

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

Политехнический институт
Факультет приборостроения,
информационных технологий и
электроники

Специальность 100503 -

Специализация -

Кафедра
«Информационная безопасность
систем и технологий»

Информационная безопасность
автоматизированных систем
Защищенные автоматизированные
системы управления

ДИПЛОМНЫЙ ПРОЕКТ

на тему

ИНФОРМАЦИОННАЯ СИСТЕМА ПЕРСОНАЛЬНЫХ ДАННЫХ

АО «РАДИОЗАВОД»

Студент

Руководитель

Нормоконтролер

Рецензент

Работа допущена к защите (протокол заседания кафедры от 26.06.18 № 10)

Заведующий кафедрой

Работа защищена с отметкой хорошо (протокол заседания ГЭК от 27.06.18 № 7)

Секретарь ГЭК

Людин Павел Васильевич

Владимир Борисович Бородин

Алексей Петрович Иванов

Наталья Васильевна Егорова

Сергей Львович Зефирков

Алексей Петрович Иванов

Пенза 2018

Проверено Зданин 6
23.06.18.

Оглавление

Введение	10
1 Анализ актуальной законодательной базы в области защиты персональных данных	12
2 Описание существующей информационной системы персональных данных «Кадры» АО «Радиозавод».....	15
2.1 Идентификация целей обработки персональных данных.....	15
2.2 Идентификация информационных процессов.....	15
2.3 Описание структуры информационной системы персональных данных «Кадры» и идентификация технических средств обработки информации.....	23
2.4 Описание существующих организационных и технических мер защиты	26
3 Оценка соответствия действующих в организации документов, регламентирующих обработку персональных данных.....	28
4 Разработка модели угроз персональных данных в информационной системе персональных данных	29
4.1 Разработка модели нарушителя	29
4.2 Определение исходного уровня защищенности информационной системы персональных данных	35
4.3 Определение вероятности реализации угроз.....	37
4.4 Определение реализуемости угроз и оценка опасности угроз....	51
4.5 Определение актуальности угроз в информационной системе персональных данных	55
5 Определение уровня защищенности информационной системы персональных данных организации.....	58
6 Определение организационных и организационно-технических требований к обеспечению уровней защищенности персональных данных в	

информационных системах персональных данных организации и выбор мер по обеспечению безопасности персональных данных.....	60
7 Выбор средств защиты для актуальных угроз безопасности информации.....	70
8 Разработка и актуализация документации, регламентирующей обработку персональных данных.....	73
9 Вредные психофизиологические факторы, влияющие на органы зрения специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие	75
Заключение	77
Список используемых источников.....	79
Приложение А Описание технологических процессов в информационной системе персональных данных «Кадры» предприятия АО «Радиозавод».....	81
Приложение Б Акт определения уровня защищенности информационной системы персональных данных «Кадры» АО «Радиозавод».....	89
Приложение В Технический паспорт на информационную систему персональных данных «Кадры» АО «Радиозавод»	91
Приложение Г Положение об обработке и защите персональных данных АО «Радиозавод».....	116
Приложение Д Техническое задание на информационную систему персональных данных «Кадры» предприятия АО «Радиозавод».....	140
Приложение Е Частная модель угроз безопасности персональных данных в информационной системе персональных данных «Кадры» АО «Радиозавод».....	150
Приложение Ж Инструкция администратора информационной безопасности информационной системы персональных данных	162
Приложение И Инструкция пользователя информационной системы персональных данных.....	169

Приложение К Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в АО «Радиозавод».....	175
--	-----

Обозначения и сокращения

АРМ – автоматизированное рабочее место;

АС – автоматизированная система;

БД – база данных;

ОС – операционная система;

ПДн – персональные данные;

КЗ – контролируемая зона;

ПО – программное обеспечение;

ИС – информационная система;

ИСПДн – информационная система персональных данных;

СЗИ – средство защиты информации;

ФЗ – федеральный закон;

ФСТЭК – Федеральная служба по техническому и экспортному контролю;

ФСБ – Федеральная служба безопасности;

НСД – несанкционированный доступ;

ПЭВМ – персональная электронно-вычислительная машина.

Введение

Необходимость обеспечения безопасности персональных данных стала насущной задачей. В настоящее время, в связи с бурным развитием информационных технологий, главным становится вопрос защиты персональных данных при их хранении, обработке и передаче с использованием средств информатизации.

Сегодня уверенно можно говорить, что информация персонального характера является одним из основных приоритетных объектов организационно-правовой защиты, так как при определенных обстоятельствах она является производной от права на неприкосновенность частной жизни.

Защита персональных данных – это требование законодательства. Для регулирования информационных правоотношений в области персональных данных законодательством устанавливается целый ряд нормативно-правовых актов. Государство обязывает организации и физических лиц выполнять требования, направленные на обеспечение надежной защиты персональных данных.

Исходя из вышеуказанных положений, тема обеспечения защиты персональных данных в информационной системе персональных данных является актуальной.

Целью работы является анализ существующей информационной системы персональных данных «Кадры» АО «Радиозавод», актуализация и приведение системы защиты в соответствие действующим законодательным нормам.

Для выполнения поставленной цели решаются следующие задачи:

- анализ актуальной законодательной базы в области защиты информации;
- описание существующей информационной системы персональных данных;

- определение актуальных угроз и разработка модели угроз;
- определение уровня защищенности и требуемых защитных мер;
- выбор средств защиты согласно актуальным угрозам;
- разработка комплекта организационной-распорядительной документации.

1 Анализ актуальной законодательной базы в области защиты персональных данных

Основным документом, определяющим политику в области защиты прав субъектов персональных данных, является Федеральный закон «О персональных данных» от 27.07.2006 №152-ФЗ, требования которого стали обязательными к исполнению с января 2007 года. Положения данного закона конкретизируются в актах Правительства РФ, методических документах Роскомнадзора, ФСБ и ФСТЭК России.

Основные требования при обработке в рамках трудовых отношений персональных данных работника, порядок их хранения, использования и передачи, а также ответственность за нарушение этих требований регламентируются законодательным актом «Трудовой кодекс Российской Федерации» от 30.12.2001 №197-ФЗ.[7]

Обязательные к выполнению требования по защите персональных данных при обработке в информационных системах персональных данных, а также порядок определения уровня защищенности устанавливаются в постановлении Правительства РФ от 01.11.2012 №1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".[2]

Состав и содержание мер по обеспечению безопасности персональных данных в информационных системах персональных данных, не являющимися государственными информационными системами, для каждого из уровней защищенности, установленных в требованиях, утвержденных ПП №1119, утверждаются Приказом ФСТЭК от 18 февраля 2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». [3]

Требования к защите информации ограниченного доступа, в том числе персональных данных, содержащейся в государственных информационных

системах утверждаются Приказом ФСТЭК от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». Таким образом, негосударственные организации должны руководствоваться приказом ФСТЭК №21, а органы государственной власти - приказом ФСТЭК №17

Для операторов, являющимися государственными или муниципальными органами, обязательными к выполнению являются требования, направленные на обеспечение выполнения обязанностей, предусмотренных ФЗ №152 «О персональных данных», которые утверждаются Постановлением Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».[10]

Требования к материальным носителям, на которые осуществляется запись биометрических данных, при их использовании, устанавливаются в соответствии с постановлением Правительства РФ от 06.07.2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».

При обработке персональных данных, осуществляемых без использования средств автоматизации, обработка и хранение таких данных регламентируются в соответствии с Положением, утвержденным Постановлением Правительства РФ от 15 сентября 2008 г. N 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».[5]

К операторам, использующим средства криптографической защиты для обеспечения безопасности персональных данных при их обработке,

предъявляются требования к составу и содержанию мер по обеспечению безопасности персональных данных, утвержденные Приказом ФСБ РФ от 10 июля 2014 г. №378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

Порядок и методики разработки модели угроз безопасности персональных данных в ИСПД описываются в методических документах ФСТЭК России. К этим документам относятся:

- методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.[6] ФСТЭК России, 2008 год;
- методика определения угроз безопасности информации в информационных системах.[8] (Проект) ФСТЭК России, 2015 год;
- базовая модель угроз безопасности персональных данных при обработке в информационных системах персональных данных.[1] ФСТЭК, 2008 год.

2 Описание существующей информационной системы персональных данных «Кадры» АО «Радиозавод»

2.1 Идентификация целей обработки персональных данных

Целью обработки ПДн является:

- управление персоналом;
- систематизация данных о работниках предприятия;
- производство расчётов заработных плат и пенсионных отчислений;

Условием прекращения обработки персональных данных является расторжение трудового договора работника предприятия.

2.2 Идентификация информационных процессов

К функциям, которые реализуются с помощью ИСПДн «Кадры», относятся:

- прием сотрудника на работу;
- увольнение работника;
- начисление работнику заработной платы.

ИС, реализующие функции организации, потребляют некоторую входную информацию, накапливают, хранят, обрабатывают ее, и выдают результаты обработки в виде некоторой выходной информации. Это указывает на то, что они являются информационными процессами со всеми их признаками.

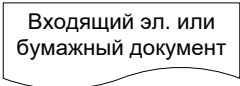
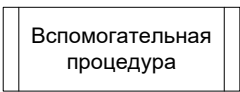
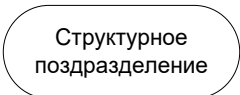
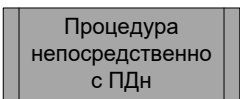
В ИСПДн «Кадры» выделено 3 информационных процесса в соответствии с реализуемыми функциями:

- прием сотрудника на работу;
- увольнение работника;
- начисление работнику заработной платы.

Описание информационных процессов представлено в виде технологических карт процессов обработки ПДн, приведенных на рисунках с 1 по 3.

Условные обозначения, используемые при описании технологических процессов в ИСПДн, представлены в таблице 1.

Таблица 1 – Условные обозначения

Обозначение	Значение
	Должностное лицо, участвующее в обработке ПДн
	Условие ветвления процесса (да/нет)
	Внешние источники ПДн
	Входящий бумажный или электронный документ, который необходим для выполнения процедуры
	Процедура технологического процесса, носящая вспомогательный характер
	Структурное подразделение, которое участвует в обработке ПДн
	Процедура технологического процесса, предусматривающая непосредственную работу с ПДн
	Путь процесса
	Логическое «И»
	Логическое «ИЛИ»

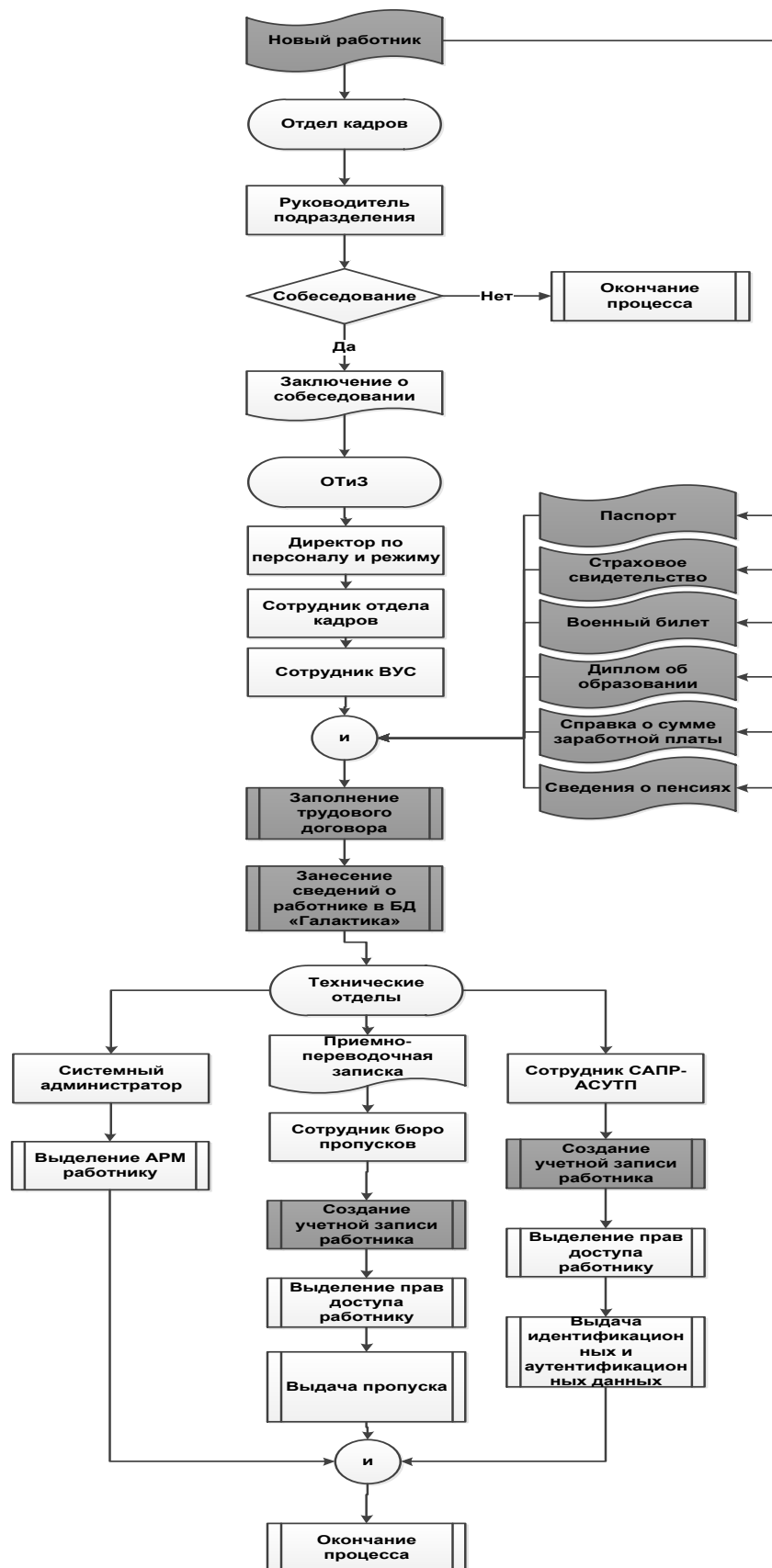


Рисунок 1 – Технологическая карта процесса приема сотрудника на работу

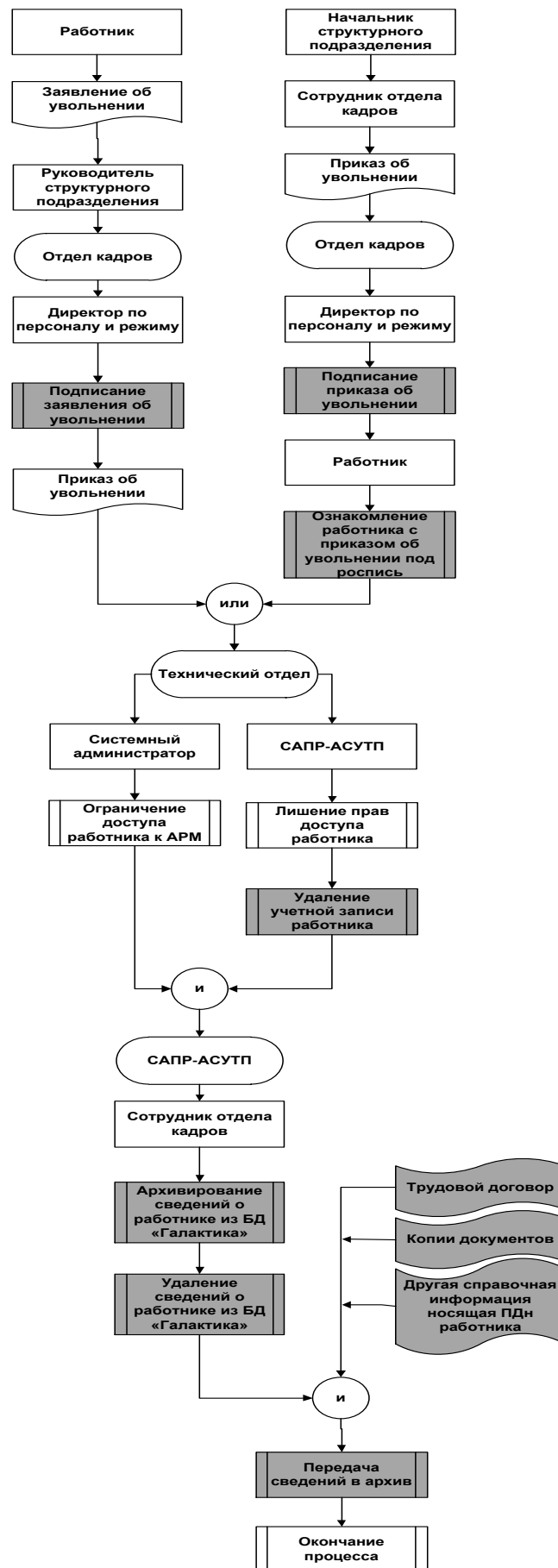


Рисунок 2 – Технологическая карта процесса увольнения работника

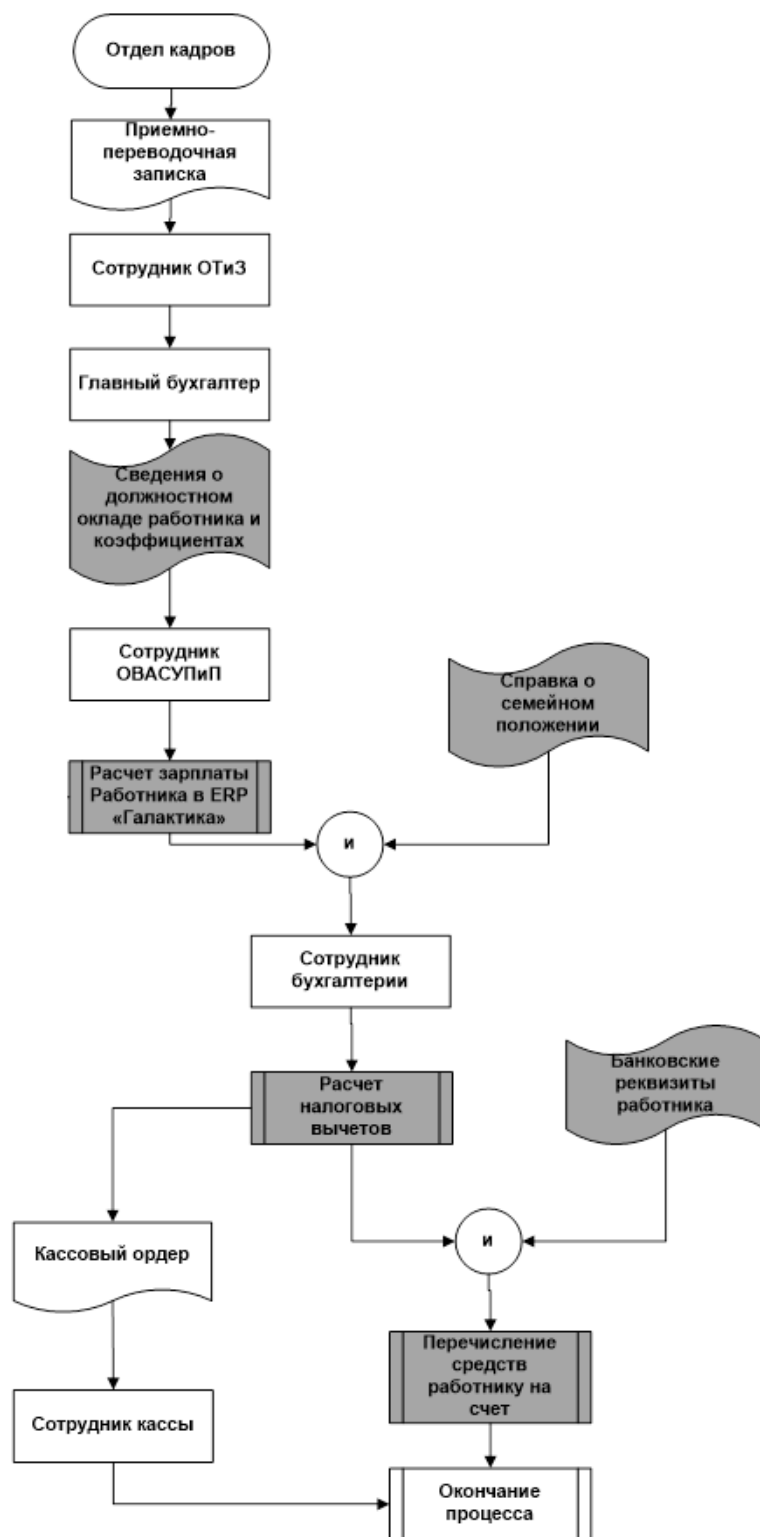


Рисунок 3 – Технологическая карта процесса начисления работнику
зарплаты

Общее описание технологических процессов обработки ПДн, включающее для каждой процедуры перечни входящих и исходящих документов, содержащих ПДн, и участников процедур, представлено в виде таблицы 2.

Таблица 2 – Общее описание технологических процессов обработки ПДн

Наименование процедуры	Входящие документы, содержащие ПДн	Исходящие документы, содержащие ПДн	Участники процедуры
Прием сотрудника на работу	<ul style="list-style-type: none"> - Паспорт - Диплом об образовании - Страховое свидетельство - Военный билет - Справка о сумме заработной платы - Трудовая книжка 	<ul style="list-style-type: none"> - Сведения в БД «Галактика» - Трудовой договор - Приемно-переводочная записка - Сведения об уникальном идентификаторе работника в ИСПДн 	<ul style="list-style-type: none"> - Руководитель подразделения - Системный администратор - Директор по персоналу и режиму - Сотрудник ВУС - Сотрудник САПР-АСУТП - Сотрудник отдела кадров - Сотрудник отдела пропусков
Начисление работнику зарплаты	<ul style="list-style-type: none"> - Трудовой договор - Сведения из БД работников - Справка о семейном положении - Банковские реквизиты работника 	<ul style="list-style-type: none"> - Кассовый ордер - Квитанция о начислении зарплаты 	<ul style="list-style-type: none"> - Главный бухгалтер - Сотрудник САПР-АСУТП - Сотрудник отдела кадров - Сотрудник ОТиЗ

Продолжение таблицы 2

Наименование процедуры	Входящие документы, содержащие ПДн	Исходящие документы, содержащие ПДн	Участники процедуры
Увольнение работника	<ul style="list-style-type: none"> - Приказ об увольнении - Копии документов работника - Трудовой договор - Трудовая книжка 	<ul style="list-style-type: none"> - Трудовая книжка - Приказ об увольнении - Расторгнутый трудовой договор - Копии документов 	<ul style="list-style-type: none"> - Директор по персоналу и режиму - Руководитель структурного подразделения - Системный администратор - Сотрудник отдела кадров - Сотрудник отдела САПР-АСУТП - Работник

Таким образом, в организации обрабатывается следующий перечень ПДн, представленный в таблице 3.

Таблица 3 – Перечень персональных данных, обрабатываемых в ИСПДн

Наименование ПДн	Цель обработки ПДн в рамках ИСПДн
<p>Первичные учетные данные:</p> <ul style="list-style-type: none"> – ФИО работника, год рождения; – серия и номер документа, удостоверяющего личность; – адрес места прописки; – телефон; – реквизиты документов об образовании; – сведения о воинском учете; – сведения о предыдущем месте работы. 	<p>Учет работников.</p> <p>Осуществление процессов согласно трудовому законодательству РФ.</p>
<p>Сведения о занимаемой должности:</p> <ul style="list-style-type: none"> – профессия, должность; – стаж работы. 	<p>Поддержание иерархии отношений между работниками.</p> <p>Осуществление процессов согласно трудовому законодательству РФ.</p>
<p>Финансовое состояние работника:</p> <ul style="list-style-type: none"> – ФИО работника, год рождения; – заработная плата работника. 	<p>Осуществление налоговых отчислений.</p> <p>Осуществление процессов согласно трудовому законодательству РФ.</p>

Продолжение таблицы 3

Наименование ПДн	Цель обработки ПДн в рамках ИСПДн
<p>Сведения о реквизитах работника:</p> <ul style="list-style-type: none"> – ИНН, номер свидетельства государственного пенсионного страхования; – сведения, необходимые для начисления заработной платы, произведения вычетов из заработной платы, для оформления бухгалтерской, налоговой и статистической отчетности (банковские реквизиты и т.п.). 	<p>Осуществление процессов согласно трудовому законодательству РФ.</p>
<p>Дополнительные сведения о работнике:</p> <ul style="list-style-type: none"> – сведения о рождении ребенка; – сведения о семейном положении. 	<p>Выплата льгот и иных надбавок.</p> <p>Осуществление процессов согласно трудовому законодательству.</p>

2.3 Описание структуры информационной системы персональных данных «Кадры» и идентификация технических средств обработки информации

Информационная структура предприятия представляет собой локально-вычислительную сеть. ЛВС предприятия логически разделена на два сегмента: общий, в котором функционируют СВТ, не входящие в ИСПДн, и сегмент ИСПДн, в котором функционируют объекты ИСПДн. Разделение осуществляется с использованием межсетевых экранов ViPNet Personal Firewall 4. В ИСПДн обеспечивается хранение, обработка и анализ информации о подразделениях и сотрудниках предприятия.

ИСПДн предназначена для решения задач управления персоналом. В состав ИСПДн предприятия входят 33 АРМ сотрудников, ERP система «Галактика» и контролер домена.

Хранение персональных данных осуществляется на сервере «Галактика» в отдельных БД «Зарплата» и «Кадры».

В ЛВС предприятия входят рабочие места системного администратора и администратора безопасности, которые подключены в общем сегменте. Рабочее место администратора безопасности предназначено для анализа защищенности операционных систем СВТ ИСПДн и прикладного программного обеспечения. Каждый из компьютеров, входящих в состав ИСПДн, является членом домена Active Directory. На контролере домена развернуты основные службы (DHCP, DNS, Active Directory).

В процессе обработки персональных данных в ИСПДн используются следующие технологии:

- персональные данные хранятся и обрабатываются в специально предназначенной для этого ERP системе «Галактика»;
- временное хранение ПДн в малых объемах возможно на АРМ сотрудников предприятия, входящих ИСПДн.

Схема конфигурации ИСПДн организации представлена на рисунке 4. Технические средства, используемые для обработки ПДн, представлены в таблице 4.

Подробные характеристики средств, используемых при обработке персональных данных, а также состав вспомогательных технических средств приведены в техническом паспорте на ИСПДн.

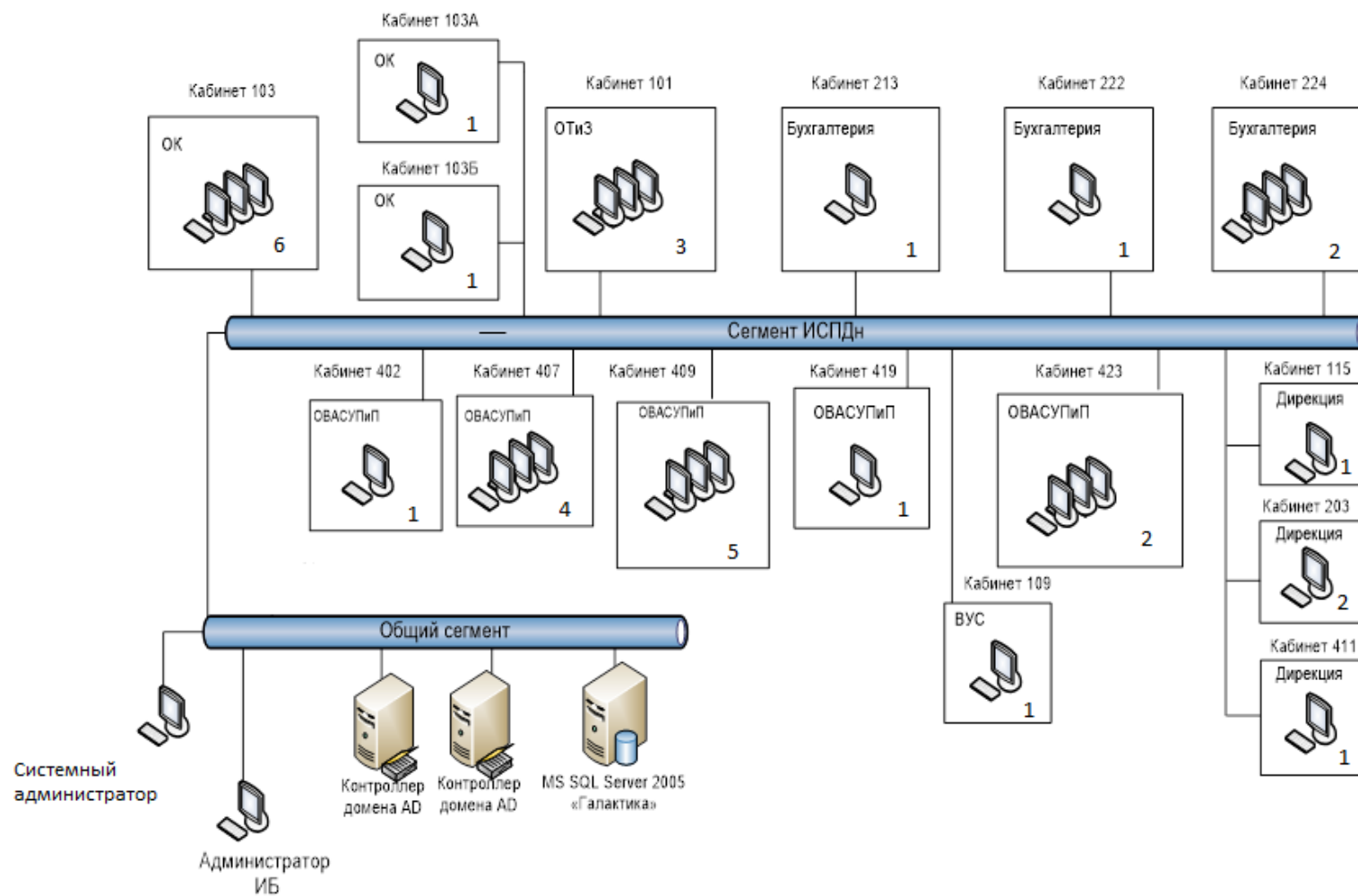


Рисунок 4 – Схема конфигурации ИСПДн

Таблица 4 – Перечень технических средств, используемых при обработке ПДн

Наименование	Программные характеристики	Установленные СЗИ	Кол-во, шт.
АРМ сотрудника предприятия	ОС Microsoft Windows 7 Pro SP1; Microsoft Office 2010	ViPNet Personal Firewall 4.	33
Сервер “Галактика”	ОС Microsoft Windows Server 2003 R2 EE(SP2); MS SQL Server 2008.	ERP система «Галактика 8.1»; Антивирус: Dr.Web для Windows версии 6.0; ViPNet Personal Firewall 4.	1

2.4 Описание существующих организационных и технических мер защиты

ИСПДн находится в пределах контролируемой зоны, на территории предприятия действует охранная сигнализация, двери оснащены замками, исключая возможность нахождения посторонних лиц в помещениях, где расположены элементы ИСПДн. При выходе из КЗ проводится проверка ручной клади. Сетевое оборудование находится в специальных комнатах, исключающих нахождение в них посторонних лиц, и телекоммуникационных шкафах.

Пользователи ИСПДн инструктируются о правилах работы с ПДн, а также о правилах работы в ЛВС. Персонал осведомлен о действиях в внештатных ситуациях.

Основной объем ПДн обрабатывается и хранится на сервере «Галактика», которая сертифицирована ФСТЭК по 4 уровню контроля отсутствия недекларированных возможностей. На АРМ установлены средства межсетевого экранирования ViPNet Personal Firewall 4 ФРКЕ 00125-01, имеющие Сертификат соответствия ФСБ России.

Установлены процедуры идентификации и аутентификации пользователей. Управление учетными записями пользователей и разграничение прав доступа в соответствии с принятой матрицей доступа реализуется штатными средствами ОС Windows.

В ИСПДн ведется учет машинных носителей информации, производится регистрация событий безопасности (вход в систему и выход из нее, попытки доступа, загрузка ОС, запуск и завершение программ, связанных с обработкой ПДн).

3 Оценка соответствия действующих в организации документов, регламентирующих обработку персональных данных

Классификация информационной системы персональных данных «Кадры» АО «Радиозавод» произведена на основании Постановления Правительства Российской Федерации от 17.11.2007 г. №781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», который в настоящее время утратил силу в связи с выходом ПП №1119. В виду этого вместо акта классификации в соответствии с действующим законодательством в организации должен быть определен уровень защищенности ИСПДн и составлен соответствующий акт определения уровня защищенности ИСПДн.

Частная модель угроз безопасности персональных данных в информационной системе персональных данных была разработана более 5 лет назад, и не актуализировалась на протяжении этого времени. По этой причине и на основании того, что была изменена структура ИСПДн и процесс обработки ПДн, было принято решение о пересмотре модели угроз в соответствии с рекомендованной методикой, описанной в методическом документе ФСТЭК России «Методика определения угроз безопасности информации в информационных системах».

Исходя из того, что в организации не выполняется даже базовый набор мер по обеспечению безопасности персональных данных, приведенный в приказе ФСТЭК России №21, было принято решение о реализации дополнительных мер в рамках системы защиты персональных данных. В связи с этим, а также с изменением структуры ИСПДн и процессом обработки ПДн необходима актуализация следующих документов:

- техническое задание на информационную систему;
- технический паспорт на информационную систему.

4 Разработка модели угроз персональных данных в информационной системе персональных данных

4.1 Разработка модели нарушителя

Результаты, полученные в ходе разработки модели нарушителя, включаются отдельным разделом в модель угроз безопасности информации.

В соответствии с проектом методического документа ФСТЭК России «Методика определения угроз безопасности информации в информационных системах» модель нарушителя должна содержать: типы, виды и потенциал нарушителей, способы реализации угроз, а также цели, которые преследует нарушитель при реализации угроз безопасности информации.[8]

Виды нарушителя, их тип, потенциал и возможные цели (мотивация) реализации угроз безопасности информации приведены в таблице 5.

Таблица 5 – Виды нарушителя и их возможные цели и потенциал

Вид нарушителя	Типы нарушителя	Возможные цели (мотивация) реализации угроз БИ	Потенциал нарушителей
Внешние субъекты (физические лица)	Внешний	Идеологические или политические мотивы. Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды	Низкий

Продолжение таблицы 5

Вид нарушителя	Типы нарушителя	Возможные цели (мотивация) реализации угроз БИ	Потенциал нарушителей
Лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора (администрация, охрана, уборщики и т.д.)	Внутренний	Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия	Низкий
Пользователи информационной системы	Внутренний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия	Низкий
Бывшие работники (пользователи)	Внешний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Месть за ранее совершенные действия	Низкий

Продолжение таблицы 5

Вид нарушителя	Типы нарушителя	Возможные цели (мотивация) реализации угроз БИ	Потенциал нарушителей
Администраторы информационной системы и администраторы безопасности	Внутренний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Мсть за ранее совершенные действия. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды. Непреднамеренные, неосторожные или неквалифицированные действия	Средний
Разработчики, производители, поставщики программных, технических и программно-технических средств	Внешний	Внедрение на этапе разработки в программные или технические средства дополнительных недекларированных возможностей. Причинение ущерба путем обмана или злоупотребления доверием	Средний

Администраторы ИС и администраторы безопасности выполняют функции по администрированию баз данных ИСПДн, поддерживают работоспособность систем в составе ИСПДн и обеспечивают их взаимодействие. Эти лица могут реализовывать угрозы информационной безопасности, используя свои привилегии для доступа к хранимой и обрабатываемой защищаемой информации, программным и техническим средствам, участвующим в обработке ПДн, а также к средствам защиты.

Администраторы ИС и администраторы безопасности осведомлены о протоколах и алгоритмах, используемых в ИСПДн и ее подсистемах, а также о концепции безопасности и используемых мерах защиты. Предполагается, что для реализации угроз или идентификации уязвимостей они могут использовать штатное оборудование, оборудование, полученное из внешних общедоступных источников (например, программное обеспечение), или специализированное оборудование.

К этим лицам, в связи с их ролью в ИСПДн, применяются особые меры, включающие тщательный подбор кандидата при принятии на работу и назначению на должность, а также контроль за выполнением своих обязанностей.

Предполагается, что назначаться на должности Администратора ИС и администратора безопасности будут только доверенные лица, поэтому они исключаются из числа вероятных нарушителей.

Потенциал нарушителей и их возможности были определены в соответствии с методическим документом ФСТЭК России «Методика определения угроз безопасности информации в информационных системах» и представлены в таблице 6.[7]

Предполагается, что нарушители имеют всю необходимую для реализации угроз информацию, кроме ключевой, парольной, аутентификационной и иной информации, доступ к которой исключается системой защиты.

Таблица 6 – Потенциал нарушителей и их возможности

Вид нарушителя	Потенциал нарушителя	Возможности по реализации УБИ
Пользователи информационной системы	Низкий	Имеют возможность получения из общедоступных источников информации об уязвимостях компонентов ИС, а также информации о средствах и способах реализации УБИ. Самостоятельно реализуют атаки на ИС.
Внешние субъекты (физические лица)	Низкий	
Бывшие работники (пользователи)	Низкий	
Лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора (администрация, охрана, уборщики и т.д.)	Низкий	
Разработчики, производители, поставщики программных, технических и программно-технических средств	Средний	Имеют все возможности нарушителей с низким потенциалом. Осведомлены о применяемых в ИС методах защиты информации. Имеют информацию о структурно-функциональных характеристиках ИС. Имеют возможность проведения анализа кода программного обеспечения с использованием общедоступных программных средств для получения информации об уязвимостях компонентов ИС.

Были определены возможные способы реализации угроз безопасности информации. Результат представлен в таблице 7.

Таблица 7 – Способы реализации угрозы

Нарушитель	Способ реализации угрозы
Внешние субъекты (физические лица)	несанкционированный физический доступ и (или) воздействие на линии, (каналы) связи, технические средства, машинные носители информации
Лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора (администрация, охрана, уборщики и т.д.)	несанкционированный физический доступ и (или) воздействие на линии, (каналы) связи, технические средства, машинные носители информации
	несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы)
Пользователи информационной системы	несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, web-приложения, иные прикладные программы общего и специального назначения)
	несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы)

Продолжение таблицы 7

Нарушитель	Способ реализации угрозы
Разработчики, производители, поставщики программных, технических и программно- технических средств	несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, web-приложения, иные прикладные программы общего и специального назначения)
	несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы)
	несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы)
Бывшие работники (пользователи)	воздействие на пользователей, администраторов безопасности, администраторов информационной системы или обслуживающий персонал (социальная инженерия)

Разработанная модель нарушителя включена в состав частной модели угроз безопасности персональных данных при их обработке в информационной системе персональных данных «Кадры» АО «Радиозавод», представленной в приложении Е.

4.2 Определение исходного уровня защищенности информационной системы персональных данных

Под общим уровнем защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн (Y_1), приведенных в таблице 8.

Таблица 8 – Показатели исходной защищенности ИСПДн

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
1. По территориальному размещению: локальная ИСПДн, развернутая в пределах одного здания	+	–	–
2. По наличию соединения с сетями общего пользования: ИСПДн, физически отделенная от сети общего пользования;	+	–	–
3. По встроенным (легальным) операциям с записями баз персональных данных: чтение, поиск, запись, удаление, сортировка, модификация, передача;	–	–	+
4. По разграничению доступа к персональным данным: ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн;	–	+	–
5. По наличию соединений с другими базами ПДн иных ИСПДн: ИСПДн, в которой используется одна база персональных данных, принадлежащая организации – владельцу данной ИСПДн;	+	–	–
6. По уровню обобщения (обезличивания) ПДн: ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта персональных данных)	–	–	+
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки: ИСПДн, не предоставляющая никакой информации.	+	–	–

В соответствии с методическим документом ФСТЭК России «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» для ИСПДн «Кадры» уровень исходной степени защищенности – средний, и числовой коэффициент исходного уровня защищенности $ИСПДн(Y_1) = 5$, так как более 70% характеристик ИСПДн соответствуют уровню не ниже «средний», а остальные низкому уровню защищенности. [6]

4.3 Определение вероятности реализации угроз

Под вероятностью реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для ИСПДн в складывающихся условиях обстановки. [6]

Числовой коэффициент (Y_2) для оценки вероятности возникновения угрозы определяется по 4 вербальным градациям этого показателя:

- маловероятно ($Y_2 = 0$);
- низкая вероятность ($Y_2 = 2$);
- средняя вероятность ($Y_2 = 5$);
- высокая вероятность ($Y_2 = 10$).

В ИСПДн при обработке ПДн выделяются следующие угрозы, представленные в таблице 9.

Угрозы и их описание взяты из следующих документов:

- методические рекомендации по составлению Частной модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных учреждений здравоохранения, социальной сферы, труда и занятости [9];
- базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных.[1]

Таблица 9 – Угрозы безопасности информации

Наименование угрозы	Описание угрозы	Вероятность реализации	Y ₂
Угрозы утечки информации по техническим каналам			
Угроза утечки акустической информации	<p>Возникновение угроз утечки речевой информации при обработке ПДн возможно только при наличии функций и средств воспроизведения ПДн или при голосовом вводе ПДн в ИСПДн.</p> <p>В ИСПДн «Кадры» функции акустического воспроизведения ПДн и функции голосового ввода отсутствуют.</p>	Маловероятная	0
Угроза утечки видовой информации	<p>Угроза реализуется за счет просмотра информации с использованием оптических и оптико-электронных средств с экранов дисплеев и других средств отображения информации, входящих в состав ИСПДн.</p> <p>В помещениях, где функционируют элементы ИСПДн, исключено нахождение посторонних лиц. Все элементы ИСПДн находятся в пределах КЗ на большой удаленности от ее границ.</p>	Низкая	2

Продолжение таблицы 9

Наименование угрозы	Описание угрозы	Вероятность реализации	Y2
Угроза утечки информации по каналам ПЭМИН	<p>Угроза возникает из-за наличия паразитных электромагнитных излучений технических средств ИСПДн.</p> <p>Отопительная система, линии телефонной связи, АТС и электрическая подстанция и другие коммуникации, по которым возможно утечка ПДн по каналам ПЭМИН, находятся в контролируемой зоне.</p>	Маловероятна	0
Угрозы уничтожения, хищения аппаратных средств ИСПДн, носителей информации путем физического доступа к элементам системы			
Кража ПЭВМ	<p>Угроза осуществляется путем несанкционированного доступа нарушителями в помещения, где расположены элементы ИСПДн.</p> <p>На территории предприятия осуществляется контроль доступа в КЗ, ведется видеонаблюдение, на выходе из КЗ проводится проверка ручной кладки.</p>	Маловероятная	0

Продолжение таблицы 9

Наименование угрозы	Описание угрозы	Вероятность реализации	У2
Кража ключей и атрибутов доступа	<p>Угроза реализуется путем несанкционированного доступа нарушителями в помещения, где расположены рабочие места пользователей.</p> <p>На предприятии осуществляется контроль доступа в КЗ, двери закрываются на замок, на территории установлена охранная сигнализация.</p>	низкая	2
Вывод из строя узлов ПЭВМ	<p>Угроза реализуется путем несанкционированного доступа нарушителями в помещения, где расположены технические средства ИСПДн, и доступа к каналам связи.</p> <p>На предприятии осуществляется контроль доступа в КЗ, двери закрываются на замок, на территории установлена охранная. Сетевое оборудование находится в специальных комнатах, исключаяющих нахождение в них посторонних лиц, и телекоммуникационных шкафах.</p>	Низкая	2

Продолжение таблицы 9

Наименование угрозы	Описание угрозы	Вероятность реализации	Y2
Кража носителей информации	<p>Угроза реализуется путем несанкционированного доступа нарушителей к носителям информации.</p> <p>На предприятии осуществляется контроль доступа в КЗ, двери закрываются на замок, на территории установлена охранный, на выходе из КЗ проводится проверка ручной клади.</p>	Маловероятная	0
Кража, модификация, уничтожение информации	<p>Угроза реализуется путем несанкционированного доступа нарушителями в помещения, где расположены рабочие места пользователей, а также располагаются технические средства и средства защиты ИСПДн.</p> <p>На предприятии осуществляется контроль доступа в КЗ, двери закрываются на замок, на территории установлена охранный сигнализация.</p>	Маловероятная	0

Продолжение таблицы 9

Наименование угрозы	Описание угрозы	Вероятность реализации	Y2
Несанкционированное отключение средств защиты	<p>Угроза реализуется путем несанкционированного доступа нарушителями в помещения, в которых расположены средства защиты ИСПДн.</p> <p>На предприятии осуществляется контроль доступа, двери закрываются на замок. В случае отключения средств защиты поступает тревожный сигнал.</p>	Маловероятная	0
<p>Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера</p>			
Непреднамеренная модификация (уничтожение) информации сотрудниками	<p>Угроза реализуется за счет человеческого фактора путем нарушения пользователями ИСПДн принятых правил работы с ПДн.</p> <p>На предприятии проводятся инструктажи по работе с ПДн.</p> <p>Производится резервное копирование ПДн.</p>	Низкая	2

Продолжение таблицы 9

Наименование угрозы	Описание угрозы	Вероятность реализации	Y2
Выход из строя аппаратно-программных средств	<p>Угроза реализуется из-за несовершенства аппаратных и программных средств, вследствие которого возможно нарушение доступности или целостности информации.</p> <p>На предприятии осуществляется резервирование основных аппаратно-программных средств ИСПДн.</p>	Низкая	2
Утрата ключей и атрибутов доступа	<p>Угроза реализуется за счет человеческого фактора путем нарушения пользователями ИСПДн положений парольной политики (создание легких паролей, компрометация паролей, передача третьим лицам).</p> <p>На предприятии осуществляется контроль доступа в КЗ, двери закрываются на замок, в помещениях, где расположены рабочие места, исключено пребывание посторонних лиц.</p>	Низкая	2
Стихийное бедствие	<p>Угроза реализуется из-за несоблюдения мер пожарной безопасности.</p> <p>На предприятии установлена пожарная сигнализация. Персонал проинструктирован о действиях в штатных ситуациях.</p>	Маловероятная	0

Продолжение таблицы 9

Наименование угрозы	Описание угрозы	Вероятность реализации	У2
Непреднамеренное отключение средств защиты	<p>Угроза реализуется за счет человеческого фактора, путем нарушения пользователями правил работы в ИСПДн и правил работы с средствами защиты.</p> <p>На предприятии осуществляется контроль доступа в КЗ.</p> <p>Пользователи инструктируются о правилах работы с ИСПДн. Существует разграничение прав доступа к настройкам средств защиты.</p>	Низкая	2
Сбой системы электроснабжения	<p>Угроза реализуется из-за несовершенства системы электроснабжения, что может привести к нарушению доступности или целостности информации.</p> <p>Осуществляется резервное копирование информации. К основным техническим средствам ИСПДн подключены источники бесперебойного питания</p>	Низкая	2

Продолжение таблицы 9

Наименование угрозы	Описание угрозы	Вероятность реализации	Y2
Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)			
Установка ПО, не связанного с исполнением служебных обязанностей	Угроза реализуется внутренним нарушителем путем установки ПО, не связанного с исполнением им служебных обязанностей, что может привести к нарушению конфиденциальности, целостности и доступности информации, а также нарушению работы технических средств ИСПДн.	Высокая	10
Недекларированные возможности системного ПО и ПО для обработки персональных данных	Угроза реализуется путем использования недекларированных функциональных возможностей СВТ, не описанных в документации, вследствие чего нарушаются свойства информации. В ИСПДн основной объем ПДн обрабатывается и хранится на сервере «Галактика», которая сертифицирована ФСТЭК по 4 уровню контроля отсутствия недекларированных возможностей.	Маловероятная	0

Продолжение таблицы 9

Наименование угрозы	Описание угрозы	Вероятность реализации	У2
Угроза внедрения вредоносных программ (вирусов)	Угроза реализуется с использованием вредоносных программ, которые могут разрушать код программ в оперативной памяти, самодублироваться, выполнять без участия пользователя деструктивные функции, искажать, дублировать, блокировать информацию.	Высокая	10
Угроза внедрения в ИСПДн аппаратных закладок	<p>Угроза осуществляется путем внедрения в технические средства ИСПДн аппаратных закладок, вследствие чего появляется возможность нештатно вмешиваться в работу системы.</p> <p>На предприятии осуществляется контроль доступа в КЗ, двери закрываются на замок, на территории установлена охранная. Сетевое оборудование находится в специальных комнатах, исключающих нахождение в них посторонних лиц, и телекоммуникационных шкафах.</p> <p>При приобретении и установке средств обработки информации проводится осмотр комплектующих на соответствие техническому паспорту изделия.</p>	Маловероятная	0

Продолжение таблицы 9

Наименование угрозы	Описание угрозы	Вероятность реализации	Y2
Угрозы преднамеренных действий внутренних нарушителей			
Угроза перехвата управления загрузкой	Угроза реализуется внутренним нарушителем путем перехвата управления загрузкой для загрузки ОС с отчуждаемых носителей для получения НСД к ИСПДн.	Средняя	5
Доступ к информации, модификация, уничтожение лиц, не допущенных к ее обработке	Угроза реализуется путем несанкционированного доступа нарушителей в помещения, где расположены технические средства обработки ПДн. На предприятии осуществляется контроль доступа в КЗ, установлено видеонаблюдение, двери закрываются на замок.	Низкая	2
Утечка информации через порты ввода/вывода	Угроза реализуется внутренними нарушителями путем несанкционированного копирования информации на подключенные к компьютерам съемные носители информации.	Высокая	10

Продолжение таблицы 9

Наименование угрозы	Описание угрозы	Вероятность реализации	Y2
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	Угроза реализуется за счет человеческого фактора путем несанкционированных действий пользователями ИСПДн, направленных на разглашение, модификацию и уничтожение информации.	Средняя	5
Угрозы, реализуемые после загрузки операционной системы	Угрозы направлены на НСД к информации. Осуществляются с использованием стандартных функций ОС (копирование, уничтожение, форматирование).	Средняя	5

Продолжение таблицы 9

Наименование угрозы	Описание угрозы	Вероятность реализации	У2
Угрозы несанкционированного доступа по каналам связи			
Угрозы внедрения по сети вредоносных программ	<p>Угроза реализуется путем удаленной установки на компьютеры вредоносного ПО с целью нарушения конфиденциальности, целостности и доступности информации.</p> <p>На всех компьютерах, входящих в состав ИСПДн, установлены средства межсетевого экранирования. Доступ к сетям международного информационного обмена отсутствует.</p>	Маловероятна	0
Угрозы удаленного запуска приложений	<p>Угроза осуществляется путем запуска на хосте ИСПДн внедренных вредоносных программ, целью которого является нарушение целостности, доступности и конфиденциальности информации, а также контроль работы хоста.</p> <p>На всех компьютерах, входящих в состав ИСПДн, установлены средства межсетевого экранирования. Доступ к сетям международного информационного обмена отсутствует.</p>	Маловероятная	0

Продолжение таблицы 9

Наименование угрозы	Описание угрозы	Вероятность реализации	Y2
Угроза выявления паролей	<p>Угроза осуществляется путем преодоления парольной защиты и получения НСД. Преодоление парольной защиты может осуществляться с помощью перебора паролей, перехвата паролей.</p> <p>На всех компьютерах, входящих в состав ИСПДн, установлены средства межсетевого экранирования. Доступ к сетям международного информационного обмена отсутствует.</p>	Маловероятная	0
Угрозы «Анализа сетевого трафика» с перехватом передаваемой по сети информации	<p>Угроза осуществляется с использованием анализатора пакетов (sniffer), который перехватывает передаваемые по сети пакеты, выделяя из них те, в которых передаются идентификатор и пароль пользователя.</p> <p>На всех компьютерах, входящих в состав ИСПДн, установлены средства межсетевого экранирования. Доступ к сетям международного информационного обмена отсутствует.</p>	Низкая	2

4.4 Определение реализуемости угроз и оценка опасности угроз

По итогам оценки уровня защищенности (Y_1) и вероятности реализации угрозы (Y_2), рассчитывается коэффициент реализуемости угрозы (Y) и определяется возможность реализации угрозы. Коэффициент реализуемости угрозы Y определяется соотношением $Y = (Y_1 + Y_2)/20$. [6]

Возможность реализации угрозы считается:

- низкой, если коэффициент реализуемости меньше 0,3;
- средней, если коэффициент реализуемости лежит в пределах от 0,3 до 0,6;
- высокой, если коэффициент реализуемости лежит в пределах от 0,6 до 0,8;
- очень высокой, если коэффициент реализуемости больше 0,8.

Оценка опасности угроз безопасности определяется путем опроса специалистов в области защиты информации и имеет три значения:

- низкая опасность – в случае, когда при реализации угрозы для субъектов ПДн наступают незначительные негативные последствия;
- средняя опасность - в случае, когда при реализации угрозы для субъектов ПДн наступают негативные последствия;
- высокая опасность - в случае, когда при реализации угрозы для субъектов ПДн наступают значительные негативные последствия.

Оценка реализуемости УБПДн представлена в таблице 10.

Таблица 10 – Реализуемость угроз безопасности персональных данных

Тип угроз безопасности ПДн	Коэффициент реализуемости угрозы (Y)	Возможность реализации	Опасность угрозы
Угрозы от утечки по техническим каналам			
Угрозы утечки акустической информации;	0,25	низкая	низкая

Продолжение таблицы 10

Тип угроз безопасности ПДн	Коэффициент реализуемости угрозы (Y)	Возможность реализации	Опасность угрозы
Угрозы утечки видовой информации;	0,35	средняя	низкая
Угрозы утечки информации по каналам ПЭМИН;	0,25	низкая	низкая
Угрозы несанкционированного доступа к информации.			
Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн			
Кража ПЭВМ;	0,25	низкая	средняя
Кража носителей информации;	0,25	низкая	средняя
Кража ключей и атрибутов доступа;	0,25	низкая	низкая
Кражи, модификации, уничтожения информации;	0,25	низкая	средняя
Вывод из строя узлов ПЭВМ, каналов связи;	0,35	средняя	низкая
Несанкционированное отключение средств защиты;	0,25	низкая	средняя
Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).			
Угроза внедрения вредоносных программ (вирусов);	0,75	высокая	высокая

Продолжение таблицы 10

Тип угроз безопасности ПДн	Коэффициент реализуемости угрозы (Y)	Возможность реализации	Опасность угрозы
Установка ПО не связанного с исполнением служебных обязанностей;	0,75	высокая	средняя
Недекларированные возможности системного ПО и ПО для обработки персональных данных;	0,25	низкая	низкая
Угроза внедрения в ИСПДн аппаратных закладок;	0,25	низкая	средняя
Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.			
Утрата ключей и атрибутов доступа;	0,25	низкая	низкая
Непреднамеренная модификация (уничтожение) информации сотрудниками;	0,35	средняя	низкая
Непреднамеренное отключение средств защиты;	0,35	средняя	низкая
Выход из строя аппаратно-программных средств;	0,35	средняя	низкая
Сбой системы электроснабжения;	0,25	низкая	низкая

Продолжение таблицы 10

Тип угроз безопасности ПДн	Коэффициент реализуемости угрозы (Y)	Возможность реализации	Опасность угрозы
Стихийное бедствие;	0,25	низкая	низкая
Угрозы преднамеренных действий внутренних нарушителей			
Утечка информации через порты ввода/вывода;	0,75	высокая	средняя
Угроза перехвата управления загрузкой	0,5	средняя	средняя
Угрозы, реализуемые после загрузки операционной системы;	0,25	низкая	средняя
Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке;	0,35	средняя	высокая
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке;	0,5	средняя	высокая
Угрозы несанкционированного доступа по каналам связи.			
Угрозы «Анализа сетевого трафика» с перехватом передаваемой по сети информации;	0,35	средняя	низкая
Угрозы выявления паролей по сети;	0,25	низкая	средняя

Продолжение таблицы 10

Тип угроз безопасности ПДн	Коэффициент реализуемости угрозы (Y)	Возможность реализации	Опасность угрозы
Угрозы удаленного запуска приложений;	0,25	низкая	средняя
Угрозы внедрения по сети вредоносных программ;	0,25	низкая	средняя

4.5 Определение актуальности угроз в информационной системе персональных данных

Из всех определенных ранее угроз безопасности были определены актуальные в соответствии с правилами отнесения УБПДн к актуальной, представленными в таблице 11.

Таблица 11 – Правила определения актуальности УБПДн

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

Оценка актуальности УБПДн на основании вышеприведенной таблицы представлена в таблице 12.

Таблица 12 – Актуальность угроз безопасности

Тип угроз безопасности ПДн	Актуальность угрозы
Угрозы от утечки по техническим каналам	
Угрозы утечки акустической информации	неактуальна
Угрозы утечки видовой информации	неактуальна
Угрозы утечки информации по каналам ПЭМИН	неактуальна

Продолжение таблицы 12

Тип угроз безопасности ПДн	Актуальность угрозы
Угрозы несанкционированного доступа к информации	
Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн	
Кража ПЭВМ	неактуальна
Кража носителей информации	неактуальна
Кража ключей и атрибутов доступа	неактуальна
Кражи, модификации, уничтожения информации	неактуальна
Вывод из строя узлов ПЭВМ, каналов связи	неактуальна
Несанкционированное отключение средств защиты	неактуальна
Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).	
Угроза внедрения вредоносных программ (вирусов)	актуальна
Установка ПО, не связанного с исполнением служебных обязанностей	актуальна
Недекларированные возможности системного ПО и ПО для обработки персональных данных.	неактуальна
Угроза внедрения в ИСПДн аппаратных закладок	неактуальна
Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.	
Утрата ключей и атрибутов доступа	неактуальна

Продолжение таблицы 12

Тип угроз безопасности ПДн	Актуальность угрозы
Непреднамеренная модификация (уничтожение) информации сотрудниками	неактуальна
Непреднамеренное отключение средств защиты	неактуальна
Выход из строя аппаратно-программных средств	неактуальна
Сбой системы электроснабжения	неактуальна
Стихийное бедствие	неактуальна
Угрозы преднамеренных действий внутренних нарушителей	
Утечка информации через порты ввода/вывода	актуальна
Угроза перехвата управления загрузкой	актуальна
Угрозы, реализуемые после загрузки операционной системы	неактуальна
Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке	неактуальна
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	актуальна
Угрозы несанкционированного доступа по каналам связи.	
Угрозы «Анализа сетевого трафика» с перехватом передаваемой по сети информации;	неактуальна
Угрозы выявления паролей по сети	неактуальна
Угрозы удаленного запуска приложений	неактуальна
Угрозы внедрения по сети вредоносных программ	неактуальна

5 Определение уровня защищенности информационной системы персональных данных организации

На основании рассмотрения циркулирующих в ИСПДн персональных данных был определен тип ИСПДн «Кадры».

ИСПДн «Кадры» является ИС, обрабатывающей иные ПДн. В информационной системе обрабатываются только ПДн сотрудников организации.

Актуальными считаются угрозы 3-го типа, не связанные с наличием недекларированных возможностей в прикладном и системном ПО, которое используется в ИСПДн.[2]

Во исполнение требований Постановления Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных», был определен уровень защищенности.

Руководствуясь типом ИСПДн, категорией субъектов ПДн, количеством субъектов, чьи ПДн обрабатываются в ИСПДн и типом актуальных угроз, в соответствии с таблицей 13 был определен уровень защищенности ИСПДн «Кадры».

Таблица 13 – Определение уровня защищенности ИСПДн

Тип ИСПДн	Категории субъектов ПДн	Количество субъектов ПДн	Тип актуальных угроз		
			1 тип	2 тип	3 тип
ИСПДн - С	не сотрудники	более 100 000	У31	У31	У32
		менее 100 000	У31	У32	У33
	сотрудники	любое	У31	У32	У33
ИСПДн - Б	не сотрудники	более 100 000	У31	У32	У33
		менее 100 000	У31	У32	У33
	сотрудники	любое	У31	У32	У33

Продолжение таблицы 13

Тип ИСПДн	Категории субъектов ПДн	Количество субъектов ПДн	Тип актуальных угроз		
			1 тип	2 тип	3 тип
ИСПДн - И	не сотрудники	более 100 000	У31	У32	У33
		менее 100 000	У31	У33	У33
	сотрудники	любое	У31	У33	У34
ИСПДн - О	не сотрудники	более 100 000	У32	У32	У34
		менее 100 000	У32	У33	У34
	сотрудники	любое	У32	У33	У34

Уровень защищенности ИСПДн «Кадры» - У34.

Акт определения уровня защищенности информационной системы персональных данных «Кадры» АО «Радиозавод» представлен в приложении Б.

6 Определение организационных и организационно-технических требований к обеспечению уровней защищенности персональных данных в информационных системах персональных данных организации и выбор мер по обеспечению безопасности персональных данных

На основании Постановления Правительства Российской Федерации от 01.11.2012 №1119 сформулированы требования к обеспечению определенного уровня защищенности ПДн.

Для ИСПДн «Кадры» необходимо обеспечение четвертого уровня защищенности персональных данных при их обработке. Согласно Постановлению Правительства Российской Федерации от 01.11.2012 №1119 необходимо выполнение следующих требований [2]:

- организация режима обеспечения безопасности помещений, где размещена ИС, исключающая проникновение или несанкционированное пребывание в этих помещениях лиц, которые не имеют права доступа к ним;
- обеспечение сохранности носителей ПДн;
- утверждение документа, который определяет перечень лиц, доступ которых к ПДн, обрабатываемым в ИС, необходим для выполнения ими служебных обязанностей;
- использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства РФ в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.[2]

ИСПДн «Кадры» находится в пределах контролируемой зоны, и помещения, где размещены элементы ИСПДн, оснащены дверьми с кодовыми замками и охранной сигнализацией, что исключает нахождение лиц, не имеющих права доступа в помещения, в этих помещениях и доступ посторонних лиц к носителям ПДн. В организации существует утвержденный руководителем документ, определяющий перечень лиц,

доступ которых к ПДн, обрабатываемым в ИСПДн, необходим для выполнения ими служебных обязанностей. Средства защиты информации, встроенные в ERP систему «Галактика», имеют сертификат соответствия ФСТЭК и классифицированы по четвертому уровню контроля недекларируемых возможностей.

Таким образом, в организации выполнены все вышеуказанные требования и ИСПДн «Кадры» соответствует требованиям ПП РФ от 01.11.2012 №1119 « Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

На основе Приказа ФСТЭК от 18.02.2013 №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» был сформирован состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных для четвертого уровня защищенности персональных данных.[3]

Выбор мер по обеспечению безопасности персональных данных, подлежащих реализации в информационной системе в рамках системы защиты персональных данных, включает:

- определение базового набора мер;
- адаптацию базового набора;
- уточнение адаптированного базового набора;
- дополнение уточненного адаптированного базового набора.

Для предотвращения угроз безопасности информации должен быть реализован следующий базовый набор мер по обеспечению безопасности персональных данных для 4-го уровня защищенности персональных данных: ИАФ.1, ИАФ.3, ИАФ.4, ИАФ.5, ИАФ.6, УПД.1, УПД.2, УПД.3, УПД.4, УПД.5, УПД.6, УПД.13, УПД.14, УПД.15, УПД.16, ОПС.3, ЗНИ.1, ЗНИ.2,

ЗНИ.8, РСБ.1, РСБ.2, РСБ.3, РСБ.7, АВЗ.1, АВЗ.2, АНЗ.2, ЗТС.2, ЗТС.3, ЗТС.4, ЗИС.3, ЗИС.20.

В процессе адаптации и уточнения базового набора мер были исключены меры, непосредственно связанные с информационными технологиями, не используемыми в ИСПДн, или структурно-функциональными характеристиками, не свойственными информационной системе, и выбраны лишь те меры, которые направлены на нейтрализацию актуальных угроз безопасности ПДн для ИСПДн «Кадры» АО «Радиозавод». Обоснование представлено в виде таблицы 14.

Таблица 14 — Адаптация и уточнение мер по обеспечению безопасности ПДн в ИСПДн «Сотрудники»

Мера по обеспечению безопасности ПДн	Адаптация	Уточнение	Обоснование
ИАФ.6 Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	+		Исключена из набора мер в связи с отсутствием внешних пользователей, не являющихся работниками оператора
УПД.13 Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	+		Исключена из набора мер, так как в ИС отсутствует возможность удаленного доступа и доступ через внешние информационно-телекоммуникационные сети
УПД.14 Регламентация и контроль использования в информационной системе технологий беспроводного доступа	+		Исключена из набора мер в связи с отсутствием технологий беспроводного доступа в организации

Продолжение таблицы 14

Мера по обеспечению безопасности ПДн	Адаптация	Уточнение	Обоснование
УПД.15 Регламентация и контроль использования в информационной системе мобильных технических средств	+		Исключена из набора мер, так как в ИС отсутствуют мобильные технические средства
УПД.16 Управление взаимодействием с информационными системами сторонних организаций (внешние ИС)	+		Исключена из набора мер в связи с отсутствием взаимодействия организации с ИС сторонних организаций
АНЗ.2 Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	+		Исключена из набора мер, так как не подходит для блокировки (нейтрализации) актуальных угроз безопасности информации
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	+		Исключена из набора мер, так как персональные данные не передаются по каналам связи, имеющие выход за пределы контролируемой зоны

Продолжение таблицы 14

Мера по обеспечению безопасности ПДн	Адаптация	Уточнение	Обоснование
ЗИС.20 Защита беспроводных соединений, применяемых в информационной системе	+		Исключена из набора мер в связи с отсутствием беспроводных соединений в организации
ЗНИ.7 Контроль подключения машинных носителей информации		+	Добавлена в связи с актуальностью угроз, связанных с несанкционированным подключением внешних носителей информации
УПД.7 Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры защиты информации, и о необходимости соблюдения им установленных оператором правил обработки информации		+	Добавлена в связи с актуальностью угрозы, реализуемой внутренним нарушителем, связанной с человеческим фактором

В результате адаптации и уточнения базового набора мер был получен следующий набор мер, подлежащий реализации в ИСПДн в рамках системы защиты персональных данных, описание которого представлено в таблице 15.

Так как модель угроз была разработана на этапе эксплуатации системы, часть базового набора защитных мер уже была реализована в рамках существующей СЗПДн. Знаком «+» в таблице 15 отмечены уже

реализованные меры по обеспечению безопасности ПДн, знаком «-» - подлежащие реализации.

Таблица 15 –Содержание выбранных мер защиты информации

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Наличие в ИСПДн
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)		
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+
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	+
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	+

Продолжение таблицы 15

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Наличие в ИСПДн
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 защиты информации, и о необходимости соблюдения им установленных оператором правил обработки информации	-
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу	+

Продолжение таблицы 15

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Наличие в ИСПДн
III. Ограничение программной среды (ОПС)		
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов	-
IV. Защита машинных носителей информации (ЗНИ)		
ЗНИ.1	Учет машинных носителей информации	+
ЗНИ.2	Управление доступом к машинным носителям	+
ЗНИ.7	Контроль подключения машинных носителей информации	-
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)	+
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.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)	-

Продолжение таблицы 15

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Наличие в ИСПДн
XII. Защита технических средств (ЗТС)		
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 и помещения и сооружения, в которых они установлены	+
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	+

Соответствие каждой актуальной угрозы и защитных мер, направленных на нейтрализацию этих угроз, представлено в таблице 16.

Таблица 16 – Сопоставление защитных мер для устранения каждой актуальной угрозы для ИСПДн

Наименование угрозы	Перечень защитных мер для её устранения
Утечка информации через порты ввода/вывода	ЗНИ.7, РСБ.3
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	УПД.7
Установка ПО, не связанного с исполнением служебных обязанностей	ОПС.3, ЗНИ.7
Угрозы внедрения вредоносных программ	АВЗ.1, АВЗ.2, ЗНИ.7
Угроза перехвата управления загрузкой	ЗНИ.7

7 Выбор средств защиты для актуальных угроз безопасности информации

В целом средства защиты информации можно разделить на несколько групп:

- технические средства;
- программные средства;
- организационные средства.

Технические средства защиты информации включают в себя различные механические, электронные и другие устройства, которые препятствуют доступу к информации.

Программные средства защиты включают в себя программы, реализующие идентификацию и аутентификацию пользователей, разграничение прав доступа, антивирусную защиту и др.

Организационные средства защиты включают в себя организационно-правовые средства (правила работы, устанавливаемые на предприятии) и организационно-технические (безопасность помещений, организация доступа на территорию и пропускных пунктов, размещение сетевого оборудования, прокладка кабельной системы и др.).

Для актуальных угроз безопасности были выбраны средства защиты информации, подлежащие реализации в ИСПДн «Кадры» АО «Радиозавод», представленные в таблице 17.

Таблица 17 – Выбор средств защиты для каждой актуальной угрозы

Наименование угрозы	Средства защиты		
	Технические	Программные	Организационные
Утечка информации через порты ввода/вывода	—	Средство контроля подключения съемных машинных носителей информации DeviceLock 8 DLP Suite.	—
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	—	—	Инструкция пользователя. Подписание договоров о неразглашении.
Установка ПО, не связанного с исполнением служебных обязанностей	—	Изолирование портов ввода/вывода с использованием DeviceLock 8 DLP Suite.	Инструкция пользователя. Инструкция администратора ИБ.

Продолжение таблицы 17

Наименование угрозы	Средства защиты		
	Технические	Программные	Организационные
Угрозы внедрения вредоносных программ	—	Установка средств антивирусной защиты Dr.Web версия 6.00.3 и обеспечение их централизованного обновления. Средство контроля подключения съемных машинных носителей информации DeviceLock DeviceLock 8 DLP Suite.	Инструкция пользователя.
Угроза перехвата управления загрузкой	—	Средство контроля подключения съемных машинных носителей информации DeviceLock DeviceLock 8 DLP Suite.	Установка пароля на BIOS.

8 Разработка и актуализация документации, регламентирующей обработку персональных данных

На основе карт технологических процессов, был разработан документ – «Описание технологических процессов в информационной системе персональных данных «Кадры» АО «Радиозавод»». Документ представлен в приложении А.

Акт определения уровня защищенности информационной системы персональных данных «Кадры» АО «Радиозавод» разработан на основании Постановления Правительства РФ от 01.11.2012 N 1119 и представлен в приложении Б.

Был актуализирован технический паспорт на информационную систему персональных данных «Кадры» АО «Радиозавод» в соответствии с измененными структурой ИСПД, техническими средствами, а также с реализованными средствами защиты. Документ представлен в приложении В.

Было разработано положение об обработке и защите персональных данных АО «Радиозавод», определяющее порядок и условия обработки ПДн работников АО «Радиозавод». Документ представлен в приложении Г.

В соответствии с принятыми мерами защиты и изменением подсистем системы защиты информации был актуализирован документ «Техническое задание на информационную систему персональных данных «Кадры» предприятия АО «Радиозавод»», представленный в приложении Д.

Был разработан документ «Частная модель угроз безопасности персональных данных в информационной системе персональных данных «Кадры» АО «Радиозавод»», представленный в приложении Е.

В целях определения основных функций, прав и обязанности администратора ИБ при эксплуатации и сопровождении ИСПДн был разработан документ «Инструкция администратора информационной безопасности информационной системы персональных данных», которым

должен руководствоваться администратор информационной безопасности при выполнении своих трудовых обязанностей. Документ представлен в приложении Ж.

В целях организации защиты информации при обработке персональных данных был разработан документ «Инструкция пользователя информационной системы персональных данных на предприятии АО «Радиозавод»», регламентирующих обязанности сотрудников, участвующих в процессе обработки персональных данных. Документ представлен в приложении И.

В целях регламентации проведения внутреннего контроля соответствия обработки персональных данных установленным требованиям был разработан документ «Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в АО «Радиозавод»», представленный в приложении К.

9 Вредные психофизиологические факторы, влияющие на органы зрения специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие

К основным психофизиологическим факторам, влияющим на органы зрения пользователей, работающих с персональными компьютерами, относятся:

- напряжение зрения;
- напряжение внимания;
- монотонность труда;
- длительно статистическое напряжение.

Человеческий глаз мгновенно реагирует на самую мелкую вибрацию текста, и тем более на мерцание текста на экране. Мышцы глаза пребывают в постоянном напряжении, что отрицательно сказывается на зрении и приводит к ухудшению остроты зрения.

Работа, связанная с использованием ПК, сопровождается напряжением функций зрительного анализатора. Основной причиной этого служит иной принцип чтения информации, отличный от способа чтения информации с бумажного носителя. При чтении текста с листа бумаги, лист располагается на столе, свет на него падает под углом, и текст считывается работником с наклоном головы. При считывании текста с экрана монитора работник не наклоняет голову, глаза смотрят вперед, и пользователь смотрит прямо на источник света (текст на экране монитора), что приводит к работе органа зрения в стрессовом режиме. Непрерывная длительная работа пользователя с ПК неизбежно приводит к ухудшению зрения, утомлению, глаза начинают слезиться.

Также отрицательно влияет на зрение неудачный подбор шрифтов, цвета, некачественный дисплей, недостаточная резкость и размытость изображения, неправильное расположение экрана.

Расстройство органов зрения значительно увеличивается при работе, осуществляемой с использованием экранов и дисплеев, более 4 часов в день. Всемирная организация здравоохранения ввела понятие «компьютерный зрительный синдром», основными симптомами которого являются покраснение век, жжение в глазах, конъюнктивиты, чувство инородного тела под веками, размытость изображения, затуманивание зрения, замедленная перефокусировка с дальних объектов на ближние и наоборот, боли в области лба и глазниц.

Для снижения нагрузки на глаза и предотвращения усталости глаз с периодичностью в два-три часа следует выполнять следующий комплекс упражнений:

- движение глазами вниз-вверх;
- движение глаз права налево и наоборот;
- движение глазами по диагонали;
- движение глазами по часовой стрелке и против нее;
- сведение глаз к носу. Для этого нужно вытянуть перед собой, взять карандаш, и медленно, не отводя глаз от карандаша, приближать его к носу;
- закрыть глаза, с силой зажмуриться, затем открыть глаза и не моргать несколько секунд;
- с открытыми глазами в такт дыханию «рисовать восьмерку»;
- переключение внимания с близких объектов на дальние и наоборот.

При усталости глаз, в случаях, если глаза начинают слезиться, и других случаях, связанных с чрезмерной нагрузкой на органы зрения, во избежание появления осложнений рекомендуется на несколько минут переключаться с работы на рассматривание удаленных предметов или просто закрывать глаза.

Заключение

В результате выпускной квалификационной работы был произведен анализ существующей информационной системы персональных данных «Кадры» АО «Радиозавод», актуализация и приведение системы защиты в соответствие действующим законодательным нормам.

Были произведены описание существующей системы персональных данных, и разработан документ «Описание технологических процессов в информационной системе персональных данных». Был определен уровень защищенности ИСПДн и составлен акт определения уровня защищенности, а также определены актуальные угрозы и составлена частная модель угроз безопасности ПДн при обработке в ИСПДн. Для актуальных угроз и в соответствии с определенным уровнем защищенности были выбраны меры защиты и соответствующие им средства защиты.

На основании изменений в структуре ИС, процессах обработки ПДн и в соответствии с выбранными мерами и средствами защиты были актуализированы следующие документы:

- паспорт на информационную систему персональных данных «Кадры» АО «Радиозавод»;
- техническое задание на информационную систему персональных данных «Кадры» предприятия АО «Радиозавод».

В результате выполнения пункта задания по разработке комплекта организационно-распорядительной документации были разработаны следующие документы:

- положение об обработке и защите персональных данных АО «Радиозавод»;
- инструкция администратора информационной безопасности информационной системы персональных данных;
- инструкция пользователя информационной системы персональных данных на предприятии АО «Радиозавод»;

– правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в АО «Радиозавод».

Задание на выпускную квалификационную работу выполнено в полном объеме.

Список используемых источников

- 1 Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. [Электронный ресурс]. – Режим доступа: <http://fstec.ru/component/attachments/download/289>
- 2 Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: постановление Правительства РФ от 01.11.2012 N 1119. [Электронный ресурс]. – Режим доступа: <http://legalacts.ru/doc/postanovlenie-pravitelstva-rf-ot-01112012-n-1119>
- 3 Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: Приказ ФСТЭК от 18 февраля 2013г. №21. [Электронный ресурс]. – Режим доступа: <https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691>
- 4 О персональных данных: Федеральный закон от 27.07.2006 N 152-ФЗ. [Электронный ресурс]. – Режим доступа: <https://rg.ru/2006/07/29/personalnnye-dannye-dok.html>
- 5 Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации: Постановление Правительства РФ от 15.09.2008 N 687. [Электронный ресурс]. – Режим доступа: <http://legalacts.ru/doc/postanovlenie-pravitelstva-rf-ot-15092008-n-687>
- 6 Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. [Электронный ресурс]. – Режим доступа: <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380>

7 Трудовой кодекс Российской Федерации от 30.12.2001 N 197-ФЗ (ред. от 05.02.2018): глава 14. [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_34683/

8 Методика определения угроз безопасности информации в информационных системах: Методический документ. [Электронный ресурс]. – Режим доступа: <https://fstec.ru/component/attachments/download/812>

9 Методические рекомендации по составлению Частной модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных учреждений здравоохранения, социальной сферы, труда и занятости. [Электронный ресурс]. – Режим доступа: <http://www.endocrincentr.ru/files/MetodichrekomendModeugroz2009.doc>

10 Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами: Постановление Правительства РФ от 21.03.2012 N 211 (ред. от 06.09.2014). [Электронный ресурс]. – Режим доступа: <http://legalacts.ru/doc/postanovlenie-pravitelstva-rf-ot-21032012-n-211>

Приложение А
(обязательное)
Описание технологических процессов в информационной системе
персональных данных «кадры» предприятия АО «Радиозавод»

«Согласовано»

Директор по персоналу и режиму

_____ С.Г. Викторov

« ____ » _____ 2018г

«Утверждаю»

Генеральный директор

_____ А.Г. Быстров

« ____ » _____ 2018г

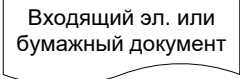
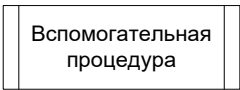
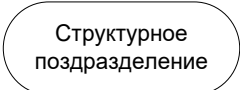
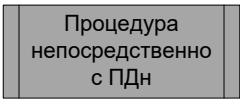
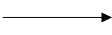
ОПИСАНИЕ

Технологических процессов в информационной системе персональных
данных «Кадры» предприятия АО «Радиозавод»

г. Пенза

2018 г.

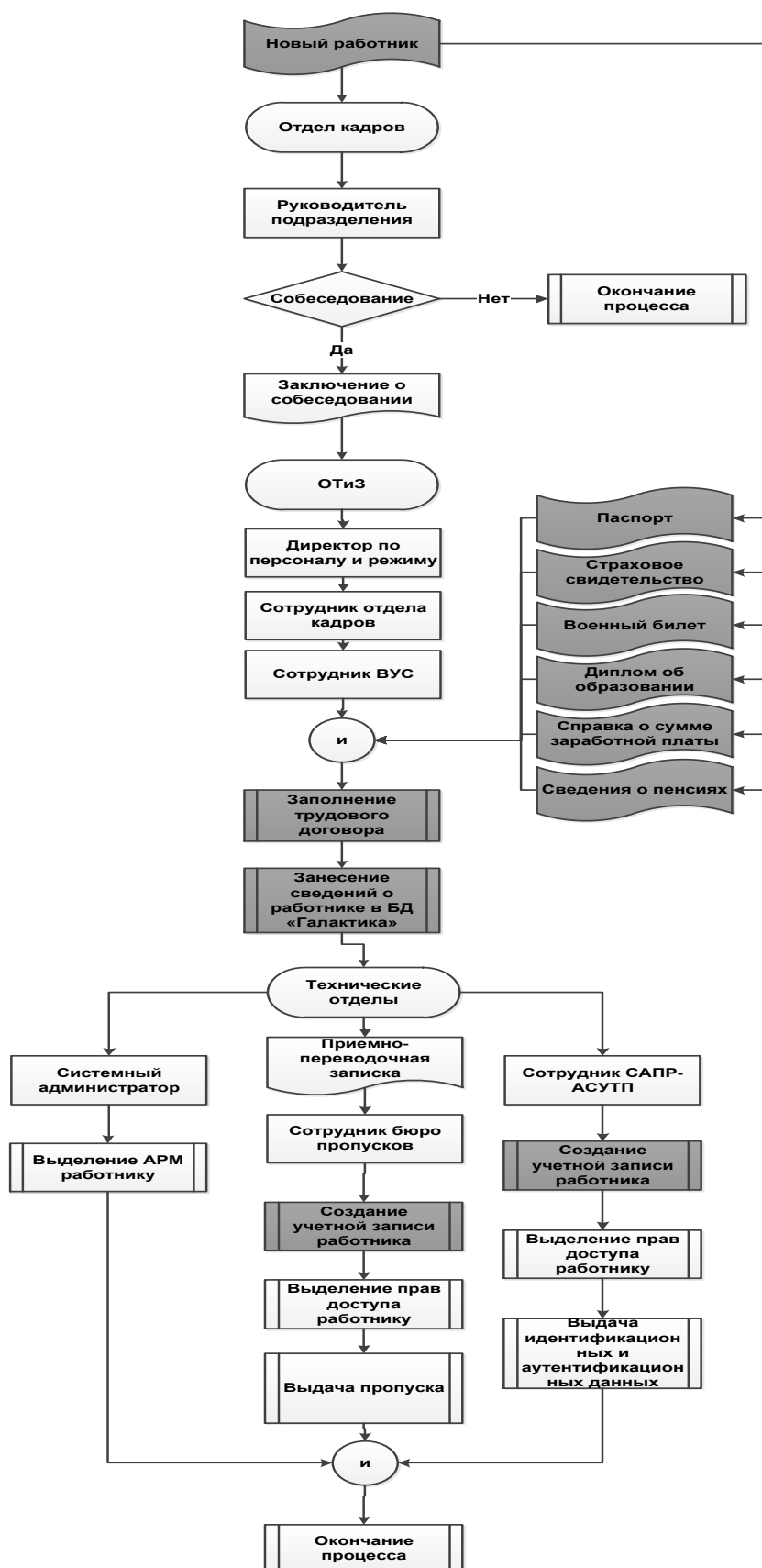
1. УСЛОВНЫЕ ОБОЗНАЧЕНИЯ

Обозначение	Значение
	Должностное лицо, которое участвует в обработке ПДн
	Условие ветвления процесса (да/нет)
	Внешние источники ПДн
	Входящий бумажный или электронный документ, который необходим для выполнения процедуры
	Процедура технологического процесса, носящая вспомогательный характер
	Структурное подразделение, которое участвует в обработке ПДн
	Процедура технологического процесса, предусматривающая непосредственную работу с ПДн
	Путь процесса
	Логическое «И»
	Логическое «ИЛИ»

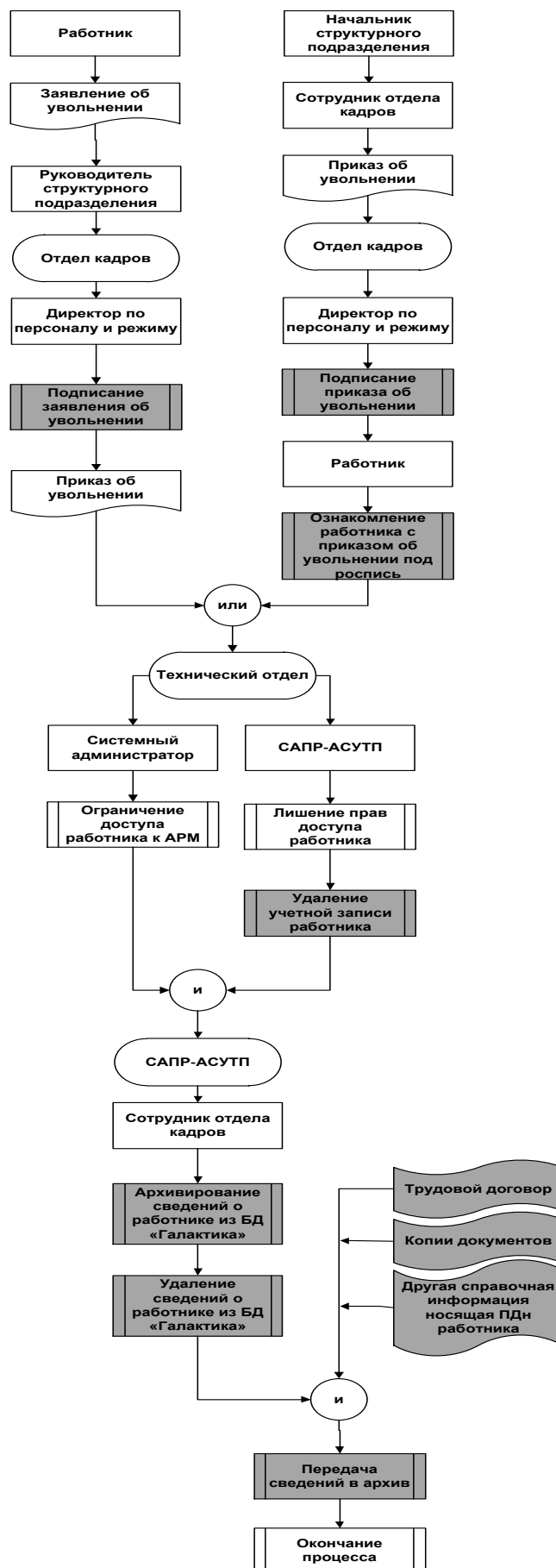
2. ТЕХНОЛОГИЧЕСКАЯ КАРТА ПРОЦЕССОВ ОБРАБОТКИ

ПДН

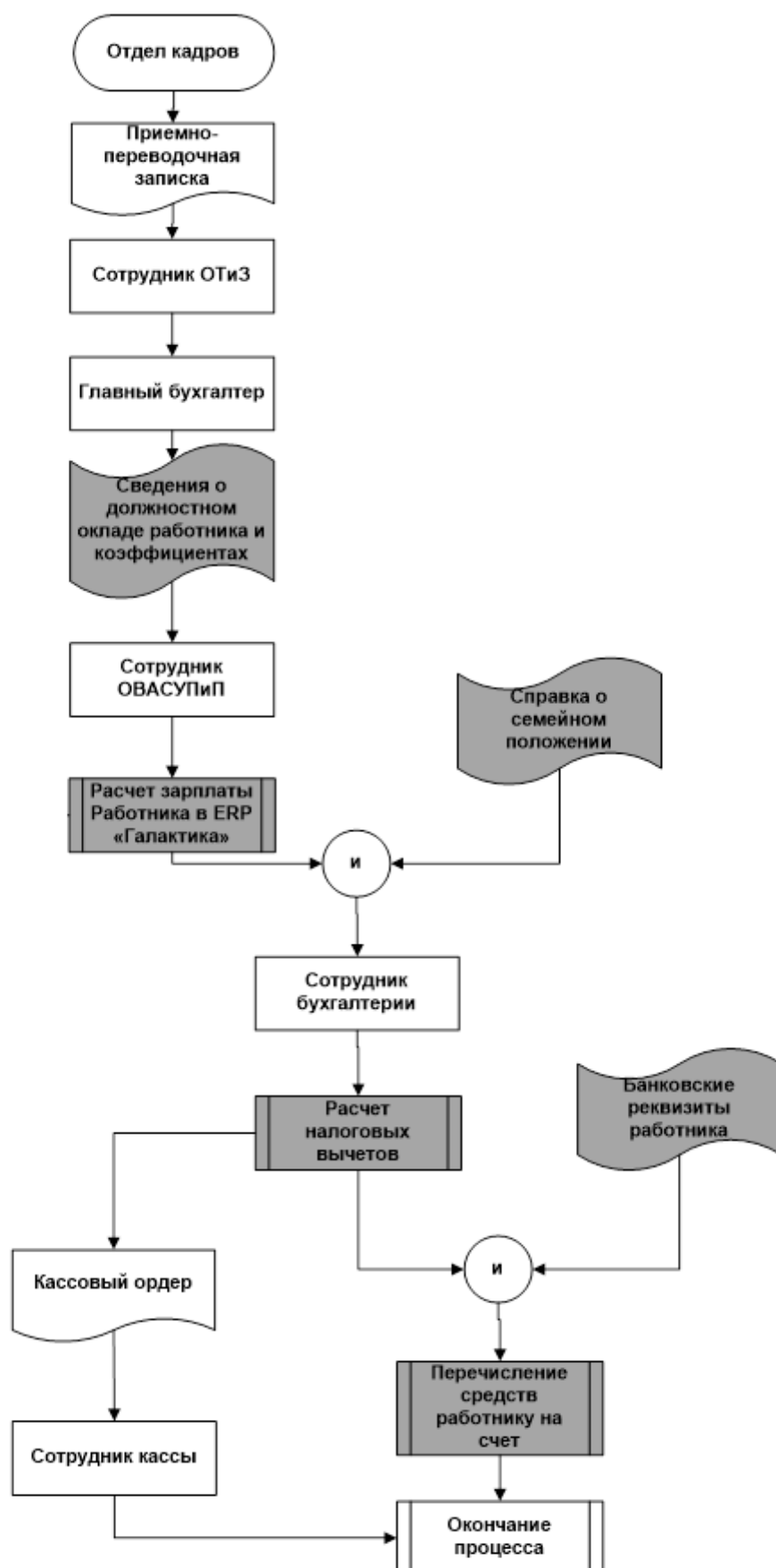
2.1. Технологическая карта процесса приема сотрудника на работу



2.2. Технологическая карта процесса увольнения работника



2.3. Технологическая карта процесса начисления работнику заработной платы



3. ОБЩЕЕ ОПИСАНИЕ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ ОБРАБОТКИ ПДн

Наименование процедуры	Входящие документы, содержащие ПДн	Исходящие документы, содержащие ПДн	Участники процедуры
Прием сотрудника на работу	<ul style="list-style-type: none"> - Паспорт - Диплом об образовании - Страховое свидетельство - Военный билет - Справка о сумме заработной платы - Трудовая книжка 	<ul style="list-style-type: none"> - Сведения в БД «Галактика» - Трудовой договор - Приемно-переводочная записка - Сведения об уникальном идентификаторе работника в ИСПДн 	<ul style="list-style-type: none"> - Руководитель подразделения - Системный администратор - Директор по персоналу и режиму - Сотрудник ВУС - Сотрудник САПР-АСУТП - Сотрудник отдела кадров - Сотрудник отдела пропусков
Начисление работнику зарплаты	<ul style="list-style-type: none"> - Трудовой договор - Сведения из БД работников - Справка о семейном положении - Банковские реквизиты работника 	<ul style="list-style-type: none"> - Кассовый ордер - Квитанция о начислении зарплаты 	<ul style="list-style-type: none"> - Главный бухгалтер - Сотрудник САПР-АСУТП - Сотрудник отдела кадров - Сотрудник ОТиЗ

Наименование процедуры	Входящие документы, содержащие ПДн	Исходящие документы, содержащие ПДн	Участники процедуры
Увольнение работника	<ul style="list-style-type: none"> - Приказ об увольнении - Копии документов работника - Трудовой договор - Трудовая книжка 	<ul style="list-style-type: none"> - Трудовая книжка - Приказ об увольнении - Расторгнутый трудовой договор - Копии документов 	<ul style="list-style-type: none"> - Директор по персоналу и режиму - Руководитель структурного подразделения - Системный администратор - Сотрудник отдела кадров - Сотрудник отдела САПР-АСУТП - Работник

Начальник ОК
 _____ Т.В. Кирюшкина
 «__» _____ 2018 г.
 Главный бухгалтер
 _____ Н.И. Игнашкина
 «__» _____ 2018 г.
 Начальник ОТиЗ
 _____ О.Ф. Емельянова
 «__» _____ 2018 г.

Начальник САПР-АСУТП
 _____ В.Е. Поляков
 «__» _____ 2018 г.
 Начальник ОВАСУПиП
 _____ Г.А. Панин
 «__» _____ 2018 г.
 Начальник ОВО
 _____ Е.М. Жеребцов
 «__» _____ 2018 г.

Начальник ОЗИ
 _____ В.Б. Бородин
 «__» _____ 2018 г.
 Инженер ОЗИ
 _____ Д.Д. Березин
 «__» _____ 2018 г.

Приложение Б
(обязательное)

Акт определения уровня защищенности информационной системы
персональных данных «Кадры» АО «Радиозавод»

Утверждаю
Генеральный директор
_____ А.Г. Быстров
«__» _____ 2018

АКТ
определения уровня защищенности ИСПДн
«Кадры» АО «Радиозавод»

Комиссия в составе:

Председатель:	- директор по персоналу и режиму	Викторов С.Г.
члены комиссии:	- начальник ОК	Кирюшкина Т.В.
	- начальник ОВАСУП и П	Панин Г.А.
	- начальник ОЗИ	Бородин В.Б.
	- инженер ОЗИ	Березин Д.Д.

Рассмотрев исходные данные на информационную систему персональных данных «Кадры» АО «Радиозавод», комиссия установила:

1. В ИСПДн обрабатываются данные субъектов персональных данных, состоящих в трудовых отношениях с предприятием (оператором).

2. Для ИСПДн актуальны угрозы третьего типа.

3. В ИСПДн одновременно обрабатываются персональные данные менее 100 000 субъектов персональных данных.

В соответствии с пунктом 12 «Требований к защите персональных данных при их обработке в информационных системах персональных данных», утвержденных постановлением Правительства Российской Федерации от 01.11.2012 № 1119, и на основании анализа исходных данных, комиссия решила – **присвоить информационной системе персональных данных «Кадры» АО «Радиозавод» четвертый уровень защищенности.**

Директор по персоналу и режиму	С.Г. Викторов
Начальник ОК	Т.В. Кирюшкина
Начальник ОВАСУП и П	Г.А. Панин
Начальник ОЗИ	В.Б. Бородин
Инженер ОЗИ	Д.Д. Березин

Приложение В

(обязательное)

технический паспорт на информационную систему персональных данных
«Кадры» АО «Радиозавод»

«Согласовано»

Директор по персоналу и режиму

_____ С.Г. Викторов

«__» _____ 2018г

«Утверждаю»

Генеральный директор

_____ А.Г. Быстров

«__» _____ 2018г

ТЕХНИЧЕСКИЙ ПАСПОРТ

на информационную систему персональных данных «Кадры» АО

«Радиозавод»

2018 г.

1 Общие сведения об ИСПДн

1.1 Наименование ИСПДн: ИСПДн «Кадры» АО «Радиозавод».

1.2 Физическое расположение ИСПДн: г. Пенза, ул. Байдукова 1, корпус №4.

1.3 Частная модель угроз безопасности персональных данных в ИСПДн «Кадры» АО «Радиозавод» утверждена генеральным директором.

1.4 ИСПДн находится в пределах контролируемой зоны на большом удалении от ее границ.

1.5 Перечень ПДн, обрабатываемых в ИСПДн «Кадры» АО «Радиозавод» приведен в таблице 1. В ИСПДн обрабатываются только данные работников.

Таблица 1 – Перечень персональных данных, обрабатываемых в ИСПДн

Наименование ПДн	Цель обработки ПДн в рамках ИСПДн
Первичные учетные данные: <ul style="list-style-type: none">– ФИО работника, год рождения;– серия и номер документа, удостоверяющего личность;– адрес места прописки;– телефон;– реквизиты документов об образовании;– сведения о воинском учете;– сведения о предыдущем месте работы.	Учет работников. Осуществление процессов согласно трудовому законодательству РФ.

Продолжение таблицы 1

Наименование ПДн	Цель обработки ПДн в рамках ИСПДн
<p>Сведения о занимаемой должности:</p> <ul style="list-style-type: none"> – профессия, должность; – стаж работы. 	<p>Поддержание иерархии отношений между работниками.</p> <p>Осуществление процессов согласно трудовому законодательству РФ.</p>
<p>Финансовое состояние работника:</p> <ul style="list-style-type: none"> – ФИО работника, год рождения; – заработная плата работника. 	<p>Осуществление налоговых отчислений.</p> <p>Осуществление процессов согласно трудовому законодательству РФ.</p>
<p>Сведения о реквизитах работника:</p> <ul style="list-style-type: none"> – ИНН, номер свидетельства государственного пенсионного страхования; – сведения, необходимые для начисления заработной платы, произведения вычетов из заработной платы, для оформления бухгалтерской, налоговой и статистической отчетности (банковские реквизиты и т.п.). 	<p>Осуществление процессов согласно трудовому законодательству РФ.</p>
<p>Дополнительные сведения о работнике:</p> <ul style="list-style-type: none"> – сведения о рождении ребенка; – сведения о семейном положении. 	<p>Выплата льгот и иных надбавок.</p> <p>Осуществление процессов согласно трудовому законодательству.</p>

2 Технологические процессы обработки ПДн, используемые в ИСПДн

Перечень технологических процессов обработки персональных данных, используемых в ИСПДн, приведен в таблице 2.

Таблица 2 – Перечень технологических процессов

№	Наименование
1	Прием сотрудника на работу
2	Увольнение работника
3	Начисление заработной платы работнику

3 Состав оборудования системы

3.1 Состав основных технических средств и систем, входящих в состав ИСПДн

Состав основных технических средств приведен в таблице 3.

Таблица 3 – Перечень основных технических средств в составе ИСПДн

№	Тип ОТСС	Программные и технические характеристики	Место установки	Кол-во, шт
1	АРМ генерального директора (инв. номер №ПЭВМ-ПДн 001)	-Процессор: Intel(R) Pentium Dual-Core G840 @ 2.80GHz -Память: 4096 Мб -HDD: 500 Гб -Материнская плата: Gigabyte GA-H61M -Интегрированная видеокарта -ОС: Лицензионная Microsoft Windows 7 SP1 -Антивирус: Dr.Web -Microsoft Office 2010 -DeviceLock 8 DLP Suite -ViPNet Personal Firewall 4	Каб. №203а	1

Продолжение таблицы 3

№	Тип ОТСС	Программные и технические характеристики	Место установки	Кол-во, шт
2	АРМ директора по персоналу и режиму (инв. номер № ПЭВМ -ПДн 002)	-Процессор: Intel(R) Celeron(R) 430 CPU1.80GHz -Память: 1024 Мб -HDD: 80 Гб -Материнская плата: Intel Bearlake G31 -Интегрированная видеокарта -ОС: Лицензионная Microsoft Windows 7SP1 -Антивирус: Dr.Web -Microsoft Office 2010 -DeviceLock 8 DLP Suite -ViPNet Personal Firewall 4	Каб. №115	1
3	АРМ первого заместителя генерального директора (инв. номер № ПЭВМ - ПДн 003)	- Процессор: Intel(R) Pentium(R) Dual-Core G840 @ 2.80GHz -Память: 4096 Мб -Жесткий диск: 500 Гб -Материнская плата: Gigabyte GA-H61M -Интегрированная видеокарта -ОС: Лицензионная Microsoft Windows 7 SP1 -Антивирус: Dr.Web -Microsoft Office 2010 -DeviceLock 8 DLP Suite -ViPNet Personal Firewall 4	Каб. №203б	1

Продолжение таблицы 3

№	Тип ОТСС	Программные и технические характеристики	Место установки	Кол-во, шт
4	АРМ управляющего по ИТО (инв. номер № ПЭВМ-ПДн 004)	-Процессор: Intel(R) Pentium Dual-Core E6300 @ 2.80GHz -Память: 2048 Мб -HDD: 250 Гб -Материнская плата: Intel Bearlake G31 -Интегрированная видеокарта -ОС: Лицензионная Microsoft Windows 7 SP1 -Антивирус: Dr.Web -Microsoft Office 2010 -DeviceLock 8 DLP Suite -ViPNet Personal Firewall 4	Каб. №411	1
5	АРМ главного бухгалтера (инв.номер № ПЭВМ-ПДн 005)	-Процессор: Intel(R) Pentium Dual-Core CPU E5200 @ 2.50GHz -Память: 2048 Мб -HDD: 160 Гб -Материнская плата: P43ME -Интегрированная видеокарта -ОС: Лицензионная Microsoft Windows 7 SP1 -Антивирус: Dr.Web -Microsoft Office 2010 -DeviceLock 8 DLP Suite -ViPNet Personal Firewall 4	Каб. №213	1

Продолжение таблицы 3

№	Тип ОТСС	Программные и технические характеристики	Место установки	Кол-во, шт
6	АРМ заместителя главного бухгалтера (инв.номер №ПЭВМ-ПДн 006)	-Процессор: Intel(R) Pentium Celeron(R) CPU @ 3.06GHz -Память: 1024 Мб -HDD: 160 Гб -Материнская плата: P5LD2 -Интегрированная видеокарта -ОС: Лицензионная Microsoft Windows 7 SP1 -Антивирус: Dr.Web -Microsoft Office 2010 -DeviceLock 8 DLP Suite -ViPNet Personal Firewall 4	Каб. №222	1
7	АРМ бухгалтера 2 категории (инв. номер №ПЭВМ-ПДн 007)	-Процессор: Intel(R) Celeron(R) D 320 2.40GHz -Память: 1024 Мб -HDD: 160 Гб -Материнская плата: P4-P800 -Интегрированная видеокарта -ОС: Лицензионная Microsoft Windows 7 SP1 -Антивирус: Dr.Web -Microsoft Office 2010 -DeviceLock 8 DLP Suite -ViPNet Personal Firewall 4	Каб. №224	1

Продолжение таблицы 3

№	Тип ОТСС	Программные и технические характеристики	Место установки	Кол-во, шт
8	АРМ бухгалтера (инв. номер №ПЭВМ-ПДн 008)	-Процессор: Intel(R) Pentium Celeron(R) CPU 1000МН -Память: 1024 Мб -HDD: 40 Гб -Материнская плата: i815-47B27X -Интегрированная видеокарта -ОС: Лицензионная Microsoft Windows 7 SP1 -Антивирус: Dr.Web -Microsoft Office 2010 -DeviceLock 8 DLP Suite -ViPNet Personal Firewall 4	Каб. №224	1
9	АРМ начальника ОТиЗ (инв. номер №ПЭВМ-ПДн 009)	-Процессор: Intel(R) Pentium Dual CPU E2180 @ 2.00GHz -Память: 1024 Мб -HDD: 80 Гб -Материнская плата: P5GC-MX/GBL -Интегрированная видеокарта -ОС: Лицензионная Microsoft Windows 7 SP1 -Антивирус: Dr.Web -Microsoft Office 2010 -DeviceLock 8 DLP Suite -ViPNet Personal Firewall 4	Каб. №101	1

Продолжение таблицы 3

№	Тип ОТСС	Программные и технические характеристики	Место установки	Кол-во, шт
10	АРМ экономиста 2 категории (инв. номер №ПЭВМ-ПДн 010)	-Процессор: Intel(R) Pentium Celeron(R) CPU @ 2.66GHz -Память: 1024 Мб -HDD: 120 Гб -Материнская плата: MS-7103 -Интегрированная видеокарта -ОС: Лицензионная Microsoft Windows 7 SP1 -Антивирус: Dr.Web -Microsoft Office 2010 -DeviceLock 8 DLP Suite -ViPNet Personal Firewall 4	Каб. №101	1
11	АРМ экономиста 1 категории (инв. номер №ПЭВМ-ПДн 011)	-Процессор: Intel(R) Pentium 4 CPU @ 3.20 GHz -Память: 512 Мб -HDD: 80 Гб -Материнская плата: 8I945PLGE-RH -Интегрированная видеокарта -ОС: Лицензионная Microsoft Windows 7 SP1 -Антивирус: Dr.Web -Microsoft Office 2010 -DeviceLock 8 DLP Suite -ViPNet Personal Firewall 4	Каб. №101	1

Продолжение таблицы 3

№	Тип ОТСС	Программные и технические характеристики	Место установки	Кол-во, шт
12	АРМ начальника ОК (инв. номер №ПЭВМ-ПДн 012)	-Процессор: Intel(R) Core(TM) i3-2100 CPU @ 3.10GHz -Память: 3096 Мб -HDD: 320 Гб -Материнская плата: H161M-P23 -Интегрированная видеокарта -ОС: Лицензионная Microsoft Windows 7 SP1 -Антивирус: Dr.Web -Microsoft Office 2010 -DeviceLock 8 DLP Suite -ViPNet Personal Firewall 4	Каб. №103б	1
13	АРМ менеджера по работе с персоналом (инв. номер №ПЭВМ-ПДн 013)	-Процессор: Intel(R) Core(TM)2 Duo CPU @ 2.50GHz -Память: 2048 Мб -HDD: 500 Гб -Материнская плата: H61 -Интегрированная видеокарта -ОС: Лицензионная Microsoft Windows 7 SP1 -Антивирус: Dr.Web -Microsoft Office 2010 -DeviceLock 8 DLP Suite -ViPNet Personal Firewall 4	Каб. №103а	1

Продолжение таблицы 3

№	Тип ОТСС	Программные и технические характеристики	Место установки	Кол-во, шт
14	АРМ менеджера по работе с персоналом (инв. номер №ПЭВМ-ПДн 014)	-Процессор: Intel(R) Celeron(TM) CPU 1000МН -Память: 512 Мб -HDD: 40 Гб -Материнская плата: i815-47B27X -Интегрированная видеокарта -ОС: Лицензионная Microsoft Windows 7 SP1 -Антивирус: Dr.Web -Microsoft Office 2010 -DeviceLock 8 DLP Suite -ViPNet Personal Firewall 4	Каб. №103а	1
15	АРМ менеджера по работе с персоналом (инв. номер №ПЭВМ-ПДн 015)	-Процессор: Intel(R) Celeron(R) CPU @ 2.53GHz -Память: 1024 Мб -HDD: 40 Гб -Материнская плата: 8I915ME -Интегрированная видеокарта -ОС: Лицензионная Microsoft Windows 7 SP1 -Антивирус: Dr.Web -Microsoft Office 2010 -DeviceLock 8 DLP Suite -ViPNet Personal Firewall 4	Каб. №103	1

Продолжение таблицы 3

№	Тип ОТСС	Программные и технические характеристики	Место установки	Кол-во, шт
16	АРМ менеджера по работе с персоналом (инв. номер №ПЭВМ-ПДн 016)	-Процессор: Intel(R) Celeron(R) CPU @ 2.40GHz -Память: 1024 Мб -HDD: 40 Гб -Материнская плата: i845PE-W83627 -Интегрированная видеокарта -ОС: Лицензионная Microsoft Windows 7 SP1 -Антивирус: Dr.Web -Microsoft Office 2010 -DeviceLock 8 DLP Suite -ViPNet Personal Firewall 4	Каб. №103	1
17	АРМ менеджера по работе с персоналом (инв. номер №ПЭВМ-ПДн 017)	-Процессор: Intel(R) Celeron(R) CPU 450 @ 2.20GHz -Память: 1024 Мб -HDD: 160 Гб -Материнская плата: G31T-M7 -Интегрированная видеокарта -ОС: Лицензионная Microsoft Windows 7 SP1 -Антивирус: Dr.Web -Microsoft Office 2010 -DeviceLock 8 DLP Suite -ViPNet Personal Firewall 4	Каб. №103	1

Продолжение таблицы 3

№	Тип ОТСС	Программные и технические характеристики	Место установки	Кол-во, шт
18	АРМ менеджера по работе с персоналом (инв. номер №ПЭВМ-ПДн 018)	-Процессор: Intel(R) Pentium (R) Dual CPU E2140 @ 1.60GHz -Память: 1024 Мб -HDD: 160 Гб -Материнская плата: MS-7235 -Интегрированная видеокарта -ОС: Лицензионная Microsoft Windows 7 SP1 -Антивирус: Dr.Web -Microsoft Office 2010 -DeviceLock 8 DLP Suite -ViPNet Personal Firewall 4	Каб. №103	1
19	АРМ менеджера по работе с персоналом (инв. номер №ПЭВМ-ПДн 019)	-Процессор: Intel(R) Core(TM) i3 CPU 550 @ 3.20GHz -Память: 3096 Мб -HDD: 320 Гб -Материнская плата: H55M-P31 -Интегрированная видеокарта -ОС: Лицензионная Microsoft Windows 7 SP1 -Антивирус: Dr.Web -DeviceLock 8 DLP Suite -ViPNet Personal Firewall 4 -Microsoft Office 2010	Каб. №103	1

Продолжение таблицы 3

№	Тип ОТСС	Программные и технические характеристики	Место установки	Кол-во, шт
20	АРМ инженера ВУС 2 категории (инв. номер №ПЭВМ-ПДн 020)	-Процессор: Intel(R) Celeron(R) CPU 1000МН -Память: 512 Мб -HDD: 60 Гб -Материнская плата: i815-47B27X -Интегрированная видеокарта -ОС: Лицензионная Microsoft Windows 7 SP1 -Антивирус: Dr.Web -Microsoft Office 2010 -DeviceLock 8 DLP Suite -ViPNet Personal Firewall 4	Каб. №109	1
21	АРМ старшего оператора ЭВМ (инв. номер №ПЭВМ-ПДн 021)	-Процессор: Intel(R) Pentium Dual CPU E2140 @ 1.60GHz -Память: 512 Мб -HDD: 80 Гб -Материнская плата: 5P945-GLi -Интегрированная видеокарта -ОС: Лицензионная Microsoft Windows 7 SP1 -Антивирус: Dr.Web -Microsoft Office 2010 -DeviceLock 8 DLP Suite -ViPNet Personal Firewall 4	Каб. №423	1

Продолжение таблицы 3

№	Тип ОТСС	Программные и технические характеристики	Место установки	Кол-во, шт
22	АРМ старшего оператора ЭВМ (инв. номер №ПЭВМ-ПДн 022)	-Процессор: Intel(R) Pentium Celeron(R) CPU 1000MH -Память: 1024 Мб -HDD: 40 Гб -Материнская плата: i815-47B27X -Интегрированная видеокарта -ОС: Лицензионная Microsoft Windows 7 SP1 -Антивирус: Dr.Web -Microsoft Office 2010 -DeviceLock 8 DLP Suite -ViPNet Personal Firewall 4	Каб. №423	1
23	АРМ инженера-программиста (инв. номер №ПЭВМ-ПДн 023)	-Процессор: Intel(R) Core(R) 2 Duo CPU E4700 @ 2.60GHz -Память: 1024 Мб -HDD: 80 Гб -Материнская плата: P5R-LE -Интегрированная видеокарта -ОС: Лицензионная Microsoft Windows 7 SP1 -Антивирус: Dr.Web -Microsoft Office 2010 -DeviceLock 8 DLP Suite -ViPNet Personal Firewall 4	Каб. №407	1

Продолжение таблицы 3

№	Тип ОТСС	Программные и технические характеристики	Место установки	Кол-во, шт
24	АРМ начальника бюро программирования (инв. номер №ПЭВМ-ПДн 024)	-Процессор: Intel(R) Pentium (R) 4 CPU @ 2.60GHz -Память: 1024 Мб -HDD: 80 Гб -Материнская плата: 8l915GMF -Интегрированная видеокарта -ОС: Лицензионная Microsoft Windows 7 SP1 -Антивирус: Dr.Web -Microsoft Office 2010 -DeviceLock 8 DLP Suite -ViPNet Personal Firewall 4	Каб. №407	1
25	АРМ инженера-программиста (инв. номер №ПЭВМ-ПДн 025)	-Процессор: Intel(R) Pentium Celeron(R) Dual CPU E2140 @ 1.60GHz -Память: 1024 Мб -HDD: 80 Гб -Материнская плата: P5LD2 -Интегрированная видеокарта -ОС: Лицензионная Microsoft Windows 7 SP1 -Антивирус: Dr.Web -Microsoft Office 2010 -DeviceLock 8 DLP Suite -ViPNet Personal Firewall 4	Каб. №407	1

Продолжение таблицы 3

№	Тип ОТСС	Программные и технические характеристики	Место установки	Кол-во, шт
26	АРМ ведущего инженера (инв. номер №ПЭВМ-ПДн 026)	-Процессор: Intel(R) Pentium (R) 4 CPU @ 2.66GHz -Память: 512 Мб -HDD: 120 Гб -Материнская плата: 8l915GMF -Интегрированная видеокарта -ОС: Лицензионная Microsoft Windows 7 SP1 -Антивирус: Dr.Web -Microsoft Office 2010 -DeviceLock 8 DLP Suite -ViPNet Personal Firewall 4	Каб. №407	1
27	АРМ старшего оператора ЭВМ (инв. номер №ПЭВМ-ПДн 027)	-Процессор: Intel(R) Pentium (R) 4 CPU @ 2.40GHz -Память: 1024 Мб -HDD: 80 Гб -Материнская плата: P4P800-E -Интегрированная видеокарта -ОС: Лицензионная Microsoft Windows 7 SP1 -Антивирус: Dr.Web -Microsoft Office 2010 -DeviceLock 8 DLP Suite -ViPNet Personal Firewall 4	Каб. №409	1

Продолжение таблицы 3

№	Тип ОТСС	Программные и технические характеристики	Место установки	Кол-во, шт
28	АРМ старшего оператора ЭВМ (инв. номер №ПЭВМ-ПДн 028)	-Процессор: Intel(R) Pentium (R) 4 CPU @ 2.40GHz -Память: 1024 Мб -HDD: 70 Гб -Материнская плата: Springdale-G -Интегрированная видеокарта -ОС: Лицензионная Microsoft Windows 7 SP1 -Антивирус: Dr.Web -Microsoft Office 2010 -DeviceLock 8 DLP Suite -ViPNet Personal Firewall 4	Каб. №409	1
29	АРМ инженера АСУ (инв. номер №ПЭВМ-ПДн 029)	-Процессор: Intel(R) Pentium (R) 4 CPU @ 3.00GHz -Память: 512 Мб -HDD: 80 Гб -Материнская плата: 945P7AA -Интегрированная видеокарта -ОС: Лицензионная Microsoft Windows 7 SP1 -Антивирус: Dr.Web -Microsoft Office 2010 -DeviceLock 8 DLP Suite -ViPNet Personal Firewall 4	Каб. №409	1

Продолжение таблицы 3

№	Тип ОТСС	Программные и технические характеристики	Место установки	Кол-во, шт
30	АРМ начальника расчётного сектора (инв. номер №ПЭВМ-ПДн 030)	-Процессор: Intel(R) Pentium (R) 4 CPU @ 2.40GHz -Память: 768 Мб -HDD: 30 Гб -Материнская плата: Springdale-G -Интегрированная видеокарта -ОС: Лицензионная Microsoft Windows 7 SP1 -Антивирус: Dr.Web -Microsoft Office 2010 -DeviceLock 8 DLP Suite -ViPNet Personal Firewall 4	Каб. №409	1
31	АРМ старшего оператора ЭВМ (инв. номер №ПЭВМ-ПДн 031)	-Процессор: Intel(R) Pentium (R) 4 CPU @ 3.00GHz -Память: 1024 Мб -HDD: 160 Гб -Материнская плата: P5GD1 -Интегрированная видеокарта -ОС: Лицензионная Microsoft Windows 7 SP1 -Антивирус: Dr.Web -Microsoft Office 2010 -DeviceLock 8 DLP Suite -ViPNet Personal Firewall 4	Каб. №409	1

Продолжение таблицы 3

№	Тип ОТСС	Программные и технические характеристики	Место установки	Кол-во, шт
32	АРМ ведущего инженера (инв. номер №ПЭВМ-ПДн 032)	-Процессор: Intel(R) Pentium (R) D CPU @ 3.40GHz -Память: 1024 Мб -HDD: 160 Гб -Материнская плата: 5P945-GLi -Интегрированная видеокарта -ОС: Лицензионная Microsoft Windows 7 SP1 -Антивирус: Dr.Web -Microsoft Office 2010 -DeviceLock 8 DLP Suite -ViPNet Personal Firewall 4	Каб. №402	1
33	АРМ начальника ОБАСУПиП (инв. номер №ПЭВМ-ПДн 033)	-Процессор: Intel(R) Celeron(R) CPU 430 @ 1.80GHz -Память: 2048 Мб -HDD: 160 Гб -Материнская плата: P5KPL-CM -Интегрированная видеокарта -ОС: Лицензионная Microsoft Windows 7 SP1 -Антивирус: Dr.Web -Microsoft Office 2010 -DeviceLock 8 DLP Suite -ViPNet Personal Firewall 4	Каб. №419	1

3.2 Состав вспомогательных технических средств и систем (ВТСС), установленных в помещениях, где расположены ОТСС

Состав ВТСС приведен в таблице 4.

Таблица 4 – Перечень ВТСС, не участвующих в обработке персональных данных

№	Тип ОТСС	Место установки	Кол-во, шт
1	Стационарный телефонный аппарат Ritmix RT-003	Каб. №103а	1
2	Стационарный телефонный аппарат Ritmix RT-003	Каб. №103б	1
3	Стационарный телефонный аппарат Ritmix RT-003	Каб. №103	3
4	Стационарный телефонный аппарат Ritmix RT-003	Каб. №101	1
5	Стационарный телефонный аппарат Ritmix RT-003	Каб. №213	1
7	Стационарный телефонный аппарат Ritmix RT-003	Каб. №222	1
8	Стационарный телефонный аппарат Ritmix RT-003	Каб. №224	1
9	Стационарный телефонный аппарат Ritmix RT-003	Каб. №402	1
10	Стационарный телефонный аппарат Ritmix RT-003	Каб. №407	2
11	Стационарный телефонный аппарат Ritmix RT-003	Каб. №409	1
12	Стационарный телефонный аппарат Ritmix RT-003	Каб. №203	1
13	Стационарный телефонный аппарат Ritmix RT-003	Каб. №115	1
14	Стационарный телефонный аппарат Ritmix RT-003	Каб. №423	1
15	Стационарный телефонный аппарат Ritmix RT-003	Каб. №109	1
16	Принтер лазерный Pantum P2500W	Каб. №103	1
17	Принтер лазерный Pantum P2500W	Каб. №107	1
18	Принтер лазерный Pantum P2500W	Каб. №213	1

3.3 Состав сетевого и коммутационного оборудования, используемого в информационной системе персональных данных

Перечень сетевого и коммутационного оборудования приведен в таблице 5.

Таблица 5 – Перечень сетевого и коммутационного оборудования

№	Тип ОТСС	Место установки	Кол-во, шт
1	Коммутатор TP-LINK TL-SF1024M	Каб. №103б	1
2	Коммутатор TP-LINK TL-SF1024M	Каб. №222	1
3	Коммутатор TP-LINK TL-SF1024M	Каб. №419	1
4	Маршрутизатор Mikrotik RB952Ui-5ac2nD	Каб. №103	1

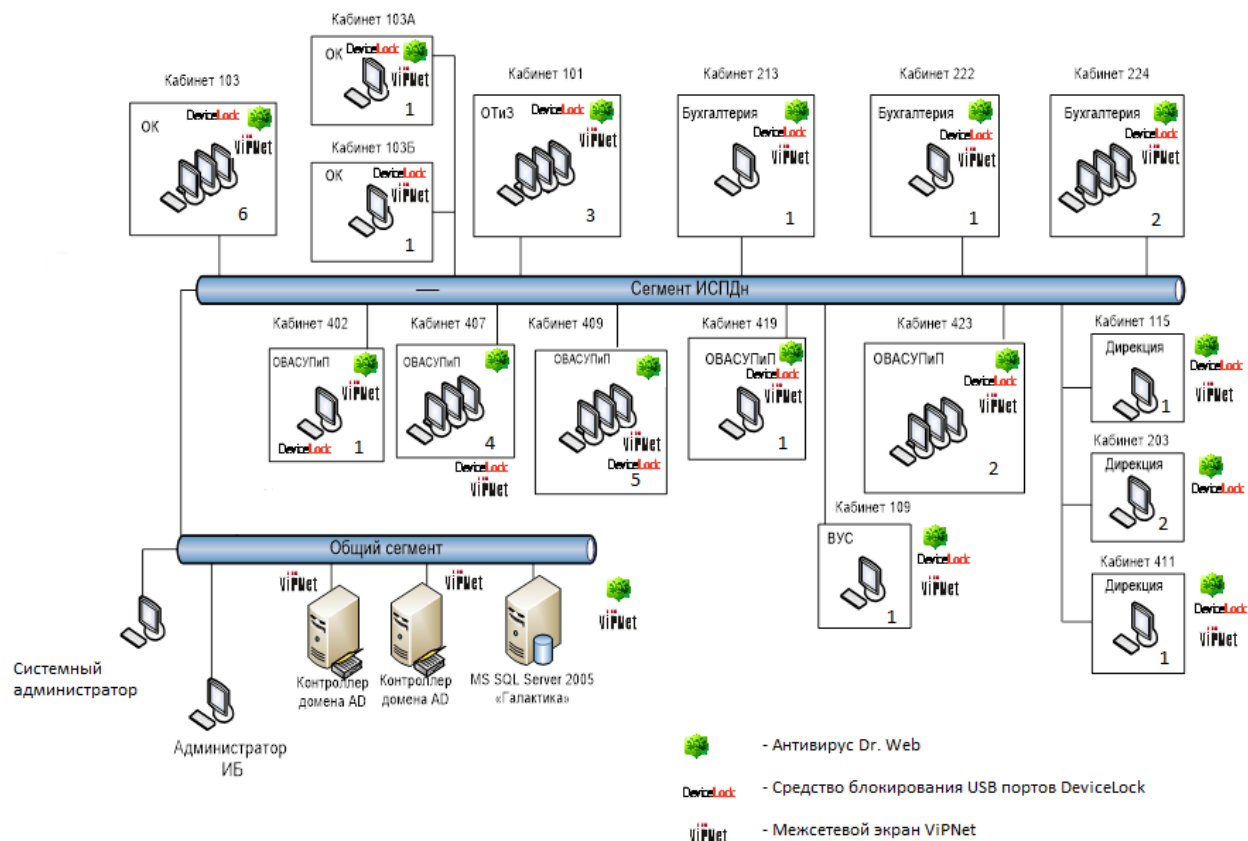
3.4 Состав средств защиты информации

Состав средств защиты информации, приведен в таблице 6.

Таблица 6 – Перечень средств защиты информации, установленных в ИСПДн

№	Наименование и тип технического средства	Сведения о сертификате	Место установки
1	MS Windows Professional 7 SP1	Сертификат ФСТЭК №2180/1 от 04.10.2011	Инв.номер №ПЭВМ-ПДн: 001,002,003,004,005,006, 007,008,009,010,011,012, 013,014,015,016,017,018,019, 020,021,022,023,024,025,026, 027,028,029,030,031,032,033
2	ViPNet Personal Firewall 4 ФРКЕ 00125-01	Сертификат соответствия ФСБ России № СФ/515-3136 от 30.06. 2017 года	Инв.номер №ПЭВМ-ПДн: 001,002,003,004,005,006, 007,008,009,010,011,012, 013,014,015,016,017,018,019, 020,021,022,023,024,025,026, 027,028,029,030,031,032,033
3	Антивирус Dr.Web версия 6.00.3	Сертификат соответствия ФСТЭК №2446 от 20.09.2017г Лицензионное соглашение № _____ от «__» _____ до «__» _____	Инв.номер №ПЭВМ-ПДн: 001,002,003,004,005,006, 007,008,009,010,011,012, 013,014,015,016,017,018,019, 020,021,022,023,024,025,026, 027,028,029,030,031,032,033
4	DeviceLock 8 DLP Suite	Сертификат соответствия ФСТЭК № 3465 от 05.11.2015	Инв.номер №ПЭВМ-ПДн: 001,002,003,004,005,006, 007,008,009,010,011,012, 013,014,015,016,017,018,019, 020,021,022,023,024,025,026, 027,028,029,030,031,032,033

4 Структурная схема информационной системы персональных данных



Начальник ОЗИ

В.Б. Бородин

«__» _____ 2018г.

Инженер ОЗИ

Д.Д. Березин

«__» _____ 2018г.

Приложение Г
(обязательное)
положение об обработке и защите персональных данных АО «Радиозавод»

«Согласовано»

Директор по персоналу и режиму

_____ С.Г. Викторov

« ____ » _____ 2018г.

«Утверждаю»

Генеральный директор

_____ А.Г. Быстров

« ____ » _____ 2018г.

ПОЛОЖЕНИЕ
об обработке и защите персональных данных
АО «Радиозавод»

2018 г

СОДЕРЖАНИЕ

1	Общие положения	119
2	Состав персональных данных	120
3	Принципы обработки персональных данных	122
4	Порядок обработки персональных данных без использования средств автоматизации	126
5	Доступ к персональным данным	128
6	Передача персональных данных	130
7	Уничтожение персональных данных	131
8	Защита персональных данных	132
9	Внутренняя защита	133
10	Внешняя защита	134
11	Ответственность	135
	Приложение №1	137
	Приложение №2	138
	Приложение 3	139

1 Общие положения

1.1 Положение об обработке и защите персональных данных на АО «Радиозавод» (далее Положение) разработано в соответствии с Трудовым кодексом Российской Федерации, Конституцией Российской Федерации, Гражданским кодексом Российской Федерации, Федеральным законом №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом №152-ФЗ «О персональных данных», Постановлением Правительства РФ №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановлением Правительства РФ №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», иными федеральными законами.

1.2 Настоящее Положение определяет порядок и условия обработки персональных данных работников АО «Радиозавод» (далее Оператор) с использованием средств автоматизации и без использования таких средств, а также ответственность за нарушение порядка работы с персональными данными.

1.3 Настоящее Положение и изменения к нему вводятся в действие приказом генерального директора или уполномоченного им лица. Руководители всех структурных подразделений обязаны ознакомить с Положением своих работников под роспись.

2 Состав персональных данных

2.1 Оператор обрабатывает следующие персональные данные работников:

- фамилия, имя, отчество работника;
- дата и место рождения работника;
- паспортные данные;
- адрес проживания (регистрации) работника;
- домашний телефон;
- сведения о предыдущем месте работы;
- семейное, социальное, имущественное положение работника;
- место работы или учебы членов семьи и родственников;
- сведения о социальных льготах;
- сведения о наличии судимостей;
- содержание трудового договора;
- сведения об образовании;
- профессия, специальность, занимаемая должность;
- сведения о трудовом и общем стаже;
- сведения о воинском учете;
- сведения о заработной плате работника.

2.2 К документам, в которых содержатся персональные данные работников, относятся:

- копия страхового свидетельства государственного пенсионного страхования;
- анкеты;
- трудовая книжка;
- заявления;
- копии документа воинского учета (для военнообязанных лиц и лиц, подлежащих призыву на военную службу);
- подлинники и копии приказов по личному составу;

- трудовой договор;
- документы об образовании, о квалификации или наличии специальных знаний (при поступлении на работу, требующую специальных знаний или специальной подготовки);
- рекомендации, характеристики;
- дела, содержащие материалы по повышению квалификации и переподготовке работника, их аттестации, служебным расследованиям;
- отчеты, аналитические и справочные материалы, передаваемые в государственные органы статистики, налоговые инспекции, другие учреждения, головную организацию;
- личные карточки (форма Т-2).

2.3 Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом.

2.4 Требования Положения не распространяются на порядок обращения со сведениями, составляющими государственную тайну.

3 Принципы обработки персональных данных

3.1 Персональные данные работника могут обрабатываться исключительно в целях обеспечения соблюдения нормативных правовых актов и законов, содействия работникам при получении образования, в трудоустройстве и продвижении по службе, контроля качества и количества выполняемой работы, обеспечения личной безопасности работников и сохранности имущества.

3.2 При обработке персональных данных работников Оператор в соответствии с нормативными документами и современными информационными технологиями определяет способы их обработки, хранения, документирования и защиты. Все меры по обеспечению конфиденциальности при сборе, хранении и обработке персональных данных работника распространяются как на бумажные, так и на электронные носители информации.

3.3 Персональные данные могут быть получены исключительно от работника. Работник самостоятельно решает вопрос передачи Оператору своих персональных данных и дает согласие на их обработку и передачу (Приложение №2).

3.4 Если получить персональные данные работника возможно только у третьей стороны, то работник должен быть уведомлен об этом заранее, и от него должно быть получено письменное согласие. Оператор обязан сообщить работнику о способах и источниках получения персональных данных, о целях, а также о характере персональных данных, подлежащих получению, и последствиях отказа работника от дачи письменного согласия на их получение.

3.5 Не допускается без согласия работника получение и обработка персональных данных о его политических, философских или религиозных убеждениях, расовой принадлежности, национальности, частной жизни, его профсоюзной деятельности, а также о его членстве в общественных объединениях. Не допускается обработка информации о состоянии здоровья

работника, кроме сведений, относящихся к вопросу о возможности выполнения работником трудовых обязанностей.

3.6 Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, которые приводят к юридическим последствиям для субъекта персональных данных либо иным способом затрагивают его законные интересы и права.

3.7 В случаях, которые связаны с вопросами трудовых отношений, в соответствии со ст. 24 Конституции РФ, возможно получение и обработка данных о частной жизни работника исключительно с его письменного согласия.

3.8 При приеме на работу работники отдела кадров и бухгалтерии принимают от поступающего на работу следующие документы:

- паспорт;
- диплом об образовании;
- военный билет;
- трудовая книжка;
- свидетельство Пенсионного фонда РФ;
- справка с места учебы детей до 23 лет;
- сведения о пенсиях (военной, по инвалидности, по возрасту);
- справка 2-НДФЛ с предыдущего места работы;
- справка о сумме заработной платы, иных выплат и вознаграждений за 2 календарных года, которые предшествуют году обращения за справкой или году прекращения работы, или текущий календарный год, на который были начислены страховые взносы;

3.9 Дополнительные документы могут быть запрошены по согласованию с работником

3.10 Пакет биографических материалов, которые характеризуют работника, формируется при заключении трудового договора и пополняется

в процессе трудовой деятельности работника. В данный пакет входят следующие категории документов, которые содержат данные о работниках:

- трудовые книжки;
- трудовые договоры;
- комплект материалов по проведению собеседований с кандидатом на должность, их тестированию и анкетированию;
- комплекты документов, которые используются при приеме на работу в процессе оформления трудовых отношений, переводе и увольнении;
- подлинники и копии приказов по кадрам;
- дела, которые содержат материалы аттестаций работников;
- информационно-справочный банк данных по персоналу;
- подлинники и копии аналитических, справочных и отчетных материалов, которые передаются руководителями структурных подразделений руководству предприятия;
- копии отчетов, которые направляются в налоговые инспекции, вышестоящие органы управления, в государственные органы статистики и другие учреждения.

3.11 Пакеты биографических материалов, которые характеризуют работника, хранятся в отделе кадров. Для хранения документов выделяются специально оборудованные сейфы и шкафы, доступ к которым случайных лиц исключен.

3.12 Персональные данные работников, представленные в электронном виде, хранятся в ERP системе «Галактика». Доступ к ним ограничен средствами самой системы.

3.13 В обязанности работника входит:

- передавать Оператору комплект достоверных, документированных персональных данных;
- сообщать об изменении своих персональных данных в отдел кадров в течение 5 рабочих дней с даты их изменений.

3.14 Работник имеет право на:

- получение информации о своих персональных данных, сроках их хранения, а также о правовых основаниях и целях их обработки;
- полный доступ к своим персональным данным и получение копий любой записи, которая содержит персональные данные работника, кроме случаев, которые предусмотрены законодательством РФ;
- получение сведений о лицах (за исключением работников Оператора), имеющих доступ к персональным;
- требование об исправлении неполных или неверных персональных данных, об их исключении;
- требование об исключении персональных данных работника, обработанных с нарушением требований
- требование об извещении Оператором всех лиц, которым ранее были доведены неполные или неверные персональные данные работника, и обо всех произведенных в них исправлениях, дополнениях и исключениях;
- обжалование в судебном порядке любых неправомерных действий или бездействия Оператора, произведенных при обработке и защите его персональных данных.

3.15 При выявлении неправомерных действий с персональными данными или при их недостоверности, в случае обращения работника, Оператор обязан заблокировать персональные данные на период проверки. В случае выявления неправомерных действий с персональными данными, Оператор в срок, не превышающий трех рабочих дней с даты такого выявления, обязан устранить допущенные нарушения. При подтверждении факта недостоверности персональных данных Оператор, на основании документов, обязан уточнить персональные данные в течение семи рабочих дней со дня предоставления таких сведений.

4 Порядок обработки персональных данных без использования средств автоматизации

4.1 При обработке персональных данных, осуществляемой без использования средств автоматизации, персональные данные работников должны храниться обособлено от иной информации методом фиксации их на отдельные материальные носители ПДн (далее материальные носители).

4.2 При хранении ПДн на материальных носителях запрещается фиксация на одном материальном носителе ПДн с несовместимыми целями их обработки. Для обработки различных категорий ПДн для каждой категории ПДн должен выделяться отдельный материальный носитель.

4.3 Работники, которые осуществляют обработку ПДн без использования средств автоматизации, должны быть проинформированы о факте обработки ими ПДн, категориях обрабатываемых ПДн и о правилах и особенностях осуществления такой обработки, установленных федеральными законами.

4.4 При обработке ПДн без использования средств автоматизации их уточнение производится путем изменения или обновления данных на материальном носителе, а если это недопустимо в связи с техническими особенностями материального носителя, то путем фиксации на том же материальном носителе сведений об изменениях, которые в них внесены, или путем изготовления нового материального носителя с уточненными ПДн.

4.5 Доступ работников предприятия к ПДн осуществляется в соответствии с матрицей доступа работников, которые имеют доступ к ПДн, утвержденной на предприятии. Работники, имеющие доступ к ПДн, обязаны соблюдать режим конфиденциальности в отношении доступной им информации.

4.6 В рабочее время все документы, которые содержат ПДн, должны находиться на рабочих столах сотрудников только в течение необходимого на их обработку времени. В процессе обработки документов, содержащих

ПДн, они должны размещаться так, чтобы исключить возможность просмотра информации посторонними лицами.

4.7 Все мероприятия, проводимые лицами, которые не допущены к обработке ПДн, должны проходить в присутствии работника, постоянно работающего в нем.

4.8 В конце рабочего дня все документы, содержащие ПДн, должны быть убраны в предназначенные для этого сейфы или шкафы.

5 Доступ к персональным данным

5.1 Внешний доступ

5.1.1 К числу массовых потребителей персональных данных вне предприятия можно отнести следующие структуры:

- инспекции труда;
- пенсионные фонды;
- органы статистики;
- налоговые инспекции;
- правоохранительные органы;
- органы социального страхования;
- страховые агентства;
- военкоматы;
- подразделения муниципальных органов управления.

5.1.2 Органы по надзору имеют и осуществляют доступ к информации только в сфере своей компетенции и в порядке, установленном законодательством РФ.

5.1.3 Предоставление персональных данных работника родственникам или членам его семьи может быть осуществлено только с письменного разрешения работника.

5.1.4 Сведения о работающем или уволенном работнике могут быть представлены представителям другой организации только с письменного согласия владельца персональных данных, если иное не предусмотрено законодательством РФ.

5.2 Внутренний доступ

5.2.1 В пределах предприятия к разряду внутренних потребителей персональных данных относятся работники подразделений, которым эти данные необходимы для выполнения своих должностных обязанностей. Список должностей работников, которые имеют доступ к документам на

бумажных и электронных носителях, приведен приказе №834, утвержденным генеральным директором предприятия 19 июля 2011 года.

5.2.2 Оператор вправе разрешать работникам доступ к персональным данным. При этом должен быть заключен договор о неразглашении персональных данных между Оператором и работником, допущенным к персональным данным.

6 Передача персональных данных

6.1 В случаях передачи персональных данных работника Оператор должен соблюдать следующие требования.

6.1.1 Передача внешнему потребителю:

- запрещается сообщать в коммерческих целях персональные данные работника без его письменного согласия;
- передача персональных данных может осуществляться только в целях выполнения задач, которые соответствуют причине сбора этих данных, и в минимальных объемах;
- лица, которые получают персональные данные работника, должны быть проинформированы о том факте, что эти данные могут быть использованы только в целях, для которых они сообщены. Лица, которые получают персональные данные работника, обязаны обеспечивать соблюдение их конфиденциальности;
- ответы на письменные запросы других организаций даются только с разрешения генерального директора и только в письменной;
- не допускается отвечать по факсу или телефону на связанные с ПДн работников вопросы;
- при передаче внешним потребителям персональных данных работника Оператор должен получить письменное согласие работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы здоровью и жизни работника или в случаях, установленных ТК РФ и федеральными законами;
- при возможности передачи обезличенных данных персональные данные обезличиваются.

6.1.2 Передача внутреннему потребителю:

- передача персональных данных внутреннему потребителю осуществляется на основании договора о неразглашении, который заключается между Оператором и работником.

7 Уничтожение персональных данных

7.1 Персональные данные работников, которые завершили трудовые отношения с предприятием, хранятся в течение 1 месяца на бумажных носителях в отделе кадров и(или) в электронном виде в информационной системе персональных данных Оператора

7.2 По истечении данного срока:

- персональные данные, хранящиеся в информационной системе персональных данных Оператора, помещаются в архив средствами программного обеспечения.

- персональные данные, хранимые на бумажных носителях, передаются в архив предприятия;

7.3 Персональные данные в архиве хранятся в течение 75 лет. После истечения этого срока они подлежат уничтожению.

7.4 Документы, которые содержат ПДн работников и не помещены в архив, подлежат уничтожению в соответствии с законом РФ об архивном деле, Уничтожение бумажных носителей ПДн производится членами назначаемой приказом директора по персоналу и режиму комиссии в составе трех человек. Факт уничтожения бумажных носителей, которые содержат ПДн, оформляется актом (Приложение №3).

7.5 Документы в бумажном виде подвергаются уничтожению таким образом, чтобы обеспечить конфиденциальность содержащейся в них информации путем сожжения или измельчения.

8 Защита персональных данных

8.1 Защита персональных данных представляет собой регламентированный технологический процесс, направленный на обеспечение целостности, доступности и конфиденциальности персональных данных и обеспечивающий достаточно надежную безопасность информации в процессе производственной и управленческой деятельности предприятия. Защита персональных данных работника обеспечивается Оператором за счет его средств, с использованием организационных и технических мер, в порядке, установленном федеральными законами.

8.2 Защите подлежит:

- информация о персональных данных работника;
- персональные данные работника, которые содержатся на электронных и бумажных носителях информации;
- документы, содержащие персональные данные работника.

8.3 Защита от несанкционированного доступа, искажения и уничтожения информации, а также от иных неправомерных действий с информацией, направленных на нарушение свойств безопасности информации, которая хранится и обрабатывается в электронном виде, обеспечивается системой защиты персональных данных.

9 Внутренняя защита

Разработка матрицы доступа работников к персональным данным является основным направлением организационной защиты и предназначена для разграничения полномочий работников предприятия при доступе к информации. Для защиты персональных данных работников на предприятии должны соблюдаться следующие меры:

- наличие в помещениях, где производится хранение и обработка персональных данных, необходимых условий для работы с документами и базами данных, содержащими персональные данные;
- утверждение состава работников, для выполнения функциональных обязанности которых требуется доступ к персональным данным;
- размещение рабочих мест работников таким образом, чтобы исключить визуальный просмотр информации, составляющей персональные данные, посторонними лицами;
- знание работниками правил обработки персональных данных и требований организационно-распорядительных документов по защите информации;
- определение перечня работников, которые имеют право доступа в помещение, где производится хранение и обработка персональных данных;
- своевременное выявление угроз информационной безопасности и нарушений требований руководящих документов в области защиты персональных данных;
- проведение с работниками инструктажей по работе с персональными данными и разъяснительная работа по предупреждению утраты носителей персональных данных.

10 Внешняя защита

10.1 Для защиты персональных данных создаются условия, которые направлены на усложнение возможности несанкционированного доступа к ним посторонним лицом. Целью и результатом несанкционированного доступа к информационным ресурсам персональных данных могут являться уничтожение, модификация, хищение, подмена, внедрение вируса и т.д.

10.2 Под посторонним лицом понимается любое лицо, которое не состоит в штате и не имеет отношения к деятельности предприятия.

10.3 Посторонние лица не должны знать технологию составления, оформления документов и дел, содержащих персональные данные, порядок их ведения и хранения, а также распределение функций и рабочие процессы, связанные с обработкой персональных данных.

10.4 Для защиты персональных данных работников необходимо соблюдать следующие меры:

- соблюдение пропускного режима предприятия;
- порядок охраны территории, зданий, помещений, транспортных средств;
- порядок приема, учета и контроля деятельности посетителей;
- требования иных документов, регламентирующих правила работы с персональными данными на предприятии.

11 Ответственность

11.1 Ответственными за сбор, обработку и хранение персональных данных работников предприятия на электронных и бумажных носителях являются работники отдела кадров. Ответственными за обеспечение технической защиты и безопасности персональных данных являются работники группы по защите конфиденциальной информации отдела защиты информации. Ответственным за организацию обработки и защиты персональных данных работников АО «Радиозавод» является директор по персоналу и режиму.

11.2 Каждый работник предприятия, получающий для выполнения своих служебных обязанностей документы, которые содержат персональные данные, несет личную ответственность за сохранность носителя и конфиденциальность полученной информации.

11.3 Работник, разрешающий доступ третьего лица к конфиденциальному документу, несет персональную ответственность за данное разрешение.

11.4 За неисполнение или ненадлежащее исполнение работниками предприятия возложенных на них обязанностей по соблюдению установленного порядка работы с персональными данными работники несут персональную ответственность.

11.5 Работники, получившие доступ к персональным данным незаконными способами, несут персональную ответственность.

11.6 Работники, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут ответственность в соответствии с действующим законодательством.

Начальник отдела кадров

Т.Н. Потиханова

Начальник юридического отдела

А.М. Комякова

Начальник ОС и ОР

М.В. Монахов

Разработал:

Начальник отдела защиты информации

В.Б. Бородин

ЛИСТ

**ознакомления с «Положением об обработке и защите персональных данных работников АО
«Радиозавод»**

[illegible]

Согласие работника на обработку персональных данных

Настоящим для обеспечения трудовых отношений с АО «Радиозавод», во исполнение требований Трудового Кодекса Российской Федерации от 30.12.2001 № 197-ФЗ и Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» я, _____

(ФИО полностью)

паспорт _____ выдан _____
дата выдачи « ____ » _____ г.,
адрес регистрации (место жительства, место пребывания) _____

в своей воле и в своем интересе даю согласие на обработку АО «Радиозавод» (далее – Оператор), местонахождение в соответствии с Уставом – г. Пенза, ул. Байдукова, 1, моих персональных данных, включающих:

1. фамилию, имя, отчество, сведения о смене фамилии, перемене имени;
2. пол, дату, месяц и год рождения, место рождения;
3. гражданство, номер основного документа, удостоверяющего личность, сведения о дате выдачи указанного документа и выдавшем его органе;
4. место регистрации (место жительства, место пребывания);
5. фотографию;
6. сведения о стаже, предыдущей трудовой деятельности;
7. сведения о пенсионном и медицинском страховании;
8. сведения о воинском учете (воинское звание, состав рода войск, сведения о постановке/снятии на (с) учет(а) и прохождении срочной службы) и подтверждающих документах;
9. сведения об образовании, квалификации, наличии специальных знаний или специальной подготовки, повышении квалификации и переподготовке, наличии ученой степени, ученого звания и документе его подтверждающем;
10. сведения о результатах медицинского осмотра (обследования), психиатрического освидетельствования, медицинского заключения, в том числе о наличии и группе инвалидности;
11. сведения о документах, подтверждающих семейное положение;
12. сведения о несовершеннолетних членах семьи в возрасте до 14 лет (фамилию, имя, отчество, пол, дату, месяц и год рождения, место рождения, место и дату регистрации, место регистрации (место жительства, место пребывания), свидетельство о рождении ребенка (детей), информацию о смене фамилии, перемене имени, состоянии здоровья);
13. сведения о наличии судимости и (или) факте уголовного преследования либо о прекращении уголовного преследования по реабилитирующим основаниям;
14. должность (профессию);
15. номера телефонов (мобильного и/или домашнего), адрес личной электронной почты;
16. сведения о заработной плате (должностном окладе, доплатах и надбавках стимулирующего и компенсационного характера, о налогах);
17. номер лицевого счета в банке;
18. сведения о заработной плате с предыдущих мест работы (данные справки 2-НДФЛ);
19. сведения о документах, подтверждающих социальный статус.

Цель обработки персональных данных – обеспечение соблюдения законов и иных нормативных актов, организация и ведение кадрового учета содействие работникам в трудоустройстве, обучении и продвижении по службе, обеспечение личной безопасности работников, контроль количества и качества выполняемой работы, обеспечение сохранности имущества, а также предоставление различных льгот и видов материального обеспечения в соответствии с действующим законодательством Российской Федерации: Трудовым кодексом Российской Федерации, Налоговым кодексом Российской Федерации, обеспечение страхования на основании Федерального закона «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования» и Федерального закона «Об обязательном социальном страховании на случай временной нетрудоспособности и в связи с материнством», а также Уставом Оператора.

Согласие дается на обработку персональных данных, т.е. на следующие действие: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных, осуществляемые без использования средств автоматизации и с использованием персонального компьютера при непосредственном участии человека, при обязательном соблюдении требований конфиденциальности моих персональных данных, а также на передачу персональных данных третьим лицам в случае, предусмотренных федеральными законами, на основании договоров, с использованием персонального компьютера или по каналам связи с соблюдением мер, обеспечивающих их защиту от несанкционированного доступа при условии, что их прием и обработка будут осуществляться лицом, обязанным сохранять требования конфиденциальности персональных данных.

Дополнительно даю согласие на публикацию в общедоступных источниках фотографии в соответствии со ст. 152.1 Гражданского кодекса РФ.

Я согласен(а), что мои персональные данные, в предусмотренных законодательством Российской Федерации пределах, будут передаваться третьим лицам: представителям банка, обслуживающего Оператора, для обеспечения выплаты заработной платы, Государственного Учреждения – отделения Пенсионного фонда РФ в Пензенской области, для пенсионного обеспечения, Инспекции Федеральной налоговой службы России в Пензенской области, для исполнения обязанности по уплате налогов, страховой медицинской компании, для обеспечения выплат по медицинскому страхованию, военных комиссариатов Пензенской области и г. Пензы и других городов, представителям иных организаций для решения задач, связанных с трудовыми отношениями с Оператором.

Настоящее соглашение действует в течении срока трудового договора. Обработка моих персональных данных должна быть прекращена по достижении заявленных целей обработки.

Я оставляю за собой право отозвать согласие на обработку персональных данных посредством составления соответствующего письменного документа, который может быть направлен мной в адрес Оператора по почте заказным письмом с уведомлением о вручении либо вручен лично под расписку уполномоченному представителю Оператора.

В случае отзыва субъектом персональных данных согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в (ч. 2 ст. 9 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»).

(ФИО (полностью) субъекта персональных данных)

(подпись)

« ____ » _____ 20 ____ г. Примечание: согласие хранится в личном деле работника.

«Утверждаю»

Директор по персоналу и режиму

_____ С.Г. Викторов

« ____ » _____ 20 ____ г.

3313

АКТ

уничтожения документов

Комиссия в составе:

— председатель комиссии _____

— члены комиссии _____

составила настоящий акт о том, что документы АО «Радиозавод», содержащиеся в приведенном ниже перечне, были полностью уничтожены

« ____ » _____ 20 ____ г. в ____ часов ____ минут в нашем присутствии.

№ п/п	Годы документов и дел	Заголовки документов и дел (групповые или индивидуальные)	Кол-во документов и дел с перечнем страниц	Примечание
1				
2				

Председатель комиссии:

(должность)

(подпись)

(расшифровка)

Члены комиссии:

(должность)

(подпись)

(расшифровка)

(должность)

(подпись)

(расшифровка)

Приложение Д

(обязательное)

Техническое задание на информационную систему персональных данных
«Кадры» предприятия АО «Радиозавод»

«Согласовано»

Директор по персоналу и режиму

_____ С.Г. Викторov

« ____ » _____ 2018г

«Утверждаю»

Генеральный директор

_____ А.Г. Быстров

« ____ » _____ 2018г

ТЕХНИЧЕСКОЕ ЗАДАНИЕ ИСПДн «Кадры»
предприятия АО «Радиозавод»

г. Пенза
2018 г.

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АРМ	Автоматизированное рабочее место
СВТ	Средство вычислительной техники
ИБ	Информационная безопасность
ИС	Информационная система
ИСПДн	Информационная система персональных данных
МЭ	Межсетевой экран
НСД	Несанкционированный доступ
ОС	Операционная система
ПДн	Персональные данные
ПО	Программное обеспечение
РД	Руководящий документ
САЗ	Средства анализа защищенности
СЗИ	Средство защиты информации
СЗПДн	Система защиты персональных данных
СМИО	Сеть международного информационного обмена
ФЗ	Федеральный закон
ПИБ	Проект информационной безопасности
ЛВС	Локально-вычислительная сеть

1 Назначение и цели создания ПИБ и СЗПДн

1.1 Назначение СЗПДн

1.1.1 Назначением ПИБ и СЗПДн является техническое и организационное обеспечение мероприятий, требуемых ст.19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

1.1.2 СЗПДн должна обеспечить конфиденциальность, целостность, доступность и иные свойства информации ПДн при их обработке в ИСПДн.

1.1.3 Назначением систем, которые проектируются на основании настоящего проекта является защита ПДн локальной ИСПДн, не подключенной к сетям международного информационного обмена.

1.2 Цели создания СЗПДн

1.2.1 Целями создания СЗПДн являются:

- соответствие требованиям обеспечения информационной безопасности, регламентируемым РД ФСТЭК России и ФСБ России, при обработке ПДн в ИСПДн,;

- обеспечение защиты ПДн в процессе хранения и обработке в ИСПДн.

1.2.2 Критериями оценки достижения поставленных целей по созданию СЗПДн являются:

- соответствие требованиям по обеспечению безопасности ПДн в ИСПДн в соответствии с приказом ФСТЭК от 18 февраля 2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

- выполнение функциональных требований настоящего проекта.

1.2.3 Подтверждением соответствия достигнутых результатов заданным целям в рамках настоящего проекта, является аттестация ИСПДн на соответствие требованиям безопасности информации.

2 Характеристика объекта защиты (ИСПДн)

Описание ИСПДн

Объектом защиты являются ПДн, обрабатываемые в локальной ИСПДн не подключенной к СММО. Обработка ПДн в ИСПДн осуществляется с использованием средств автоматизации. В составе ИСПДн функционирует 33 АРМ и 3 сервера. Все компоненты ИСПДн находятся на одном объекте. Обработка персональных данных ведется в многопользовательском режиме, с разграничением прав доступа. Все технические средства находятся в пределах РФ. Объем обработки персональных данных не превышает 100 000 записей о субъектах ПДн. При входе в систему и выдаче запросов на доступ проводится аутентификация пользователей ИСПДн. Все пользователи имеют собственные роли: администратор безопасности, пользователи с правом чтения-записи, пользователи с правом чтения данных.

3 Требования к СЗПДн

3.1 Общие требования к СЗПДн

В состав СЗПДн должны входить следующие подсистемы:

- управления доступом;
- регистрации и учета;
- антивирусной защиты;
- обеспечения целостности;
- обеспечения межсетевой безопасности.

3.1.1 Ввиду отсутствия в ИСПДн подключения к сетям международного информационного обмена из рассмотрения исключены подсистемы криптографической защиты, анализа защищенности и обнаружения атак.

3.1.2 Подсистема управления доступом должна проводить процедуры идентификации пользователя, его авторизации и осуществлять разграничение доступа пользователей к ресурсам ИСПДн на основании утвержденной матрицы доступа.

3.1.3 Подсистема регистрации и учета должна обеспечивать регистрацию действий пользователей в ходе работы с ресурсами ИСПДн и учет событий ИБ.

3.1.4 Подсистема обеспечения целостности должна обеспечивать контроль целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды.

3.1.5 Подсистема антивирусной защиты должна осуществлять защиту информационных ресурсов ИСПДн от внедрения вредоносного ПО. Подсистема антивирусной защиты должна быть направлена на нейтрализацию угроз внедрения вредоносного ПО в системное и прикладное ПО, а также на обход СЗИ.

3.1.6 Подсистема обеспечения межсетевой безопасности должна обеспечивать безопасное межсетевое взаимодействие систем внутри сети.

3.1.7 Требования к численности и квалификации персонала

Квалификация и численность персонала должны быть достаточны для осуществления ими своих обязанностей, настройки используемых прикладных, сетевых и общесистемных сервисов ИСПДн, а также настройки СЗИ. Персонал ИСПДн должен осуществлять обслуживание и эксплуатацию ИСПДн в рабочее время.

3.1.8 Требования к надежности

Компоненты СЗПДн должны быть рассчитаны на функционирование в режиме круглосуточной работы и позволять осуществлять восстановление системы после сбоев и процедуру резервного копирования.

3.1.9 Требования безопасности

В процессе эксплуатации и обслуживания оборудования СзПДн должна обеспечиваться безопасность персонала. Конструкция оборудования, используемого персоналом, должна обеспечивать защиту от поражения электрическим током.

3.1.10 Требования по сохранности информации при авариях

Должна обеспечиваться сохранность информации при авариях в ИСПДн путем резервного копирования.

3.1.11 Требования к защите от влияния внешних воздействий

Защита от внешних воздействий информации, обрабатываемой в ИСПДн, должна осуществляться в рамках организационно-технических мероприятий по физической защите и обеспечению безопасности на объектах размещения СВТ ИСПДн.

3.1.12 Требования к защите патентов

При проектировании и эксплуатации СзПДн должны соблюдаться положения законодательных актов Российской Федерации по соблюдению авторских прав.

3.1.13 Требования по стандартизации и унификации

В СзПДн должны использовать однотипные компоненты для снижения расходов на обслуживание и ремонт, удобства эксплуатации и взаимозаменяемости компонентов. Должна обеспечиваться совместимость технических средств и ПО, используемыми в ИСПДн, с техническими средствами и ПО СзПДн.

3.2 Требования к выполняемым системой функциям

3.2.1 В подсистеме управления доступом:

- должна осуществляться идентификация пользователей и проверка подлинности субъектов доступа при входе в систему по паролю, длиной не менее восьми символов;
- должно обеспечиваться управление правами субъектов доступа и разграничение доступа субъектов к объектам доступа на основании правил разграничения доступа.

3.2.2 В подсистеме регистрации и учета:

- должна осуществляться регистрация загрузки операционной системы, входа субъектов в систему и их выхода из системы. В параметрах

регистрации указываются идентификатор субъекта, дата и время входа в систему и выхода из нее, дата загрузки системы, результат попытки входа;

- должен проводиться учет всех носителей информации с присвоением им идентификатора и занесением данных в журнал.

3.2.3 В подсистеме обеспечение целостности:

- должна быть обеспечена целостность программных средств защиты информации в составе СЗПДн и неизменность программной среды. Целостность СЗИ проверяется при загрузке системы, а целостность программной среды достигается путем исключения средств модификации объектного кода программ в процессе хранения и обработки ПДн;

- должно проводиться периодическое тестирование функций СЗПДн с применением тест-программ, имитирующих попытки НСД;

- должна осуществляться физическая охрана технических средств и носителей информации, используемых в ИСПДн, которая предусматривает исключение несанкционированного доступа в помещения, где расположены элементы ИСПДн, посторонних лиц, и хранилище носителей информации, особенно в нерабочее время;

- помещения, в которых функционируют СВТ, входящие в ИСПДн, должны быть оборудованы средствами, исключающими несанкционированный просмотр информации с устройств вывода информации.

3.2.4 В подсистеме антивирусной защиты:

- должны использоваться средства антивирусной защиты, позволяющие обеспечивать обнаружение компьютерных программ, предназначенных для несанкционированного блокирования, уничтожения, копирования или модификации информации, либо нейтрализации СЗИ.

3.2.5 В подсистеме межсетевой безопасности

Сегмент сети, в котором функционируют ИСПДн, должен быть обособлен от ЛВС предприятия с помощью применения персонального распределенного межсетевого на всех СВТ, входящих в состав ИСПДн.

МЭ должен обеспечивать:

- фильтрацию пакетов служебных протоколов, которые предназначены для диагностики и управления работой сетевых устройств;
- фильтрацию сетевых пакетов;
- регистрацию и учет фильтруемых пакетов (время, адрес и результат фильтрации);
- регистрацию запуска процессов и программ;
- контроль целостности информационной и программной части;
- тестирование процесса контроля за целостностью программной и информационной части и процедуры восстановления, а также процесса реализации правил фильтрации;
- восстановление работоспособности межсетевого экрана после отказов или сбоев оборудования.

3.3 Требования к программному обеспечению

3.3.1 Должны использоваться СЗИ от НСД, сертифицированные по требованиям безопасности информации.

3.3.2 При создании СЗПДн и в процессе эксплуатации ИСПДн должно использоваться только лицензионные операционные системы и программное обеспечение.

3.4 Этапы создания

Процесс создания СЗПДн проходит в несколько этапов:

- разработка внутренней нормативной документации в области защиты ПДн;
- приобретение, установка и настройка СЗИ;
- обучение персонала предприятия нормативным документам и работе с СЗИ;
- опытная эксплуатация СЗПДн;
- сдача СЗПДн в рабочую эксплуатацию;
- аттестация ИСПДн.

4 Основные требования к средствам защиты

В состав системы защиты должны быть включены следующие средства:

- средства идентификации (опознавания) и аутентификации (подтверждения подлинности) пользователей ИСПДн;
- средства разграничения доступа пользователей и обслуживающего персонала к информационным ресурсам ИСПДн;
- средства резервирования технических средств, дублирование массивов и носителей информации;
- средства антивирусной защиты;
- средства межсетевого экранирования с целью обеспечивать безопасное межсетевое взаимодействие;
- средства блокирования использования съемных носителей и накопителей информации.

5 Мероприятия по подготовке к вводу в действие СЗПДн

На этапе ввода СЗПДн в эксплуатацию должны обеспечиваться следующие меры:

- определение перечня лиц, которые допущены к обработке ПДн, обрабатываемых в ИСПДн;
- разграничение прав доступа в помещения, где находятся элементы ИСПДн, должно регламентироваться внутренними организационно-распорядительными документами;
- определение ПДн, циркулирующего в ИСПДн;
- подключение к источникам бесперебойного питания компонентов СЗПДн;
- оборудование серверных помещений средствами пожарной сигнализации и средствами пожаротушения, а также системами вентиляции и кондиционирования воздуха.

Начальник ОЗИ _____ В.Б. Бородин

Инженер ОЗИ _____ Д.Д. Березин

Приложение Е

(обязательное)

Частная модель угроз

безопасности персональных данных в информационной системе

персональных данных «Кадры» АО «Радиозавод»

СОГЛАСОВАНО

Директор по персоналу и режиму

_____ С.Г. Викторов

«__» _____ 2018

УТВЕРЖДАЮ

Генеральный директор

_____ А.Г. Быстров

«__» _____ 2018

ЧАСТНАЯ МОДЕЛЬ УГРОЗ

безопасности персональных данных в информационной системе

персональных данных «Кадры» АО «Радиозавод»

2018 г.

1 Общие положения

Частная модель угроз безопасности персональных данных (далее- Модель) в информационной системе персональных данных «Кадры» АО «Радиозавод» (далее-ИСПДн) определяет актуальные угрозы безопасности персональных данных при их обработке в ИСПДн.

Нормативно-правовой основой для разработки настоящей модели угроз являются следующие нормативные и методические документы РФ:

Для разработки модели угроз использовались следующие нормативные и методические документы, стандарты:

- Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

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

- Методический документ ФСТЭК России «Методика определения угроз безопасности информации в информационных системах»

- Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

Модель угроз формируется и утверждается оператором и может быть пересмотрена:

- по решению оператора на основании результата проводимых анализа и оценки угроз безопасности персональных данных с учетом особенностей информационной системы или изменений в ее структуре;

- в результате проведения мероприятий по контролю за выполнением требований к обеспечению безопасности персональных данных при их обработке в информационной системе.

2 Описание информационной системы и особенностей её функционирования

2.1 Общие сведения

Предприятие АО «Радиозавод» расположено по адресу 440039 г. Пенза, ул. Байдукова 1. На его территории размещено 9 кирпичных корпусов и несколько служебных построек, находящихся в пределах КЗ. Система отопления зданий подключена к котельной, расположенной на территории предприятия. На АО «Радиозавод» действует контрольно-пропускной режим, исключая неконтролируемое пребывание на территории посторонних лиц. Все внутренние телефоны предприятия, в том числе имеющие выход в город, подключены к мини АТС, находящейся в пределах КЗ. Линии электропитания, проходящие по территории завода, подключены к электроподстанции находящейся в пределах КЗ. На территории предприятия установлены камеры видеонаблюдения.

2.2 Цель и задачи, решаемые информационной системой

Целью обработки ПДн является:

- управление персоналом;
- систематизация данных о работниках предприятия;
- производство расчётов заработных плат и пенсионных отчислений;

К функциям, которые реализуются с помощью ИСПДн «Кадры» АО «Радиозавод», относятся:

- прием сотрудника на работу;
- увольнение работника;
- начисление работнику заработной платы.

2.3 Описание структурно-функциональных характеристик информационной системы

Информационная структура предприятия представляет собой локально-вычислительную сеть. ЛВС предприятия логически разделена на два сегмента: общий, в котором функционируют СВТ, не входящие в ИСПДн, и

сегмент ИСПДн, в котором функционируют объекты ИСПДн. Разделение осуществляется с использованием межсетевых экранов ViPNet Personal Firewall 4. В ИСПДн обеспечивается хранение, обработка и анализ информации о подразделениях и сотрудниках предприятия. ИСПДн предназначена для решения задач управления персоналом. В состав ИСПДн предприятия входят 33 АРМ сотрудников, ERP система «Галактика» и контролер домена. Хранение персональных данных осуществляется на сервере «Галактика» в отдельных БД «Зарплата» и «Кадры». СВТ, входящие в состав ИСПДн.

В ЛВС предприятия входят рабочие места системного администратора и администратора безопасности, которые подключены в общем сегменте. Рабочее место администратора безопасности предназначено для анализа защищенности операционных систем СВТ ИСПДн и прикладного программного обеспечения. Каждый из компьютеров, входящих в состав ИСПДн, является членом домена Active Directory. На контролере домена развернуты основные службы (DHCP, DNS, Active Directory).

Доступ к сети интернет отсутствует, все средства функционируют в рамках локальной сети.

В процессе обработки персональных данных в ИСПДн используются следующие технологии:

- персональные данные хранятся и обрабатываются в специально предназначенной для этого ERP системе «Галактика»;
- временное хранение ПДн в малых объемах возможно на АРМ сотрудников предприятия, входящих ИСПДн.

Схема конфигурации ИСПДн организации представлена на рисунке 1.

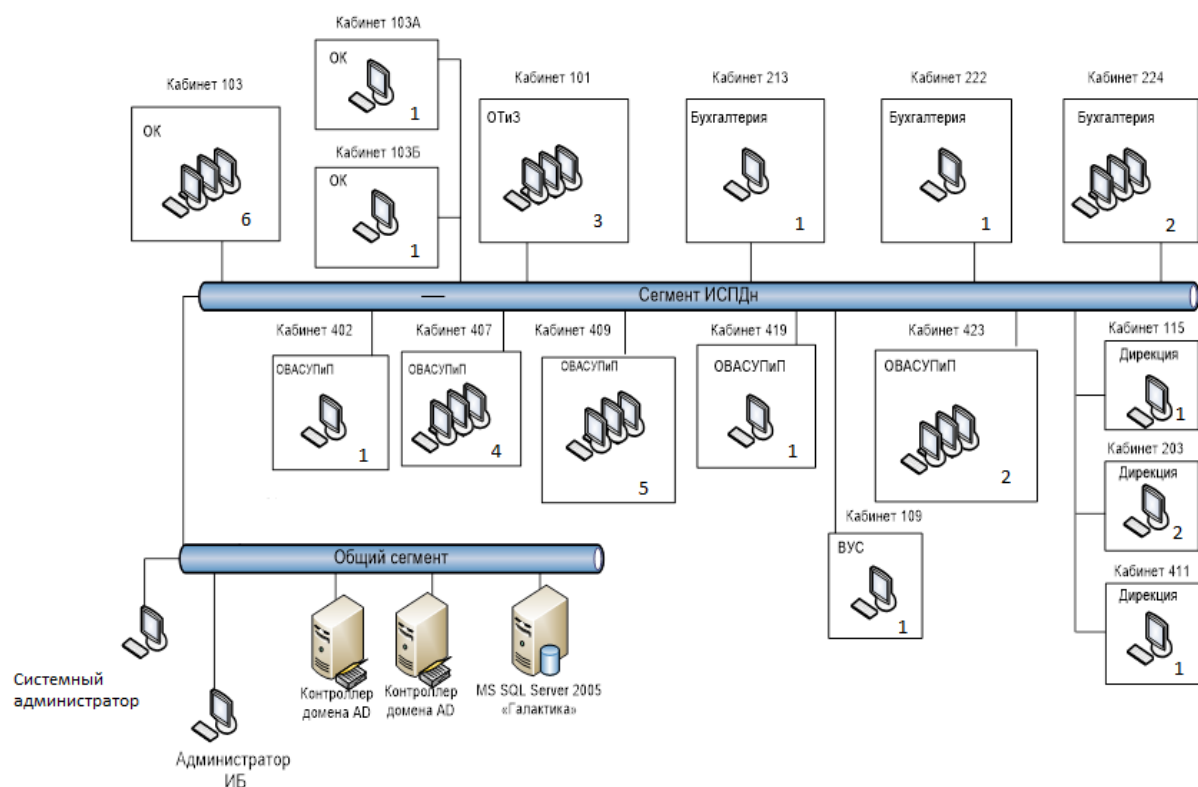


Рисунок 1 – Схема конфигурации ИСПДн

2.4 Состав персональных данных, обрабатываемых в информационной системе персональных данных

В ИСПДн обрабатываются следующие персональные данные:

- фамилия, имя, отчество работника;
- дата и место рождения работника;
- паспортные данные;
- адрес проживания (регистрации) работника;
- домашний телефон;
- семейное, социальное, имущественное положение работника;
- место работы или учебы членов семьи и родственников;
- сведения об образовании;
- сведения о заработной плате работника;
- сведения о социальных льготах;
- сведения о наличии судимостей;

- занимаемая должность, специальность и профессия;
- сведения о трудовом стаже;
- сведения о предыдущем месте работы;
- сведения о воинском учете;
- сведения, которые содержатся в трудовом договоре.

3 Возможности нарушителей (модель нарушителя)

3.1 Типы, вид и потенциал нарушителей

Типа виды и соответствующий потенциал нарушителей:

- физические лица (Внешний) - низкий потенциал;
- лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора (Внутренний) - низкий потенциал;
 - пользователи информационной системы (Внутренний) - низкий потенциал;
 - разработчики, производители, поставщики программных, технических и программно-технических средств (Внешний) - средний потенциал;
 - бывшие работники (Внешний) - низкий потенциал.

Администраторы ИС и администраторы безопасности выполняют функции по администрированию баз данных ИСПДн, поддерживают работоспособность систем в составе ИСПДн и обеспечивают их взаимодействие. Эти лица могут реализовывать угрозы информационной безопасности, используя свои привилегии для доступа к хранимой и обрабатываемой защищаемой информации, программным и техническим средствам, участвующим в обработке ПДн, а также к средствам защиты.

Администраторы ИС и администраторы безопасности осведомлены о протоколах и алгоритмах, используемых в ИСПДн и ее подсистемах, а также о концепции безопасности и используемых мерах защиты. Предполагается, что для реализации угроз или идентификации уязвимостей они могут

использовать штатное оборудование, оборудование, полученное из внешних общедоступных источников (например, программное обеспечение), или специализированное оборудование.

К этим лицам, в связи с их ролью в ИСПДн, применяются особые меры, включающие тщательный подбор кандидата при принятии на работу и назначению на должность, а также контроль за выполнением своих обязанностей.

Предполагается, что назначаться на должности Администратора ИС и администратора безопасности будут только доверенные лица, поэтому они исключаются из числа вероятных нарушителей.

3.2 Возможные цели нарушителей

Цели нарушителей:

- причинение имущественного ущерба путем мошенничества или иным преступным путем;
- выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды;
- идеологические или политические мотивы;
- причинение имущественного ущерба путем обмана или злоупотребления доверием;
- непреднамеренные, неосторожные или неквалифицированные действия;
- месть за ранее совершенные действия.

3.3 Возможные способы реализации угроз безопасности информации

Для физических лиц существует способ реализации угроз БИ в виде несанкционированного физического доступа и (или) воздействия на линии, (каналы) связи, технические средства, машинные носители информации

Для лиц, обеспечивающих функционирование информационных систем или обслуживающих инфраструктуру оператора (администрация, охрана, уборщики и т.д.), существуют следующие способы реализации угроз БИ:

- несанкционированный физический доступ и (или) воздействие на линии, (каналы) связи, технические средства, машинные носители информации;

- несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы).

Для пользователей информационной системы существуют следующие способы реализации угроз БИ:

- несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, web-приложения, иные прикладные программы общего и специального назначения);

- несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы).

Для разработчиков, производителей, поставщиков программных, технических и программно-технических средств существуют следующие способы реализации угроз БИ:

- несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, web-приложения, иные прикладные программы общего и специального назначения);

- несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы);

- несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы).

Для бывших работников (пользователей) существует способ реализации угрозы БИ в виде воздействия на пользователей,

администраторов безопасности, администраторов информационной системы или обслуживающий персонал (социальная инженерия)

4 Актуальные угрозы безопасности информации

Описание актуальных угроз БИ для ИСПДн «Кадры» АО «Радиозавод», которое включает наименование угрозы, уязвимости ИСПДн, объекты воздействия, последствия от реализации угрозы, а также способы реализации угрозы, приведено в таблице 1.

Таблица 1 – Описание актуальных угроз БИ

Наименование угрозы	Источник угрозы	Уязвимость	Способ реализации	Последствия
Угроза утечки через порты ввода/вывода	Лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора	Отсутствие контроля за подключением неучтенных съемных носителей	Угроза реализуется внутренними нарушителями путем несанкционированного копирования информации на подключенные к компьютерам съемные носители информации.	Нарушение конфиденциальности
	пользователи информационной системы			
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	пользователи информационной системы	Отсутствие у пользователей инструкций, описывающих порядок работы с ПДн, и неосведомленность об ответственности за их нарушение.	Угроза реализуется за счет человеческого фактора путем несанкционированных действий пользователями ИСПДн, направленных на разглашение, модификацию и уничтожение информации.	Нарушение конфиденциальности, целостности и доступности
	бывшие работники			
Установка ПО, не связанного с исполнением служебных обязанностей	пользователи информационной системы	Отсутствие положений, регламентирующих работу в ЛВС. Отсутствие контроля за подключением неучтенных съемных носителей.	Угроза реализуется внутренним нарушителем путем установки ПО, не связанного с исполнением им служебных обязанностей, что может привести к нарушению конфиденциальности, целостности и доступности информации, а также нарушению работы технических средств ИСПДн.	Нарушение конфиденциальности, целостности, доступности

Продолжение таблицы 1

Наименование угрозы	Источник угрозы	Уязвимость	Способ реализации	Последствия
Угрозы внедрения вредоносных программ	разработчики, производители, поставщики программных, технических и программно-технических средств	Отсутствие мер антивирусной защиты	Угроза реализуется путем внедрения со съемных носителей вредоносных программ, которые могут разрушать код программ в оперативной памяти, самодублироваться, выполнять без участия пользователя деструктивные функции, искажать, дублировать, блокировать информацию.	Нарушение конфиденциальности, целостности, доступности
	пользователи информационной системы			
Угроза перехвата управления загрузкой	пользователи информационной системы	Отсутствие ограничения доступа к BIOS. Отсутствие контроля за подключением неучтенных съемных носителей.	Угроза реализуется внутренним нарушителем путем перехвата управления загрузкой для загрузки ОС с отчуждаемых носителей для получения НСД к ИСПДн.	Нарушение конфиденциальности, целостности, доступности.
	лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора			

Приложение Ж

(обязательное)

Инструкция администратора информационной безопасности информационной системы персональных данных

УТВЕРЖДАЮ

Директор по персоналу и
режиму

_____ С.Г. Викторов

«___» _____ 2018 г.

ИНСТРУКЦИЯ

администратора информационной безопасности информационной системы персональных данных

Введена в действие с _____

1 Список используемых сокращений

ИБ – информационная безопасность.

ИСПДн – информационная система персональных данных.

АС – автоматизированная система.

ПЭВМ – персональная электронно-вычислительная машина.

НСД – несанкционированный доступ.

СЗИ – средство защиты информации.

2 Общие положения

Инструкция определяет основные функции, права и обязанности администратора ИБ АС в области обеспечения информационной безопасности при эксплуатации и сопровождении ИСПДн.

Настоящая Инструкция является руководящим документом администратора ИБ АС.

Администратор ИБ назначается из числа сотрудников отдела защиты информации, имеющих высшее профильное образование, и обеспечивает бесперебойное функционирование установленных СЗИ от НСД. Администратор ИБ подчиняется непосредственно начальнику отдела защиты информации. При выполнении своих должностных обязанностей администратор ИБ руководствуется инструкциями по эксплуатации СЗИ, данной инструкцией и другими ОРД, регламентирующими работу с ПДн, утвержденными на предприятии.

Для обеспечения бесперебойной работы СЗИ от НСД в ИСПДн назначаются два администратора информационной безопасности (с целью замещения в случае временного отсутствия одного из администраторов).

3 Квалификационные требования и необходимый уровень знаний

Администратор ИБ должен обладать:

- высшим профильным образованием или пройти курсы повышения квалификации в области администрирования СЗИ от НСД;
- всей полнотой знаний о ИСПДн и её структуре.

Администратор ИБ должен знать:

- основные положения документов ФСТЭК и ФСБ, федеральных законов и распоряжений вышестоящих организаций, которые регламентируют порядок работы и защиту ПДн и другой конфиденциальной информации;
- внутренние ОРД, регламентирующие порядок защиты и работы с ПДн и другими сведениями конфиденциального характера;

- принципы администрирования и эксплуатации СЗИ от НСД, которые применяются в ИСПДн.

4 Обязанности администратора ИБ

Администратор информационной безопасности совместно со специалистами по информационным технологиям:

- контролирует целостность программных и аппаратных средств, а также хранимой и обрабатываемой информации;
- обеспечивает корректную работу подсистем управления доступом, регистрации и учета информационных ресурсов;
- обеспечивает доступность и конфиденциальность хранимой, обрабатываемой и передаваемой по каналам связи информации.

На администратора безопасности возлагаются следующие обязанности:

- совместно со специалистами по информационным технологиям обеспечивать разграничение доступа пользователей к защищаемой информации в соответствии с утвержденной матрицей доступа;
- следить за сохранностью пломб на корпусах ПЭВМ;
- знать уровень защищенности ИСПДн и следить соблюдением технологии обработки информации и за тем, чтобы обработка информации производилась только с использованием учтенных носителей информации;
- контролировать соблюдение пользователями требований ОРД;
- контролировать соблюдение требований по учету и хранению носителей конфиденциальной информации и персональных данных;
- проводить полную антивирусную проверку ПЭВМ в ИСПДн не реже 1 раза в квартал;
- осуществлять контроль монтажа оборудования специалистами сторонних организаций, который производится на защищаемом объекте организации;
- участвовать в проверках и испытаниях ИСПДн;

- незамедлительно докладывать руководителю отдела защиты информации об обнаруженных попытках НСД к информации ограниченного доступа;
- осуществлять не реже одного раза в месяц обновление антивирусных баз на ПЭВМ в ИСПДн;
- при изменении конфигурации системы вносить соответствующие изменения в паспорт ИСПДн;
- проводить не реже одного раза в год контроль выполнения требований защиты информации ограниченного доступа;
- участвовать в приемке новых программных средств, эксплуатация которых планируется в ИСПДн;
- вести журнал учета работы с ИСПДн. Форма журнала регистрации представлена в приложении 1.

Регистрации в журнале учета работ ИСПДн подлежат:

- некорректная работа прикладных и системных программных средств, которая затрудняет эксплуатацию ПЭВМ;
- выход из строя или некорректная работа узлов ПЭВМ или периферийных устройств;
- обновление антивирусных баз;
- обновление программного обеспечения, используемого в ИСПДн;
- вскрытие ПЭВМ с указанием цели вскрытия и проводимых работ;
- создание резервных копий с носителей информации;
- перебои в системе электроснабжения;
- замена системного блока с указанием факта гарантированного удаления информации с жесткого диска.

При выявлении фактов утечки информации администратор ИБ обязан немедленно приостановить работу в ИСПДн.

При выявлении нарушений конфиденциальности или целостности защищаемой информации администратор ИБ обязан в письменной форме доложить об этом руководителю отдела защиты информации и занести соответствующую запись в журнал учета работы ИСПДн, описав факт нарушения, предпринятые рекомендуемые им действия.

5 Права администратора ИБ

Администратор информационной безопасности имеет право:

- требовать от работников организации соблюдения технологии обработки ПДн, установленной на предприятии, и исполнения ОРД, которые регламентируют обработку и защиту информации;
- участвовать в анализе ситуаций, которые связаны с функционированием СЗИ, и расследованиях попыток или фактов НСД;
- требовать от пользователей ИСПДн прекращения обработки информации в случае:
 - нарушения порядка работ, установленного на предприятии;
 - нарушения работоспособности технических средств, входящих в состав ИСПДн, и систем защиты информации.
- получения информации о возможном проведении технической разведки в отношении объекта;
- окончания срока действия сертификатов соответствия ФСТЭК России.

6 Ответственность

Администратор безопасности несет ответственность за своевременность и качество выполнения функций и задач, возложенных на него в соответствии с настоящей инструкцией. Роспись работника в листе ознакомления с инструкцией означает его согласие и обязательство исполнения (Приложение №2).

Начальник ОЗИ

Руководитель группы логистики

Инженер ОЗИ

В.Б. Бородин

М.В. Монахов

Д.Д. Березин

ЛИСТ

**ознакомления с инструкцией администратора
информационной безопасности ИСПДн**

№ п/п	Фамилия, имя, отчество работника	Дата и подпись работника после ознакомления с инструкцией

Приложение И

(обязательное)

Инструкция пользователя информационной системы персональных данных

«Утверждаю»

Генеральный директор

_____ А.Г. Быстров

«__» _____ 2018 г.

ИНСТРУКЦИЯ

пользователя информационной системы персональных данных на
предприятии АО «Радиозавод»

1 Общие положения

1.1 Настоящая Инструкция разработана для организации защиты информации при обработке персональных данных в АО «Радиозавод» (далее – Предприятие) и регламентирует обязанности сотрудников, которые участвуют в процессах автоматизированной обработки информации, а также имеют доступ к программным и аппаратным средствам, с использованием которых осуществляется обработка персональных данных (далее – Пользователи).

1.2 Пользователь несет персональную ответственность за свои действия.

1.3 Методическое руководство работой пользователя осуществляется Администратором локальной вычислительной сети и Администратором безопасности.

2 Обязанности работников, имеющих доступ к ПДн.

2.1 Работники, которые получили доступ к персональным данным, обязаны обеспечивать их конфиденциальность и пресекать действия других лиц, которые могут привести к разглашению такой информации. О таких фактах или возможной утечке персональных данных необходимо немедленно информировать руководителя структурного подразделения.

2.2 Персональные данные не подлежат разглашению. Прекращение доступа к такой информации не освобождает сотрудника от взятых им обязательств по неразглашению.

2.3 В случае оставления занимаемой должности работник обязан вернуть все документы и материалы, относящиеся к деятельности подразделения, организации, а также копии данных материалов, если таковые имеются.

Пользователь обязан:

2.4 Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, регламентирующих порядок действий по обработке и защите персональных данных.

2.5 Знать и соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами информационной системы персональных данных, которые установлены на его рабочем месте.

2.6 Соблюдать требования парольной политики.

2.7 Использовать для работы только учтенные носители информации.

2.8 Немедленно ставить в известность руководителя подразделения или специалиста отдела по защите информации:

- в случае утери носителя с персональными данными;
- при компрометации личных паролей;

- в случае нарушений целостности пломб на аппаратных средствах, используемых в ИСПДн, или иных фактов, которые указывают на совершение попыток несанкционированного доступа к элементам ИСПДн;
- при некорректной работе технических и программных средств, используемых на АРМ, а также при перебоях в системе электроснабжения;
- в случае обнаружения дополнительных устройств, подключенных к АРМ;
- при обнаружении несанкционированных изменений в конфигурации программных или аппаратных средств ИСПДн.

2.9 Уборка помещений должна проводиться только в присутствии работника, имеющего доступ в помещение.

2.10 АРМ, используемые для работы с персональными данными, должны быть размещены таким образом, чтобы исключалась возможность визуального просмотра экрана видеомонитора, не имеющими отношения к конкретно обрабатываемой информации работниками.

2.11 Пользователь должен быть ознакомлен с положениями настоящей Инструкции. Факт ознакомления подтверждается подписью в листе, приведенном в приложении №1.

2.12 Обо всех выявленных нарушениях, связанных с информационной безопасностью Предприятия, а так же для получения консультаций по вопросам информационной безопасности, необходимо обратиться в ОЗИ по внутренним телефонам (37-17) или (44-09).

2.13 Для получения консультаций по вопросам работы и настройке элементов ИСПДн необходимо обращаться к Администратору локальной вычислительной сети по внутренним телефонам (36-13), (42-86).

Пользователям запрещается:

- использовать сведения ограниченного распространения при подготовке открытых публикаций;

- выносить документы ограниченного распространения из служебных помещений, делать выписки или снимать копии с таких документов;
- оставлять незаблокированным компьютер в случае отсутствия пользователя на своем рабочем месте (для блокировки необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt> и выбрать опцию <Блокировка>);
- самовольное изменение конфигурации аппаратных средств, входящих в состав ИСПДн;
- установка на АРМ пользователей дополнительного программного обеспечения, не связанного с исполнением своих трудовых обязанностей;
- осуществлять обработку персональных данных в присутствии посторонних лиц;
- отключать средства защиты информации;
- передавать посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн;
- самостоятельно производить ремонт или настройку АРМ.

3 Организация парольной защиты

3.1 Личные пароли доступа к АРМ пользователя выдаются Администратором локальной вычислительной сети, пароли доступа к элементам ERP «Галактика» выдаются Начальником бюро программирования ОВАСУПиП или лицом замещающим его. В дальнейшем замена пароля производится самостоятельно.

3.2 Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 3 месяца.

3.3 Правила формирования пароля:

- длина пароля должна быть не менее 8 символов;
- пароль не может совпадать с именем учетной записи;
- пароль обязательно должен включать в себя буквы в нижнем и верхнем регистрах и цифры;

- запрещается использовать в качестве пароля имена, даты рождения, адреса, номера машин и иную информацию, которую можно узнать, основываясь на информации о пользователе;
- при смене пароля новый пароль должен отличаться от предыдущего;
- запрещается использовать в качестве пароля один и тот же повторяющийся символ.

3.4 Правила хранения пароля:

- запрещается хранить пароли в бумажном виде, фотографировать и записывать на носители информации;
- запрещается передавать свой пароль другим пользователям;
- запрещается использовать учетную запись другого пользователя.

Работники обязаны:

- знать и выполнять требования настоящей Инструкции;
- своевременно сообщать Начальнику бюро программирования ОБАСУПиП об утере или компрометации паролей.

4 Ответственность

4.1 Пользователь несет ответственность за все свои действия, нарушающие требования настоящей инструкции, а также действия, которые совершаются с его учетной записи, если он не предпринимал действий, направленных на предотвращение несанкционированного использования его учетной записи.

4.2 Разглашение персональных данных субъекта, утрата документов или иных носителей информации, содержащих персональные данные, и нарушение обязанностей по защите персональных данных в ходе ее обработки влечет дисциплинарное взыскание в виде: замечание, выговора, увольнения.

4.3 В случае публичного распространения информации о частной жизни лица, предусмотрена уголовная ответственность в соответствии со ст. 137 УК РФ (нарушение неприкосновенности частной жизни).

ЛИСТ

**ознакомления с Инструкцией пользователя информационной системы
персональных данных сотрудников АО «Радиозавод»**

№ п/п	Фамилия, имя, отчество работника	Дата и подпись работника после ознакомления с Инструкцией

Приложение К
(обязательное)

Правила осуществления внутреннего контроля соответствия обработки
персональных данных требованиям к защите персональных данных в АО
«Радиозавод»

«Согласовано»

Директор по персоналу и режиму

_____ С.Г. Викторov

«__» _____ 2018г

«Утверждаю»

Генеральный директор

_____ А.Г. Быстров

«__» _____ 2018г

ПРАВИЛА

осуществления внутреннего контроля соответствия обработки
персональных данных требованиям к защите персональных данных
в АО «Радиозавод»

2018 г

1 Настоящие Правила определяют основания, форму и порядок осуществления в АО «Радиозавод» (далее – Предприятие) внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, которые установлены Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» и принятыми нормативными актами.

2 Настоящие Правила разработаны в соответствии с:

– Федеральным законом от 27 июля 2006 г. № 152 ФЗ «О персональных данных»;

– Постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» и другими нормативными правовыми актами.

3 В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям на Предприятии организовывается проведение периодических проверок условий обработки персональных данных (далее - Проверка).

4 Основанием для проведения Проверок являются требования Федерального закона №152-ФЗ (часть 1, статья 18.1) и постановления Правительства №1119 (п.17).

5 Проверка осуществляется комиссией по обеспечению безопасности персональных данных, которая назначается приказом генерального директора Предприятия (далее – Комиссия). В состав Комиссии входит не менее 3 человек.

6 Проверка проводится не реже чем один раз в год. Перед проведением Проверки не позднее 10 рабочих дней до начала Проверки

руководителям структурных подразделений, где будет осуществляться Проверка, направляются уведомления о ее проведении. Внеплановая Проверка проводится в течение трех рабочих дней с момента поступления заявления на такую Проверку

7 При проведении Проверки должны устанавливаться:

- соответствие организационных и технических мер по обеспечению безопасности персональных данных требованиям к защите персональных данных;
- факт ознакомления с локальными актами Предприятия в области обеспечения безопасности и обработки персональных данных;
- соблюдение установленного порядка доступа в помещения, где ведется обработка персональных данных;
- соответствие оборудования и программных средств, используемых в информационной системе персональных данных, техническому паспорту информационной системы;
- соблюдение сроков хранения персональных данных, а также порядка их уничтожения;
- соответствие выполнения требований по определению уровня защищенности и требований, предъявляемых для обеспечения этого уровня защищенности в соответствии с постановлением Правительства №1119;
- наличие фактов несанкционированного доступа к персональным данным и принятие необходимых мер;
- соответствие персональных данных, обрабатываемых на Предприятии, утвержденным перечням персональных данных.

8 Комиссия имеет право:

- запрашивать у работников Предприятия информацию, которая необходима для реализации полномочий комиссии;
- привлекать к проведению проверок работников Предприятия;

- вносить предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных;
- принимать меры прекращению или приостановлению процесса обработки персональных данных, который осуществляется с нарушением требований законодательства Российской Федерации;
- принимать меры по устранению нарушений требований к защите персональных данных, выявленных в ходе проведения Проверки;
- требовать от должностных лиц, осуществляющих обработку персональных данных, уточнения, блокирования или уничтожения полученных незаконным путем или недостоверных персональных данных;
- вносить предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке.

9 В отношении персональных данных, которые стали известны входящим в состав комиссии лицам при проведении Проверок, должна обеспечиваться конфиденциальность.

10 Проверка должна быть завершена не позднее чем через 30 дней со дня принятия решения о её проведении. О результатах проведенной Проверки и мерах, которые необходимо принять для устранения выявленных нарушений, в течение 10 рабочих дней со дня завершения проверки председатель комиссии в форме письменного заявления обязан доложить директору по персоналу и режиму.