроприбор» – 3л., ф. А1 (плакат)
- информационные потоки в информационных системах АО «ПО «Электроприбор» – 3л., ф. А1 (плакат);
- отношение защитных мер и актуальных угроз – 2л., ф. А1(плакат).

Электронная копия отчета и графической части ВКР должна быть представлена на магнитном или оптическом носителе.

4 Сроки выполнения ВКР

Тема утверждена приказом ректора ПГУ № 491 а/о от «25» 04 2016 г.

Дата выдачи задания «17» февраля 2016 г.

Время дипломного проектирования с 18.04 2016 г. по 20.06 2016 г.

Задание к исполнению принял « » _____ 2016 г.

Исполнитель ВКР Сазонов Г.С. Сазонов Г.С.

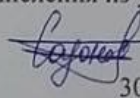
Ректору Пензенского
государственного университета
А. Д. Гулякову
студента 5 курса ФПИТЭ
очной формы обучения
Сазонова Геннадия Сергеевича

заявление.

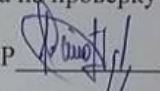
Я, Сазонов Геннадий Сергеевич, студент 5 курса очной формы обучения специальности 10.05.03 – «Информационная безопасность автоматизированных систем», прошу провести проверку с использованием системы «Антиплагиат» дипломного проекта на тему «Обеспечение защиты конфиденциальной информации в АО «ПО «Электроприбор», выполненной мной самостоятельно, на содержание элементов плагиата.

Все прямые заимствования из печатных и электронных источников, а также из защищенных ранее выпускных квалификационных работ, кандидатских и докторских диссертаций имеют соответствующие ссылки.

Я ознакомлен с действующим Стандартом университета «Выпускная квалификационная работа обучающихся по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры», согласно которому обнаружение плагиата является основанием для недопуска ВКР к защите и отчисления из университета.

 /Г.С. Сазонов/
30.05.2016

ВКР представлена на проверку 31.05.2016

Руководитель ВКР  /Р.М. Дубин/

Протокол

проверки на оригинальность в системе «Антиплагиат.ВУЗ» выпускной квалификационной работы на тему «Обеспечение защиты конфиденциальной информации в АО «ПО «Электроприбор» студента 5 курса Г.С. Сазонова специальности 10.05.03 – «Информационная безопасность автоматизированных систем».

Руководитель ВКР, начальник отдела ТЗИиПДТР АО «ПО «Электроприбор» Дубин Ринат Мансурович.

Отчет о проверке № 1

ФИО: Иванов Алексей Петрович
дата загрузки: 02.06.2016 23:48:15
пользователь: sp_nestov@yandex.ru / ID: 1267386
отчет предоставлен сервисом «Антиплагиат»
на сайте <http://www.antiplagiat.ru>

Информация о документе

№ документа: 32
Имя исходного файла: ВКР_Сазонов_ГС_11ПМ1.pdf
Размер текста: 2293 кБ
Тип документа: Не указано
Символов в тексте: 269527
Слов в тексте: 30905
Число предложений: 861

Информация об отчете

Дата: Отчет от 03.06.2016 06:43:11 - Последний готовый отчет
Комментарий: не указан
Оценка оригинальности: 72.15%
Заимствования: 27.85%
Цитирование: 0%



Оригинальность: 72.15%
Заимствования: 27.85%
Цитирование: 0%

14.06.2016 г.

Секретарь ГЭК

Р.М. Дубин

А.П.Иванов

УТВЕРЖДАЮ
Заместитель генерального
директора по безопасности
АО «ПО «Электроприбор»
Н.А. Дудко
« 11.01.2016г. »

АКТ О ВНЕДРЕНИИ
результатов выпускной квалификационной работы
Сазонова Г.С.

Комиссия в составе Дубина Р.М. (председатель), Зосимова И.В. и Николаевой А.Г. установила, что представленные в выпускной квалификационной работе результаты по обеспечению защиты конфиденциальной информации в АО «ПО «Электроприбор» использованы в системе защиты информации организации. В частности, внедрены:

- 1) политика по обеспечению защиты конфиденциальной информации;
- 2) инструкция администратора безопасности;
- 3) инструкция по соблюдению режима конфиденциальности.

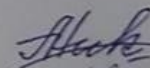
Председатель комиссии:
начальник ОТЗИиПДТР



Р.М.Дубин

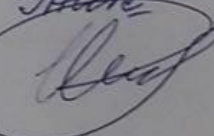
Члены комиссии:

ведущий инженер ОТЗИиПДТР



А.Г.Николаева

инженер 1 категории ОТЗИиПДТР



И.В.Зосимов

ОТЗЫВ

на выпускную квалификационную работу студента

Пензенского государственного университета

Сазонова Геннадия Сергеевича

Тема работы: Обеспечение защиты конфиденциальной информации в АО «ПО «Электроприбор».

Целью выпускной квалификационной работы Сазонова Г.С. являлась разработка политики по обеспечению защиты конфиденциальной информации в АО «ПО «Электроприбор».

Политика по обеспечению защиты конфиденциальной информации в организации разработана на основе методических и руководящих документов ФСТЭК России, а также внутренних стандартов и стандартов вышестоящих организаций в области защиты информации.

Содержание выпускной квалификационной работы полностью соответствует требованиям задания на выпускную квалификационную работу. В результате выполнения работы поставленные техническим заданием вопросы решены в полном объеме, с грамотным обоснованием.

В ходе дипломного проектирования Сазонов Г.С. показал себя грамотным специалистом, умеющим самостоятельно ставить и решать технические задачи, а также продемонстрировал умение работать с научной, технической, нормативной и методической литературой.

Сазонов Г.С. проявил высокую степень усвоения знаний по общетехническим и специальным дисциплинам, а также умение использовать их в самостоятельной работе.

Решаемые технические задачи полно и квалифицировано изложены в пояснительной записке к выпускной квалификационной работе. Графическая часть работы соответствует установленным требованиям.

Разработанная в ходе выполнения задания на выпускную квалификационную работу политика по обеспечению защиты конфиденциальной информации организации принята для внедрения в систему

защиты информации АО «ПО «Электроприбор», о чем свидетельствует акт о внедрении.

Выпускная квалификационная работа Сазонова Г.С. выполнена на высоком уровне, соответствующем квалификации специалиста по защите информации, удовлетворяет требованиям, предъявляемым к выпускным квалификационным работам студентов, обучающихся по специальности 100503 «Информационная безопасность автоматизированных систем», и может быть допущен к защите в Государственной аттестационной комиссии. При наличии акта о внедрении результатов ВКР, выполнение ВКР оценивается в 20 баллов.

Руководитель дипломной работы:

Начальник ОТЗИ и ПДТР
АО «ПО «Электроприбор»



Дубин Р.М.

РЕЦЕНЗИЯ

на выпускную квалификационную работу студента

Пензенского государственного университета

Сазонова Геннадия Сергеевича

Тема работы: Обеспечение защиты конфиденциальной информации в АО «ПО «Электроприбор».

Целью выпускной квалификационной работы Сазонова Г.С. являлась разработка политики по обеспечению защиты конфиденциальной информации в АО «ПО «Электроприбор».

Политика по обеспечению защиты конфиденциальной информации в организации разработана на основе методических и руководящих документов ФСТЭК России, а также внутренних стандартов и стандартов вышестоящих организаций в области защиты информации.

Содержание выпускной квалификационной работы полностью соответствует теме и требованиям задания на выпускную квалификационную работу. В результате выполнения работы поставленные заданием вопросы решены в полном объеме, с грамотным обоснованием.

Актуальность темы дипломной работы обусловлена востребованностью обеспечения надёжной защиты конфиденциальной информации с целью выполнения требований законодательства РФ, предотвращения незапланированных финансовых и иных потерь, упущения коммерческой выгоды и поддержания стабильного функционирования организации.

Разработанная в ходе выполнения задания на выпускную квалификационную работу политика по обеспечению защиты конфиденциальной информации организации, а также иные выводы и рекомендации, сделанные в ходе выполнения работы являются корректно обоснованными и имеют серьёзное практическое значение для системы защиты информации АО «ПО «Электроприбор» в целом, о чём, свидетельствует акт о внедрении.

В качестве недостатка можно отметить отсутствие сравнения рекомендуемых к применению программных средств защиты информации с существующими на рынке аналогичными решениями.

Выпускная квалификационная работа Сазонова Г.С. выполнена на высоком уровне, соответствующем квалификации специалиста по защите информации, удовлетворяет требованиям, предъявляемым к выпускным квалификационным работам студентов, обучающихся по специальности 100503 «Информационная безопасность автоматизированных систем», и может быть допущена к защите в Государственной аттестационной комиссии. Выполнение ВКР оценивается в 9 баллов.

Рецензент:

Зам. директора по режиму
АО «ПО «Электроприбор»



Дудко Н.Н.