

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования

«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт
Факультет приборостроения,
информационных технологий и
электроники

Кафедра
«Информационная безопасность
систем и технологий»

Специальность 10.05.03 –

Информационная безопасность
автоматизированных систем

Специализация –

Защищенные автоматизированные
системы управления

ДИПЛОМНЫЙ ПРОЕКТ

на тему

АВТОМАТИЗИРОВАННАЯ СИСТЕМА ОТДЕЛА КАДРОВ НА ФГУП
ФНПЦ «ПО «СТАРТ» ИМ. М.В.ПРОЦЕНКО» В ЗАЩИЩЕННОМ
ИСПОЛНЕНИИ

Студент Клюев Дмитрий Владимирович

Руководитель нач.отдела сист.програм. Совватейкин С.Н.

Нормоконтролёр Фатеев А.Г.

Рецензент нач.отдела защиты информации Курамов В.Г.

Работа допущена к защите (протокол заседания кафедры от 26.06.18 № 16)

Заведующий кафедрой С.Л. Зефилов

Работа защищена с отметкой удовлетворительно (протокол заседания ГЭК от 27.06.18 № 6)

Секретарь ГЭК А.П. Иванов

Пенза 2018

Проверено Замос
26.06.2018 бсг/Султанов

Оглавление

Введение.....	5
1 Описание текущего состояния автоматизированной системы «Отдел кадров» на ФГУП ФНПЦ «ПО «Старт» им. М.В.Проценко».....	6
1.1 Описание автоматизированной системы «Отдел кадров», её целей функционирования, основных производственных процессов.....	6
1.2 Описание информационных процессов, с помощью которых реализуются задачи деятельности организации.....	7
1.3 Описание структуры автоматизированной системы «Отдел кадров» и описание технических средств обработки информации	10
1.4 Описание физической модели автоматизированной системы «Отдел кадров».....	15
1.5 Выявление и описание информационных систем персональных данных в отделе кадров.....	16
2 Разработка модели нарушителя ИБ.....	22
3 Описание актуальных для ПДн организации угроз и разработка частной модели угроз.....	26
4 Определение уровня защищенности информационных систем персональных данных отдела кадров.....	39
5 Определение организационных и организационно-технических требований к обеспечению уровней защищенности персональных данных в информационных системах персональных данных отдела кадров.....	41
5.1 Определение базового набора мер по обеспечению безопасности для информационных системах персональных данных.....	41

5.2	Адаптация и уточнение мер по обеспечению безопасности персональных данных в информационной системе персональных данных «Контрагенты»	43
5.3	Описание защитных мер для ИСПДн №1 «Контрагенты».....	46
5.4	Адаптация и уточнение мер по обеспечению безопасности персональных данных в информационной системе персональных данных «Сотрудники».....	54
5.5	Описание защитных мер для ИСПДн №2 «Сотрудники».....	56
6	Выбор и обоснование средств защиты информации для автоматизированной системы «Отдел кадров» в защищенном исполнении.....	64
7	Описание АСЗИ «Отдел кадров».....	69
8	Вредные психофизиологические факторы, влияющие на опорно-двигательный аппарат специалиста по защите информации, методы и средства физической культуры, снижающие их воздействие.....	71
	Заключение.....	74
	Список используемых источников.....	75

Обозначение и сокращения

АС – автоматизированная система;

АСЗИ – автоматизированная система в защищенном исполнении;

АРМ – автоматизированное рабочее место;

БД – база данных;

Д – доступность;

ИОД – информация ограниченного доступа;

ИС – информационная система;

ИСПДн – информационная система персональных данных;

К – конфиденциальность;

КЗ – контролируемая зона;

НСД – несанкционированный доступ;

ПДн – персональные данные;

ПО – программное обеспечение;

СЗИ – средство защиты информации;

СЗПДн – средство защиты персональных данных;

СУБД – система управления базы данных;

ФЗ – федеральный закон;

ФСТЭК – Федеральная служба по техническому и экспортному контролю;

Ц – целостность.

Введение

В текущий момент времени в информационной безопасности существует множество проблем, и одной из таких является защита персональных данных граждан Российской Федерации. Задачи защиты персональных данных осложняются тем, что информационное пространство очень велико. Низкоквалифицированный персонал организации, отсутствие оборудования и помещений – всё это может повлечь за собой неправильную обработку персональных данных, а из этого следует, что граждане РФ получают материальный ущерб и/или моральный вред.

Абсолютно все предприятия и организации в Российской Федерации используют в ходе своей деятельности обработку персональных данных. Регулированию информационных правоотношений уделяется важное значение, а также законодательством назначен целый ряд нормативно-правовых актов.

Актуальность и новизна данной выпускной квалификационной работы заключается в том, чтобы формирование требований к обеспечению защиты персональных данных в автоматизированной системе отдела кадров на ФГУП ФНПЦ «ПО «Старт» им. М.В.Проценко» происходило на основе последних редакций нормативно-правовых актов и методических документов по защите персональных данных.

1 Описание текущего состояния автоматизированной системы «Отдел кадров» на ФГУП ФНПЦ «ПО «Старт» им. М.В.Проценко»

1.1 Описание автоматизированной системы «Отдел кадров», её целей функционирования, основных производственных процессов

Целью функционирования отдела кадров на ФГУП ФНПЦ «ПО «Старт» им. М.В.Проценко» является способствование достижению целей всего предприятия посредством обеспечения ФГУП ФНПЦ «ПО «Старт» им. М.В.Проценко» необходимыми кадрами, а также продуктивное использованием рабочего потенциала.

Эта цель достигается путем выполнения в отделе кадров на ФГУП ФНПЦ «ПО «Старт» им. М.В.Проценко» следующих функций:

- выбор и отбор сотрудников, распределение сотрудников на местах;
- контроль эффективного использования сотрудников в различных отраслях деятельности предприятия;
- регистрация приема, перевода и сокращения сотрудников в соответствии с трудовым кодексом РФ, приказами руководителей и внутренними положениями;
- оформление справок о трудовой деятельности и трудовых книжек, а также хранение и их учёт;
- ведение документации по всем сотрудникам предприятия, награждение или премирование отличившихся сотрудников;
- оформление характеристик сотрудникам в ВУЗы, техникумы, военкоматы, суды, органы МВД и т.д.;
- оформление целевых направлений на нужное число специалистов по определенным специальностям;
- учет образования сотрудников (высшее и среднетехническое, среднеспециальное, а также научных работников;

- утверждение нужных документов для привлечения к ответственности сотрудников, нарушивших трудовую дисциплину;
- ведение табельного учета и обязательного медицинского страхования на ФГУП ФНПЦ «ПО «Старт» им. М.В.Проценко»;
- сбор материалов по пенсионному страхованию и учет каждого работника в системе Государственного пенсионного страхования.

Целью автоматизированной системы «Отдел кадров» является достижение упорядоченной работы отдела кадров на ФГУП ФНПЦ «ПО «Старт» им. М.В.Проценко», более скорое и эффективное многофакторное исследование самых рациональных принципов функционирования отдела кадров на ФГУП ФНПЦ «ПО «Старт» им. М.В.Проценко».

Для достижения этой цели в отделе кадров на ФГУП ФНПЦ «ПО «Старт» им. М.В.Проценко» выполняются следующие функции:

- оформление трудовых договоров с работниками;
- хранение сведений из личных карточек работников и вывод их на печать.

1.2 Описание информационных процессов, с помощью которых реализуются задачи деятельности организации

Структурная модель информационного процесса «Оформление трудовых договоров с работниками» представлена на рисунке 1.

Входной информацией в данном процессе являются ПДн работников, а также документы, определенные ст.65 ТК РФ.

Работники, поступающие на работу на предприятие предоставляют свои ПДн на бумажном носителе сотрудникам отдела кадров. Сотрудник отдела кадров (Оператор) вносит эту информацию в БД, где она и будет храниться, и откуда она будет поступать в электронном виде в отдел кадров. На этом же этапе составляется трудовой договор с будущими сотрудниками организации

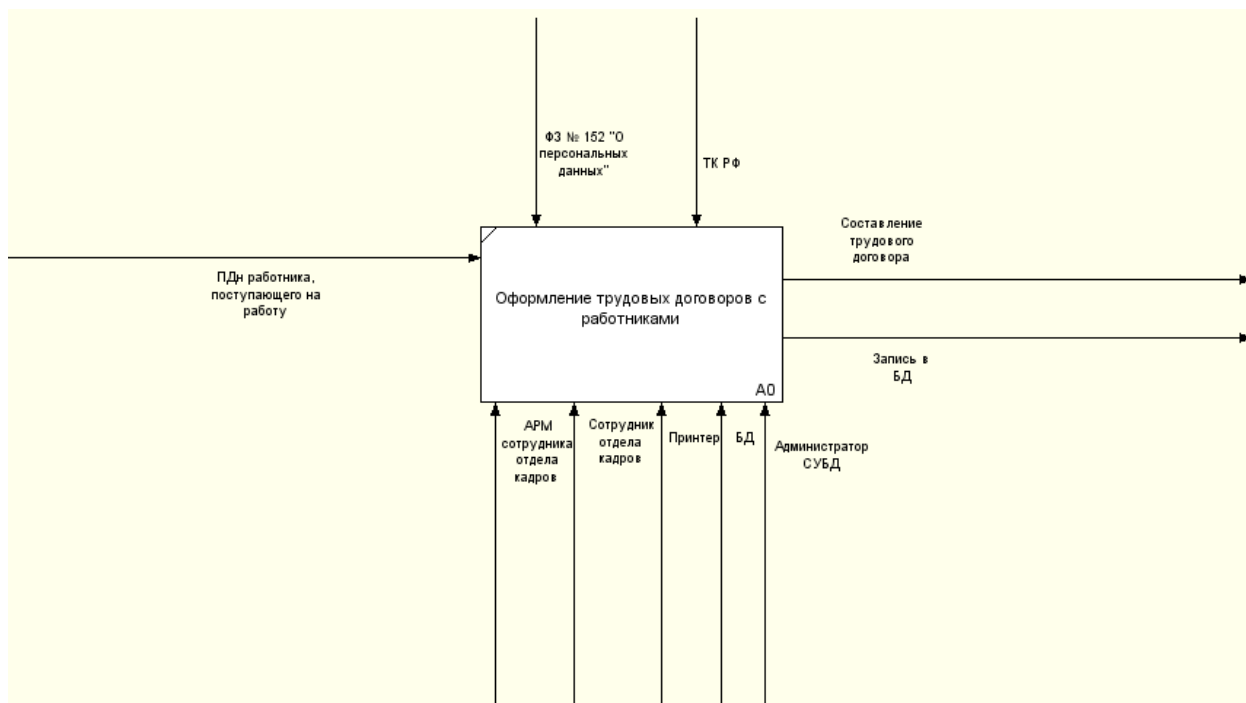


Рисунок 1 – Структурная модель информационного процесса «Оформление трудовых договоров с работниками»

Входной информацией в данном процессе являются ПДн работников, а также документы, определенные ст.65 ТК РФ.

Работники, поступающие на работу на предприятие предоставляют свои ПДн на бумажном носителе сотрудникам отдела кадров. Сотрудник отдела кадров (Оператор) вносит эту информацию в БД, где она и будет храниться, и откуда она будет поступать в электронном виде в отдел кадров. На этом же этапе составляется трудовой договор с будущими сотрудниками организации

Результатом этого процесса является составление трудового договора, а также запись информации в БД.

Все обработанные в отделе кадров данные хранятся в БД отдела кадров и в архиве (сейфе) в бумажном виде. Обработанная информация продолжает храниться в течении 50 лет, в соответствии со ст. 22.1 Закона от 22.10.2004 г. №125-ФЗ. При наличии доступа у сотрудника к запрошенной информации, обработанная информация поступает на АРМ. Выводится информация на монитор в удобном виде для восприятия сотрудником.

Структурная модель информационного процесса «Хранение сведений из личных карточек работников и вывод их на печать» представлена на рисунке 2.

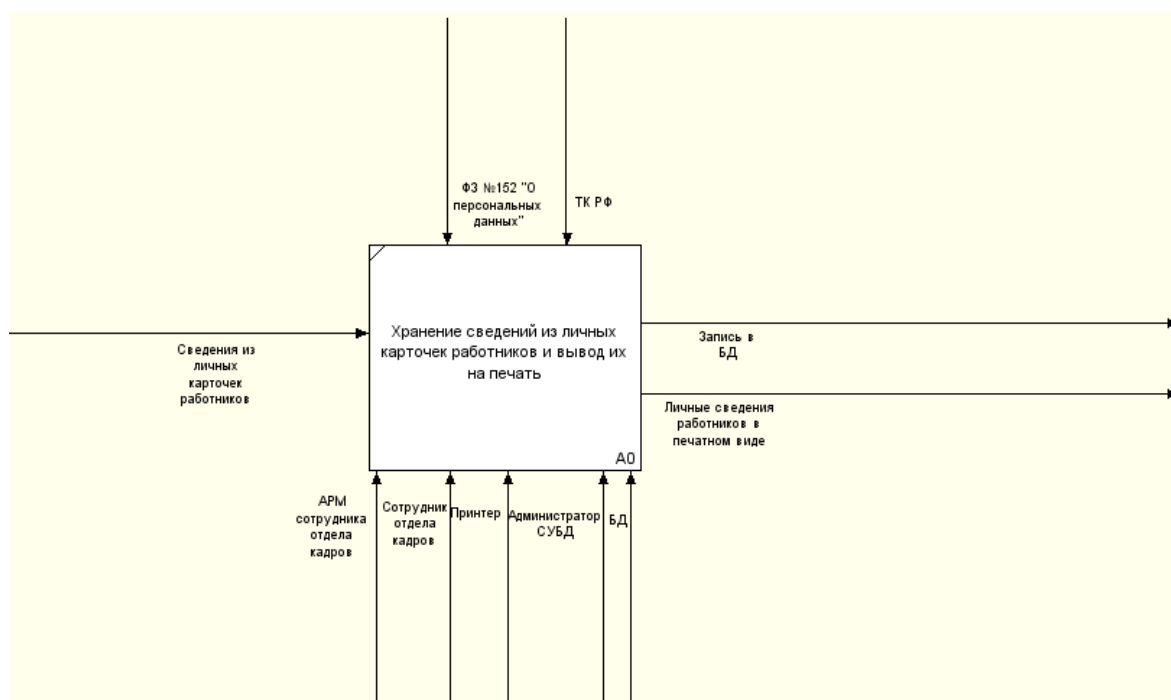


Рисунок 2 – Структурная модель информационного процесса «Хранение сведений из личных карточек работников и вывод их на печать»

Входной информацией в данном процессе являются сведения из личных карточек работников.

Сотрудник отдела кадров запрашивает сведения из личных карточек работников.

Далее сотрудник отдела кадров с использованием АРМ вносит соответствующие актуальные изменения в сведения из личных карточек работников и при необходимости выводит их на печать. Результатом этого процесса являются хранение измененных/уточненных сведений из личных карточек сотрудников в БД отдела кадров, а также сведения из личных карточек сотрудников в печатном виде на бумажном носителе.

Информация хранится в электронном виде в БД отдела кадров и в сейфе в печатном виде в одном экземпляре. Обработанная информация продолжает храниться в течении 50 лет, в соответствии со ст. 22.1 Закона от 22.10.2004 г. №125-ФЗ. При наличии доступа у сотрудника к запрошенной информации,

обработанная информация поступает на АРМ. Выводится информация на монитор в удобном виде для восприятия сотрудником.

Сведениями конфиденциального характера в двух этих процессах являются ПДн сотрудников и сведения из личных карточек сотрудников.

1.3 Описание структуры автоматизированной системы «Отдел кадров» и описание технических средств обработки информации

Описание структуры АС «Отдел кадров», которая позволяет выполнять функции, возлагаемые на неё, представлено на рисунке 3.

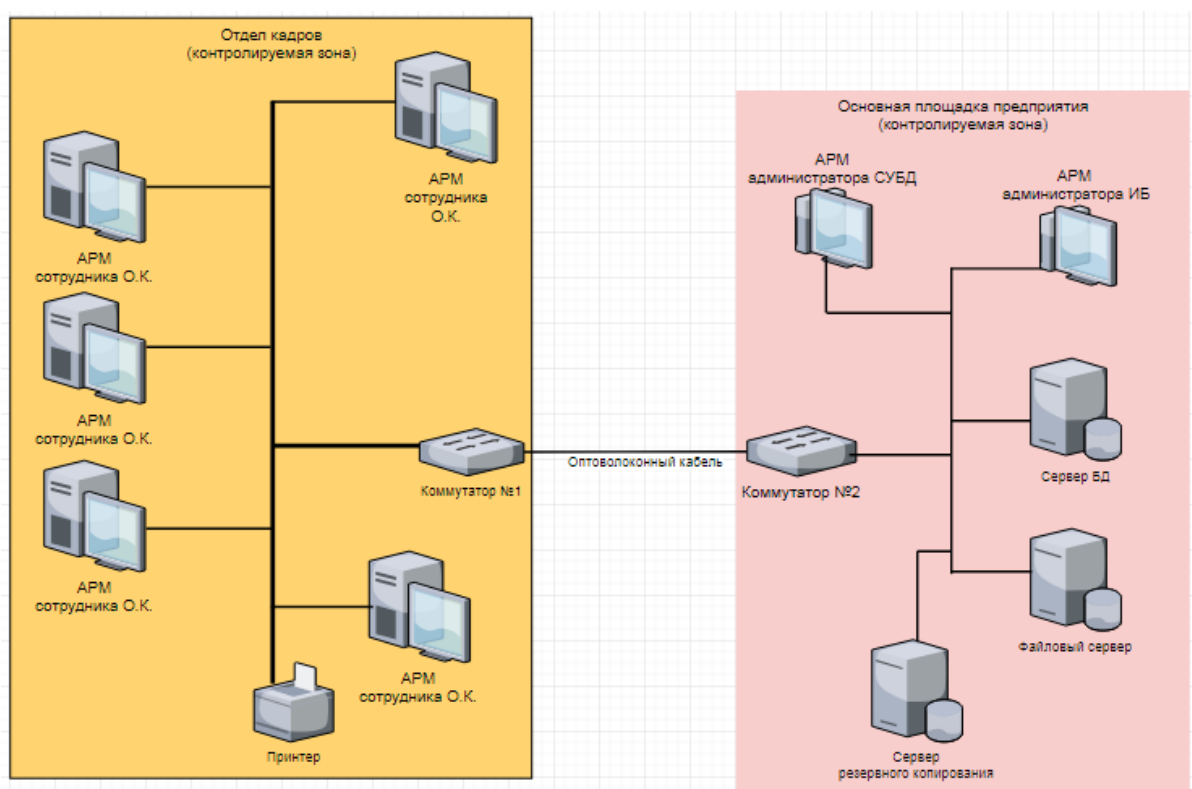


Рисунок 3 – Структура АС «Отдел кадров»

Далее на основе структуры АС «Отдел кадров» и описанных ранее информационных процессов была разработана инфологическая модель АС «Отдел кадров», показывающая циркуляцию информации путем использования информационных ресурсов в системе. Результат представлен на рисунке 4.

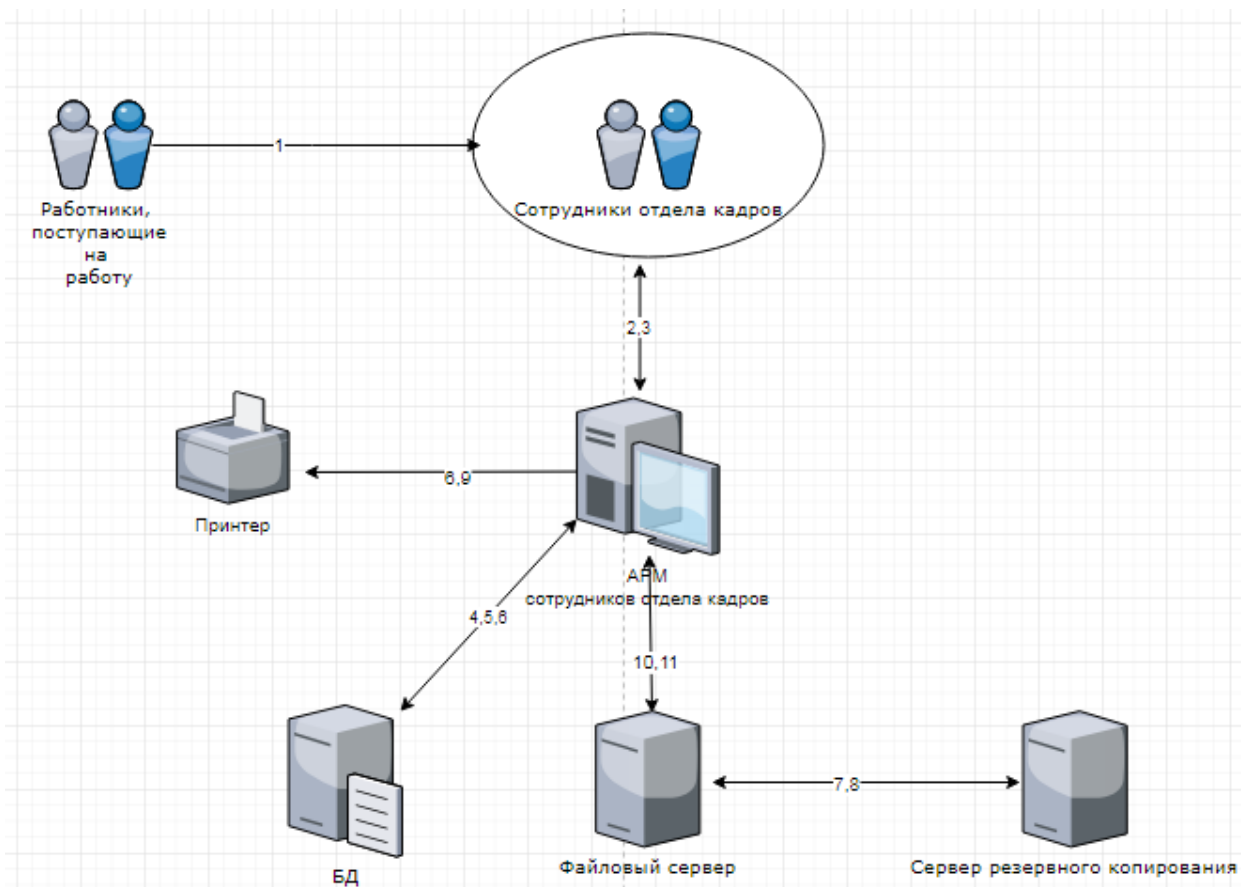


Рисунок 4 – Информационные потоки в АС «Отдел кадров»

Обозначение информационных потоков представлено в таблице 1.

Таблица 1 – Информационные потоки

Обозначение потока	Информационный поток
1	Предоставление ПДн на бумажном носителе
2	Внесение ПДн
3	Запрос/изменение/ввод сведений из личных карточек работников
4	Сведения из личных карточек работников
5	Внесение ПДн в БД
6	Вывод на печать трудового договора
7	Создание/отправка резервной копии/последних обновлений на сервер резервного копирования
8	Восстановление данных из резервной копии
9	Вывод на печать сведений из личных карточек работников
10	Отправка копии трудового договора/сведений из личных карточек работников в электронном виде
11	Запрос копии трудового договора/сведений из личных карточек работников в электронном виде

Далее для описания структуры АС «Отдел кадров» были рассмотрены технические средства, входящие в систему. В данную АС входят:

- сервер БД, где хранится ИОД. Сервера находятся в пределах контролируемой зоны. Они используют сетевые соединения по протоколу TCP/IP для подключения клиентов и обслуживания их запросов. Сервер находится под управлением СУБД MySQL. Объем оперативной памяти – 128Гб. Объем дискового пространства – 1Тб. Процессор: AM3 Athlon II X2 AD235EHDK23GQ 45W Regor 2700MHz 2000MHz 1MB x2 N/A C2 All;

- файловый сервер. В состав файлового сервера входят следующие компоненты:

- ОС Ubuntu Server 12.04;

- клиент MySQL 4.7.11;

- СУБД Postgres SQL 9;

- антивирус «Kaspersky Endpoint Security 8»;

- сервер резервного копирования. В его состав входят:

- сервер HPE Proliant DL360 HPM Gen9 E5-2660v4 Rack(1U)/2xXeon14C/2.0GHz(35MB)/4x16GbR1D_2400/P440arFBWC(2GB/RAID/1/10/5/50/6/60)/noHDD(8+2up)SFF/noDVD/iLOAdv/7RFans/4x1GbEth/2x10Gb-SFP+ FlexLOM/EasyRK/2x800wFPlat – 1 шт;

- жесткий диск 759208-B21 HPE 300GB 2,5"(SFF) SAS 15K 12G Hot Plug w Smart Drive SC Entry HDD (for HP Proliant Gen8/Gen9 servers) – 3 шт;

- трансивер 455883-B21 HPE Ethernet Optical Transceivers, 10Gb, SR, SFP+ for 523/530/546/557/560SFP+, 640SFP28/640FLR-SFP28 & other – 2 шт;

- модуль памяти KTH-PL424S/16G Kingston fo HP/Compaq – 4 шт;

- панель 764632-B21 HPE DVD/USB Universal Media Bay (DVD-RW, USB 2.0, and VGA) Kit for 8SFF DL360 Gen9 – 1 шт;

- принтер HP LaserJet Pro M402dn (G3V21A) (A4, 1200dpi, 4800x600, 38ppm, 128Mb, 2tray 100+250, Duplex, USB2.0/GigEth, PS3 em.,

ePrint, AirPrint, 3y warr, cartridge 9000);

- источник бесперебойного питания APC SRT5KRMXLI Smart-UPS SRT RM, 5000VA/4500W, On-Line, Extended-run, Rack 3U (Tower convertible), Pre-Inst. Web/SNMP, with PC Business, Black;

- АРМ отдела кадров. АРМ имеют типовую структуру и одинаковы для всех сотрудников. Все АРМ находятся в пределах КЗ. На АРМ сотрудников установлены следующие программные средства:

- ОС Windows 7;
- MS Office 2007;
- компьютерная справочная правовая система «Консультант Плюс»;
- антивирус «Kaspersky Endpoint Security 8»;
- СЗИ от НСД «Secret Net 7».

В состав АРМ администратора СУБД входят следующие программные компоненты:

- Ubuntu Gnome 16.04 LTS;
- Libreoffice 5.4.1;
- клиент MySQL 4.7.11;
- Chromium;
- антивирус «Kaspersky Endpoint Security 8»;
- СЗИ от НСД «Secret Net 7».

В состав АРМ администратора СУБД входят следующие аппаратные компоненты:

- ПЭВМ MT i5-7500 (3.4GHz, QC,6M), 16GB DDR4 2400MHz, 2TB SATA 7.2k RPM 6Gbps Entry 3.5" Cabled HD, Intel HD Graphics, RW, mse, keyb, Audio, 3Y NBD – 1 шт;

- видеокарта ASUS GT730-SL-2GD3-BRK// GT730-SL-2GD3-BRK, VGA,DVI,HDMI,2GD3, 90YV06P0-M0NA00 – 1 шт;
- сетевой адаптер Gigabit Ethernet Single port Fiber Gigabit NIC for 32-bit PCI Express x1 bus, SC connector – 1 шт;
- монитор 24" Dell U2412M, BK/BK S-IPS, LED 1920x1200, 8ms, 300 cd/m2, 1000:1, 178/178, DVI, DP, HAS, Pivot, 4xUSB 2.0, Black – 1 шт.

АС отдела кадров обменивается данными по локальной сети по оптоволоконному кабелю.

В качестве коммутационного оборудования используются коммутаторы Cisco WS- C3550-12.

Все аппаратные ресурсы АС «Отдел кадров» объединены между собой.

После этого параметры АС «Отдел кадров» на ФГУП ФНПЦ «ПО «Старт» им. М.В.Проценко» были представлены в таблице 2.

Таблица 2 – Параметры АС «Отдел кадров»

Характеристики АС	Параметры АС
Структура АС	Локальная АС
Подключение АС к сетям общего пользования и (или) сетям международного информационного обмена	Отсутствует
Режим обработки информации	Многопользовательская
Режим разграничения прав доступа пользователей	Система с разграничением прав доступа
Местонахождение технических средств АС	Все технические средства находятся в пределах РФ

1.4 Описание физической модели автоматизированной системы «Отдел кадров»

Был описан план помещения, в котором расположен отдел кадров и компоненты АС «Отдел кадров». Общая площадь «Отдела кадров» составляет 630 кв. метров. Высота потолка составляет 3,2 метра. Материал внешних и внутренних стен – керамический кирпич.

Общее количество сотрудников отдела кадров - 5 человек. В помещении отдела кадров располагаются: 5 АРМ сотрудников отдела кадров, принтер шкаф/сейф, помещение для проведения инструктажей.

На рисунке 5 представлено размещение всех АРМ, а также расположение сейфа/шкафа, а также план всего этажа, на котором находится отдел кадров.

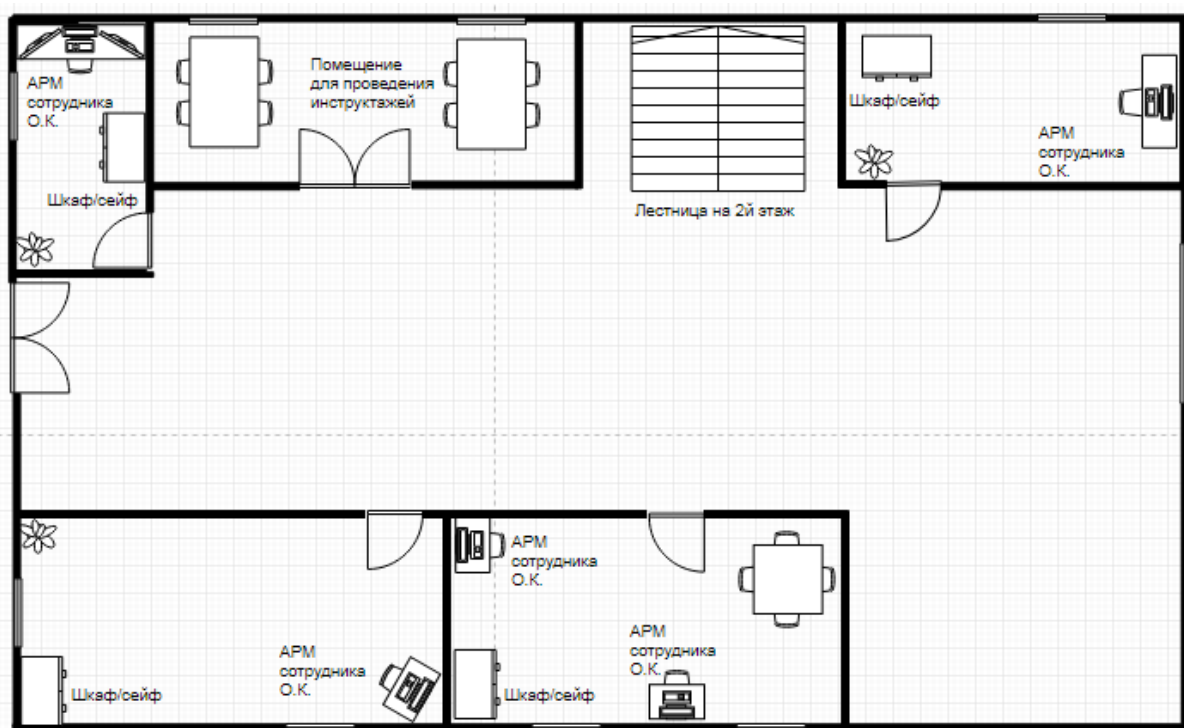


Рисунок 5 – План этажа отдела кадров

1.5 Выявление и описание информационных систем персональных данных в отделе кадров

Определение условий создания и использования персональных данных.

Для описания условий создания и использования ПДн в организации для ПДн были определены следующие характеристики:

- цель обработки ПДн в данной ИСПДн;
- перечни ПДн, обрабатываемых в организации в связи с реализацией трудовых отношений, а также в связи с оказанием услуг и осуществлением функций организации и содержание ПДн (фамилия, имя, отчество, дата рождения, паспортные данные, сведения о состоянии здоровья и т.п.);
- действия, осуществляемые с данными в ходе их обработки (действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных);
- сроки обработки и хранения ПДн;
- условия прекращения обработки ПДн и порядок их уничтожения при достижении целей обработки или при наступлении иных законных оснований;
- категории субъектов, персональные данные которых обрабатываются.

Затем ПДн были распределены по категориям: общедоступные, биометрические, специальные и иные, кроме этого ПДн были поделены на две категории: ПДн сотрудников организации и ПДн субъектов ПДн, не являющихся сотрудниками организации. Результаты категорирования представлены в таблице 3.

Таблица 3 – Перечень персональных данных, обрабатываемых в автоматизированной системе «Отдел кадров»

Содержание ПДн	Цели обработки ПДн	Основание для обработки ПДн	Сроки обработки и хранения ПДн, основания для прекращения обработки ПДн	Категория ПДн	Вид обработки (с использованием средств автоматизации, без использования средств автоматизации, смешанная)
Обработка ПДн сотрудников организации					
Фамилия, имя, отчество Паспортные данные (серия/номер/дата/кем выдан) Пол Дата рождения (число/месяц/год) Место рождения Адрес прописки Состояние в браке Состав семьи Место работы ИНН Номер страхового свидетельства ПФР Номер диплома Общий трудовой стаж Сведения о социальных льготах Табельный номер работника Должность работника Структурное подразделение Данные по отпускам	Осуществление финансовых операций (выплата заработной платы, отпускные, оплата больничного листа).	Трудовые отношения между работником и Фондом (ст. 16 ТК РФ). Трудовой договор с работником.	Срок обработки зависит от срока работы сотрудников, чьи ПДн используются в ИС; Документы о работнике хранятся 75 лет в соответствии со ст. 22 ФЗ «Об архивном деле в РФ». Основанием для прекращения обработки ПДн служит расторжение трудового договора	Иные	Смешанный

Продолжение таблицы 3

Обработка ПДн субъектов ПДн, не являющихся сотрудниками организации					
Фамилия, имя, отчество Паспортные данные (серия/номер/дата /кем выдан) контактный телефон, ИНН	составление финансово-расчетных документов о взаимодействии с контрагентами	Договорные отношения между Предприятием и контрагентом	Срок обработки зависит от срока действия договоров с контрагентами, чьи ПДн используются в ИС; Срок хранения договоров возмездного оказания услуг с физическими лицами - 50 лет, Это следует из ст. 22.1 Закона от 22.10.2004 г. №125-ФЗ Основание для прекращения обработки ПДн служит расторжение договора с контрагентами	Иные	Смешанный

Далее был разработан перечень информационных систем персональных данных. Для составления перечня ИСПДн была составлена матрица доступа сотрудников предприятия к ПДн, отражающая права всех групп пользователей ПДн на действия с ПДн Действия с персональными данными, включают сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных).

Матрица доступа для организации представлена в таблице 4.

Таблица 4 – Матрица доступа для организации

Группа	Уровень доступа к ПДн	Разрешенные действия	Сотрудники
Администратор ИСПДн	Обладает полной информацией о системном и прикладном программном обеспечении ИС-ПДн. Обладает полной информацией о технических средствах и конфигурации ИС-ПДн. Имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн. Обладает правами конфигурирования и административной настройки технических средств ИС-ПДн.	- хранение - уточнение - использование - обезличивание - блокирование - уничтожение	Администратор безопасности

Продолжение таблицы 4

Группа	Уровень доступа к ПДн	Разрешенные действия	Сотрудники
Разработчик ИСПДн	Обладает информацией об алгоритмах и программах обработки информации на ИСПДн. Обладает правами внесения изменений в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения. Располагает всей информацией о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн.	<ul style="list-style-type: none"> - хранение - уточнение - использование - обезличивание - блокирование - уничтожение 	Системный администратор
Операторы ИСПДн	Обладает правами доступа к подмножеству ПДн. Располагает информацией о топологии ИСПДн на базе локальной и (или) распределенной информационной систем, через которую он осуществляет доступ, и составе технических средств ИСПДн.	<ul style="list-style-type: none"> - сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение 	Сотрудники отдела кадров

Основанием для допуска к ПДн является необходимость обработки ПДн в связи с выполнением должностных обязанностей. Основанием для прекращения доступа к ПДн является увольнение сотрудника, либо его перевод на другую должность, которая не требует работы с ПДн.

На основании перечня ПДн, обрабатываемых в отделе кадров и матрицы доступа к этим ПДн были установлены следующие ИСПДн: ИСПДн№1 «Контрагенты» и ИСПДн №2 «Сотрудники».

Описание установленных ИСПДн представлено в таблице 5.

Таблица 5 – Описание установленных ИСПДн

Наименование ИСПДн	Категория ПДн	Расположение ИСПДн	Сотрудники	Количество обрабатываемых ПДн субъектов
ИСПДн№1 «Контрагенты»	Иные	На территории РФ	Для субъектов, не являющихся сотрудниками предприятия	Более 100 000
ИСПДн №2 «Сотрудники»	Иные	На территории РФ	Для субъектов, являющихся сотрудниками предприятия	Более 100 000

2 Разработка модели нарушителя ИБ

Нарушители подразделяются на два типа.

Внешние нарушители — лица, не имеющие физический доступ, но которые могут обладать логическим доступом через каналы связи, выходящие за пределы КЗ, к компонентам АС и содержащейся в них информации.

Внутренние нарушители — лица, имеющие физический и логический доступ к компонентам АС и информации содержащейся в них. А именно:

- устройств ввода/вывода (отображения) информации;
- программных, программно-технических и технических средств обработки информации;
- съемных машинных носителей информации;
- машинных носителей информации, выведенных из эксплуатации;
- активного (коммутационного) и пассивного оборудования каналов связи;
- каналов связи, выходящих за пределы КЗ.

Основные виды внешних и внутренних нарушителей (источников угроз) приведены в таблице 6.

Таблица 6 — Основные виды внешних и внутренних нарушителей

Обозначение	Источник угроз
ИУ1	Разработчики, производители, поставщики программных, технических и программно-технических средств
ИУ2	Лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ
ИУ3	Внешние субъекты (физические лица)
ИУ4	Лица, обеспечивающие функционирование системы или обслуживающие инфраструктуру оператора (администрация, охрана, уборщики и т.д.)
ИУ5	Пользователи АС
ИУ6	Администраторы АС системы и администраторы безопасности

Нарушители, обладающие базовым потенциалом, имеют возможность получить информацию об уязвимостях отдельных компонентов системы, опубликованную в общедоступных источниках. Они обладают возможностью получить информацию о методах и средствах реализации угроз БИ, опубликованных в общедоступных источниках, и (или) самостоятельно осуществить создание методов и средств реализации атак на ИС.

Нарушители, обладающие средним потенциалом, умеют пользоваться всеми возможностями нарушителей с базовым потенциалом. Они имеют осведомленность о мерах ЗИ, применяемых в ИС, а также возможность получить информацию об уязвимостях отдельных компонентов ИС (с использованием имеющихся в свободном доступе программных средств) путем анализа кода прикладного ПО и отдельных программных компонентов общесистемного ПО. Эти нарушители имеют доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования ИС.

Нарушители, обладающие высоким потенциалом, умеют пользоваться всеми возможностями нарушителей со средним потенциалом, имеют возможность осуществлять НСД из выделенных сетей связи, к которым возможен физический доступ. Они имеют возможность получить доступ к ПО чипсетов (микропрограммам), системному и прикладному ПО, телекоммуникационному оборудованию и другим программно-техническим средствам ИС для преднамеренного внесения в них уязвимостей или программных закладок, а также хорошую осведомленность о мерах ЗИ, применяемых в ИС, об алгоритмах, аппаратных и программных средствах, используемых в ИС. У них имеется возможность получать информацию об уязвимостях с помощью специальных исследований (в том числе с привлечением специализированных научных организаций) и применения специально разработанных средств для анализа ПО. Имеют возможность создания методов и средств реализации угроз БИ благодаря привлечению узкоспециализированных научных организаций и реализации угроз с применением специально

разработанных средств, в том числе обеспечивающих скрытное проникновение в ИС и воздействие на нее. Имеют возможность создания и применения специальных технических средств для добывания информации (воздействия на информацию или технические средства), распространяющейся в виде явлений или физических полей.

В качестве возможных целей (мотивации) реализации нарушителями угроз БИ в АС «Отдел кадров» могут быть:

- нанесение ущерба предприятию и его отдельным сферам деятельности;
- дискредитация или дестабилизация деятельности предприятия;
- получение конкурентных преимуществ;
- внедрение дополнительных функциональных возможностей в ПО или программно-технические средства на этапе разработки;
- реализация угроз ИБ из мести;
- реализация угроз ИБ непреднамеренно из-за неосторожности или не-квалифицированных действий.

Основные методы реализации угроз в АС «Отдел кадров» приведены в таблице 7.

Таблица 7 — Основные методы реализации угроз в АС «Отдел кадров»

Обозначение	Методы реализации угроз
М1	НСД и (или) воздействия на объекты на аппаратном уровне
М2	НСД и (или) воздействия на объекты на общесистемном уровне
М3	НСД и (или) воздействия на объекты на прикладном уровне (СУБД, иные прикладные программы общего и специального назначения)
М4	Несанкционированный физический доступ и (или) воздействия на каналы связи, технические средства, машинные носители информации
М5	Воздействия на пользователей, администраторов безопасности, администраторов ИС или обслуживающий персонал

В итоге была разработана модель нарушителя ИБ АС «Отдел кадров», которая является составной частью модели угроз ИБ АС «Отдел кадров» и содержит:

- типы, виды и потенциал нарушителей, которые могут обеспечить реализацию угроз ИБ;
- цели, которые могут преследовать нарушители каждого вида при реализации угроз ИБ;
- возможные способы реализации угроз ИБ.

Модель нарушителя ИБ АС «Отдел кадров» представлена в таблице 8.

Таблица 8 — Модель нарушителя ИБ АС «Отдел кадров»

№ п/п	Тип нарушителя	Вид нарушителя	Потенциал нарушителя	Методы реализации угроз
1	Внешние	ИУ1	Средний	М1, М2, М3
		ИУ2	Средний	М1
		ИУ3	Низкий	М4, М5
2	Внутренние	ИУ4	Средний	М3
		ИУ5	Высокий	М3, М4
		ИУ6	Высокий	М2, М3, М4

3 Описание актуальных для ПДн организации угроз и разработка частной модели угроз

При обработке ПДн в отделе кадров в соответствии с методическим документом ФСТЭК «Базовая модель угроз безопасности ПДн при их обработке в ИСПДн» были определены угрозы, представленные в таблице 9.

Таблица 9 — Угрозы безопасности

№ п/п	Описание угрозы	Источник угрозы	Нарушаемые свойства	Объекты воздействия	Уязвимость
1	Угрозы утечки видовой информации; [2]	Персонал, имеющий доступ в контролируемую зону, но не имеющий доступа к защищаемой информации	К	Информация, обрабатываемая на АРМ ИСПДн, информация, содержащаяся на электронных или бумажных носителях информации	Отсутствие физической защиты помещений, в которых расположены ИСПДн, нарушение правил использования физического управления доступом к помещениям, в которых расположены ИСПДн

Продолжение таблицы 9

№ п/ п	Описание угрозы	Источник угрозы	Нарушаемые свойства	Объекты воздействия	Уязвимость
2	Угроза действия вредоносных программ (вирусов); [2]	Персонал, имеющий доступ к защищаемой информации, персонал, осуществляющий администрирование информационной системы и средств защиты, наличие сети взаимодействия (локальной сети)	К, Д	Информация, обрабатываемая на АРМ ИСПДн, информация, обрабатываемая на серверах ИСПДн	Слабости разграничения доступа к управлению, бездействие администратора безопасности
3	Установка ПО, не связанного с исполнением служебных обязанностей [2]	Персонал, имеющий доступ к защищаемой информации, персонал, осуществляющий администрирование информационной системы и средств защиты	К, Д, Ц	Информация, обрабатываемая на АРМ ИСПДн, информация, обрабатываемая на серверах ИСПДн	Отсутствие контроля за ПО, устанавливаемым в организации

Продолжение таблицы 9

№ п / п	Описание угрозы	Источник угрозы	Нарушаемые свойства	Объекты воздействия	Уязвимость
4	Угроза разглашения информации, модификация, уничтожение сотрудниками допущенными к ее обработке; [2]	Персонал, имеющий доступ к защищаемой информации	К, Ц, Д	Информация, обрабатываемая на АРМ ИСПДн, информация, обрабатываемая на серверах ИСПДн, информация, содержащаяся на электронных или бумажных носителях информации	Отсутствие контроля действий сотрудников в помещениях в которых содержатся оборудование и носители данных
5	Утечка информации через порты ввода/вывода [2]	Персонал, имеющий доступ к защищаемой информации	К, Ц, Д	Информация, обрабатываемая на АРМ ИСПДн, информация, обрабатываемая на серверах ИСПДн, информация, содержащаяся на электронных или бумажных носителях информации	Отсутствие контроля действий сотрудников в помещениях в которых содержатся оборудование и носители данных

Актуальной считается угроза, которая может быть реализована в ИСПДн и представляет опасность для ПДн.

Для оценки возможности реализации угрозы применяются два показателя: уровень исходной защищенности ИСПДн и вероятность реализации рассматриваемой угрозы.

Уровень исходной защищенности ИСПДн - обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн, приведенных в таблице 10.

Таблица 10 – Показатели исходной защищенности ИСПДн №1 «Контрагенты»

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: локальная сеть	–	+	–
3. По встроенным (легальным) операциям с записями баз персональных данных: запись, удаление, сортировка;	–	+	–
4. По разграничению доступа к персональным данным: ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн	+	–	–
5. По наличию соединений с другими базами ПДн иных ИСПДн: ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн);	+	–	–
6. По уровню обобщения (обезличивания) ПДн: ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;	–	+	–
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки: ИСПДн, не предоставляющая ПДн	–	+	–

По результатам анализа таблицы 10 доля характеристик ИСПДн №1 «Контрагенты», соответствующих уровню «высокий», составляет ниже 70%, а доля характеристик ИСПДн, соответствующих уровню «средний», составляет долю, больше 70%. Таким образом, ИСПДн №1 «Контрагенты» имеет средний уровень защищенности.

Показатели исходной защищенности для ИСПДН №2 «Сотрудники» приведены в таблице 11.

Таблица 11 – Показатели исходной защищенности ИСПДН №2 «Сотрудники»

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: локальная сеть	–	+	–
3. По встроенным (легальным) операциям с записями баз персональных данных: запись, удаление, сортировка;	–	+	–
4. По разграничению доступа к персональным данным: ИСПДН, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДН	+	–	–
5. По наличию соединений с другими базами ПДн иных ИСПДН: ИСПДН, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДН);	+	–	–
6. По уровню обобщения (обезличивания) ПДн: ИСПДН, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;	–	+	–
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДН без предварительной обработки: ИСПДН, не предоставляющая ПДн	–	+	–

По результатам анализа таблицы 11 доля характеристик ИСПДН №2 «Сотрудники», соответствующих уровню «высокий», составляет ниже 70%, а доля характеристик ИСПДН, соответствующих уровню «средний», составляет долю, больше 70%. Таким образом, ИСПДН №2 «Сотрудники» имеет средний уровень защищенности. [2]

При составлении перечня актуальных угроз безопасности ПДн каждого уровня для каждого уровня исходной защищенности ставится в соответствие числовой коэффициент Y_1 , а именно:

- 0 для высокого уровня исходной защищенности;
- 5 для среднего уровня исходной защищенности;
- 10 для низкого уровня исходной защищенности.

Для каждой вероятности возникновения угрозы — Y_2 :

- 0 для маловероятной угрозы;
- 2 для низкой вероятности угрозы;
- 5 для средней вероятности угрозы;
- 10 для высокой вероятности угрозы.

Коэффициент реализуемости угрозы Y определяется по формуле (1).

$$Y=(Y_1+Y_2)/20 \quad (1)$$

Вероятность каждой угрозы определяется по вербальному показателю опасности на основе опроса экспертов, этот показатель имеет четыре значения: маловероятный, низкий, средний и высокий:

- маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации злоумышленниками, не имеющими легального доступа в помещение, где хранятся носители информации);

- низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, применены соответствующие СЗИ);

- средняя вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны;

- высокая вероятность – объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты.

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы следующим образом:

– если выполняется условие формулы (2), то возможность реализации угрозы признается низкой;

$$0 \leq Y \leq 0,3 \quad (2)$$

– если выполняется условие формулы (3), то возможность реализации угрозы признается средней;

$$0,3 < Y \leq 0,6 \quad (3)$$

– если выполняется условие формулы (4), то возможность реализации угрозы признается высокой;

$$0,6 < Y \leq 0,8 \quad (4)$$

– если выполняется условие формулы (5), то возможность реализации угрозы признается очень высокой.

$$Y > 0,8 \quad (5)$$

Результаты определения возможности реализации каждой угрозы в ИСПДн представлены в таблицах 12 и 13.

Таблица 12 – Результаты определения возможности реализации угроз в ИСПДн №1 «Контрагенты»

№	Угрозы	Вероятность реализации угроз	Y_1	Y_2	Y	Возможность реализации угрозы
1	Угрозы утечки видовой информации	Средняя	5	5	0,5	Средняя
2	Угроза действия вредоносных программ (вирусов)	Высокая		10	0,75	Высокая
3	Установка ПО, не связанного с исполнением служебных обязанностей	Средняя		5	0,5	Средняя

Продолжение таблицы 12

№	Угрозы	Вероятность реализации угроз	Y1	Y2	Y	Возможность реализации угрозы
4	Угроза разглашения информации, модификация, уничтожение сотрудниками допущенными к ее обработке	Средняя	5	2	0,35	Средняя
5	Утечка информации через порты ввода/вывода	Средняя		2	0,35	Средняя

Таблица 13 – Результаты определения возможности реализации угроз в ИСПДн №2 «Сотрудники»

№	Угрозы	Вероятность реализации угроз	Y1	Y2	Y	Возможность реализации угрозы
1	Угрозы утечки видовой информации	Средняя	5	5	0,5	Средняя
2	Угроза действия вредоносных программ (вирусов)	Высокая		10	0,75	Высокая
3	Установка ПО, не связанного с исполнением служебных обязанностей	Средняя		5	0,5	Средняя
4	Угроза разглашения информации, модификация, уничтожение сотрудниками допущенными к ее обработке	Средняя		2	0,35	Средняя
5	Утечка информации через порты ввода/вывода	Средняя		2	0,35	Средняя

Далее была проведена оценка опасности каждой угрозы. При оценке опасности на основе опроса экспертов (специалистов в области защиты информации) был определен вербальный показатель опасности для рассматриваемой ИСПДн. Этот показатель имеет три значения:

– незначительные негативные последствия (показатель опасности – низкий) – последствия для субъекта малоощутимы (незначительный финансовый или моральный ущерб, при этом репутация субъекта, его материальное благополучие, жизнь и здоровье не затронуты);

– негативные последствия (показатель опасности – средний) – последствия приводят к ощутимым по объему или значению финансовым и (или) моральным и (или) репутационным потерям. Основные интересы и права личности, закрепленные Конституцией РФ, не затронуты;

– значительные негативные последствия (показатель опасности – высокий) – последствия приводят к критическим финансовым, моральным, репутационным потерям для субъекта, вплоть до потери средств к существованию, здоровья, жизни.

На основе опроса экспертов был определен показатель опасности для каждой угрозы. Результаты представлены в таблицах 14 и 15.

Таблица 14 – Оценка опасности угроз для ИСПДн №1 «Контрагенты»

№	Угрозы	Показатель опасности угрозы
1	Угрозы утечки видовой информации	Высокая
2	Угроза действия вредоносных программ (вирусов)	Высокая
3	Установка ПО, не связанного с исполнением служебных обязанностей	Средняя
4	Угроза разглашения информации, модификация, уничтожение сотрудниками допущенными к ее обработке	Средняя
5	Утечка информации через порты ввода/вывода	Высокая

Таблица 15 – Оценка опасности угроз для ИСПДн №2 «Сотрудники»

№	Угрозы	Показатель опасности угрозы
1	Угрозы утечки видовой информации	Высокая
2	Угроза действия вредоносных программ (вирусов)	Высокая
3	Установка ПО, не связанного с исполнением служебных обязанностей	Средняя
4	Угроза разглашения информации, модификация, уничтожение сотрудниками допущенными к ее обработке	Средняя

Продолжение таблицы 15

№	Угрозы	Показатель опасности угрозы
5	Утечка информации через порты ввода/вывода	Высокая

Затем был осуществлен выбор из предварительного перечня угроз безопасности тех, которые относятся к актуальным для данной ИСПДн, в соответствии с правилами, показанными в таблице 16.

Таблица 16 — Правила отнесения угрозы безопасности ПДн к актуальной

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

Результаты определения актуальности угроз представлены в таблицах 17 и 18.

Таблица 17 – Актуальность угроз для ИСПДн №1 «Контрагенты»

Угроза	Возможность реализации угрозы	Показатель опасности угрозы	Актуальность
Угрозы утечки видовой информации	Средняя	Высокая	Актуальная
Угроза действия вредоносных программ (вирусов)	Высокая	Высокая	Актуальная
Установка ПО, не связанного с исполнением служебных обязанностей	Средняя	Средняя	Актуальная
Угроза разглашения информации, модификация, уничтожение сотрудниками допущенными к ее обработке	Средняя	Средняя	Актуальная

Продолжение таблицы 17

Угроза	Возможность реализации угрозы	Показатель опасности угрозы	Актуальность
Утечка информации через порты ввода/вывода	Средняя	Высокая	Актуальная

Таблица 18 – Актуальность угроз для ИСПДн №2 «Сотрудники»

Угроза	Возможность реализации угрозы	Показатель опасности угрозы	Актуальность
Угрозы утечки видовой информации	Средняя	Высокая	Актуальная
Угроза действия вредоносных программ (вирусов)	Высокая	Высокая	Актуальная
Установка ПО, не связанного с исполнением служебных обязанностей	Средняя	Средняя	Актуальная
Угроза разглашения информации, модификация, уничтожение сотрудниками допущенными к ее обработке	Средняя	Средняя	Актуальная
Утечка информации через порты ввода/вывода	Средняя	Высокая	Актуальная

Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

После этого в определенном подмножестве актуальных угроз выявляется наличие угроз 1, 2 и 3 типов. По результатам анализа угроз была составлена модель угроз безопасности, представленная в таблице 19.

Таблица 19 — Модель угроз безопасности ПДн

ИСПДн №1 «Контрагенты»						
Описание угрозы	Вероятность реализации угрозы Y_2	Коэффициент реализуемости угрозы Y	Опасность угрозы	Актуальность угрозы	Последствия	Тип угрозы
Угрозы утечки видовой информации	Средняя	Средняя	Высокая	Актуальная	Нарушение К	3
Угроза действия вредоносных программ (вирусов)	Высокая	Высокая	Высокая	Актуальная	Нарушение К, Д	3
Установка ПО, не связанного с исполнением служебных обязанностей	Средняя	Средняя	Средняя	Актуальная	Нарушение К, Д	3
Угроза разглашения информации, модификация, уничтожение сотрудниками допущенными к ее обработке	Средняя	Средняя	Средняя	Актуальная	Нарушение Ц, Д	3
Утечка информации через порты ввода/вывода	Средняя	Средняя	Высокая	Актуальная	Нарушение К, Ц, Д	3

Продолжение таблицы 19

ИСПДн №2 «Сотрудники»						
Описание угрозы	Вероятность реализации угрозы Y_2	Коэффициент реализуемости угрозы Y	Опасность угрозы	Актуальность угрозы	Последствия	Тип угрозы
Угрозы утечки видовой информации	Средняя	Средняя	Высокая	Актуальная	Нарушение К	3
Угроза действия вредоносных программ (вирусов)	Высокая	Высокая	Высокая	Актуальная	Нарушение К, Д	3
Установка ПО, не связанного с исполнением служебных обязанностей	Средняя	Средняя	Средняя	Актуальная	Нарушение К, Д	3
Угроза разглашения информации, модификация, уничтожение сотрудниками допущенными к ее обработке	Средняя	Средняя	Средняя	Актуальная	Нарушение Ц, Д	3
Утечка информации через порты ввода/вывода	Средняя	Средняя	Высокая	Актуальная	Нарушение К, Ц, Д	3

4 Определение уровня защищенности информационных систем персональных данных отдела кадров

Данный этап выпускной квалификационной работы посвящен определению уровней защищенности персональных данных в отделе кадров на ФГУП ФНПЦ «ПО «Старт» им. М.В.Проценко».

Актуальной угрозой является та, что может быть реализована в ИСПДн, и представляющая опасность для ПДн. Согласно Постановлению Правительства РФ №1119 для ИСПДн существуют угрозы трех типов:

- угрозы 1 типа - связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе;
- угрозы 2 типа - связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе;
- угрозы 3 типа - не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Актуальным типом угроз в отделе кадров на ФГУП ФНПЦ «ПО «Старт» им. М.В.Проценко» является третий тип.

В отделе кадров существует две ИСПДн:

- ИСПДн №1 «Контрагенты»;
- ИСПДн №2 «Сотрудники».

ИСПДн №1 «Контрагенты» является ИС, предназначенной для работы с ПДн контрагентов предприятия, обрабатывающей более 100 000 субъектов ПДн иной категории, не являющихся сотрудниками оператора, для которой актуальны угрозы 3-го. Таким образом, для ИСПДн №1 «Контрагенты» необходимо обеспечение 3-го уровня защищенности ПДн при их обработке в ИС.

ИСПДн №2 «Сотрудники» является ИС, предназначенной для обработки ПДн сотрудников предприятия, обрабатывающей более 100 000 субъектов ПДн

иной категории, являющихся сотрудниками оператора, для которой актуальны угрозы 3-го. Таким образом, для ИСПДн №1 «Контрагенты» необходимо обеспечение 3-го уровня защищенности ПДн при их обработке в ИС. [4]

5 Определение организационных и организационно-технических требований к обеспечению уровней защищенности персональных данных в информационной системе персональных данных отдела кадров

5.1 Определение базового набора мер по обеспечению безопасности для информационных системах персональных данных

На предыдущем этапе было определено, что для ИСПДн №1 «Контрагенты» необходимо обеспечение 3-го уровня защищенности персональных данных при их обработке, таким образом, согласно Постановлению Правительства Российской Федерации от 1.11.2012 №1119 необходимо выполнение следующих требований:

- организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
- обеспечение сохранности носителей ПДн;
- утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к ПДн, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;
- использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз;
- назначение должностного лица (работника), ответственного за обеспечение безопасности ПДн в информационной системе.[4]

На основании приказа ФСТЭК России от 18.02.2013 №21 был определен базовый набор мер по обеспечению безопасности для ИСПДн №1 «Контрагенты» 3-го уровня защищенности. В него входят следующие требования:

- идентификация и аутентификация субъектов доступа и объектов доступа: ИАФ.1, ИАФ.3, ИАФ.4, ИАФ.5, ИАФ.6;

- управление доступом субъектов доступа к объектам доступа: УПД.1, УПД.2, УПД.3, УПД.4, УПД.5, УПД.6, УПД.10, УПД.11, УПД.13, УПД.14, УПД.15, УПД.16;
- защита машинных носителей персональных данных: ЗНИ.8;
- регистрация событий безопасности: РСБ.1, РСБ.2, РСБ.3, РСБ.7;
- антивирусная защита: АВЗ.1, АВЗ.2;
- контроль (анализ) защищенности персональных данных: АНЗ.1, АНЗ.2, АНЗ.3, АНЗ.4;
- защита среды виртуализации: ЗСВ.1, ЗСВ.2, ЗСВ.3, ЗСВ.9, ЗСВ.10;
- защита технических средств: ЗТС.3, ЗТС.4;
- защита информационной системы, ее средств, систем связи и передачи данных: ЗИС.3, ЗИС.20;
- управление конфигурацией информационной системы и системы защиты персональных данных: УКФ.1, УКФ.2, УКФ.3, УКФ.4. [5]

Для ИСПДн №2 «Сотрудники» необходимо обеспечение 4-го уровня защищенности персональных данных при их обработке, таким образом, согласно Постановлению Правительства Российской Федерации от 1.11.2012 №1119 необходимо выполнение следующих требований:

- организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
- обеспечение сохранности носителей ПДн;
- утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к ПДн, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;
- использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз. [4]

На основании приказа ФСТЭК России от 18.02.2013 №21 был определен базовый набор мер по обеспечению безопасности для ИСПДн №2 «Сотрудники» 4-го уровня защищенности. В него входят следующие требования:

- идентификация и аутентификация субъектов доступа и объектов доступа: ИАФ.1, ИАФ.3, ИАФ.4, ИАФ.5, ИАФ.6;
- управление доступом субъектов доступа к объектам доступа: УПД.1, УПД.2, УПД.3, УПД.4, УПД.5, УПД.6, УПД.13, УПД.14, УПД.15, УПД.16;
- регистрация событий безопасности: РСБ.1, РСБ.2, РСБ.3, РСБ.7;
- антивирусная защита: АВЗ.1, АВЗ.2;
- контроль (анализ) защищенности персональных данных: АНЗ.2;
- защита среды виртуализации: ЗСВ.1, ЗСВ.2;
- защита технических средств: ЗТС.3, ЗТС.4;
- защита информационной системы, ее средств, систем связи и передачи данных: ЗИС.3; [5]

5.2 Адаптация и уточнение мер по обеспечению безопасности персональных данных в информационной системе персональных данных «Контрагенты»

Далее была произведена адаптация и уточнение мер по обеспечению безопасности ПДн в ИСПДн №1 «Контрагенты» с учетом не выбранных ранее мер, приведенных в приказе ФСТЭК от 18 февраля 2013 г. N 21. В результате были определены меры по обеспечению безопасности ПДн, которые направлены на нейтрализацию всех актуальных угроз безопасности ПДн для конкретной ИС. Результаты приведены в таблице 20.

Таблица 20 — Адаптация и уточнение мер по обеспечению безопасности ПДн в ИСПДн №1 «Контрагенты»

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 сотрудником оператора.
УПД.12 Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки		+	Добавлена для сохранения атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки
УПД.13 Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	+		Исключена из набора мер в связи с отсутствием внешних информационно-телекоммуникационных сетей в организации.
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.
УПД.16 Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	+		Исключена из набора мер в связи с отсутствием взаимодействия организации с информационными системами сторонних организаций.

Продолжение таблицы 20

Мера по обеспечению безопасности ПДн	Адаптация	Уточнение	Обоснование
ЗНИ.4 Исключение возможности несанкционированного ознакомления с содержанием персональных данных, хранящихся на машинных носителях, и (или) использования носителей персональных данных в иных информационных системах		+	Добавлена для предотвращения утечки персональных данных путем несанкционированного доступа к ним
РСБ.4 Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти		+	Добавлена для предотвращения переполнения объема памяти
ОЦІ.7 Контроль точности, полноты и правильности данных, вводимых в информационную систему		+	Добавлена для предотвращения введения ложной информации.
ЗСВ Защита среды виртуализации	+		Исключены все меры, связанные со средой виртуализации в связи с отсутствием среды виртуализации в данной организации.
ЗИС.20 Защита беспроводных соединений, применяемых в информационной системе	+		Исключена из набора мер в связи с отсутствием беспроводных соединений в организации.

С учетом адаптированного и уточненного перечня мер по обеспечению безопасности для ИСПДн №1 «Контрагенты» было составлено описание полученного набора мер.

5.3 Описание защитных мер для ИСПДн №1 «Контрагенты»

5.3.1 Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ).

В ИС предусмотрена идентификация и аутентификация пользователей, являющихся работниками оператора.

При доступе в ИС осуществляется идентификация и аутентификация пользователей, являющихся работниками оператора, и процессов, запускаемых от имени этих пользователей, а также процессов, запускаемых от имени системных учетных записей.

В ИС существует возможность однозначного сопоставления идентификатора пользователя с запускаемыми от его имени процессами.

В ИС до начала информационного взаимодействия (передачи защищаемой информации от устройства к устройству) должна осуществляться идентификация и аутентификация устройств (технических средств).

Характеристики пароля:

- минимальная длина должна быть не менее 8 символов;
- алфавит должен состоять из латинских букв в двух регистрах и цифр;
- минимальный срок действия пароля должен составлять 60 дней;
- максимальное количество неуспешных попыток должно составлять 6;
- вводимые символы пароля отображаются условными знаками «*».

5.3.2 Управление доступом субъектов доступа к объектам доступа (УПД).

В обязанности администратора ИС входит создание, активация, блокирование и уничтожение учетных записей пользователей. Основываясь на задачах, решаемых пользователями в ИС и взаимодействующими с ней ИС, администратор ИС предоставляет пользователям права доступа к объектам доступа ИС.

Администратором должны быть использованы автоматизированные средства поддержки управления учетными записями пользователей.

По окончании установленного периода времени использования учетных записей они блокируются. Период времени неиспользования равен 45 дням.

В ИСПДн №1 «Контрагенты» используется ролевой метод управления доступом. Правила разграничения доступа реализуются на основе установленных администратором матриц доступа.

В ИС осуществляется управление информационными потоками при передаче информации между устройствами.

При достижении максимального числа неуспешных попыток доступа учетная запись пользователя автоматически блокируется и может быть разблокирована только администратором.

Блокирование сеанса пользователя происходит при его не активности в течение 5 минут, при этом происходит затухание экрана.

Работникам оператора не разрешены какие-либо действия до прохождения ими процедуры идентификации и аутентификации.

В ИС обеспечивается поддержка (обновление, назначение, изменение) и сохранение атрибутов безопасности (меток безопасности), установленных оператором, связанных с информацией в процессе ее хранения и обработки.

Администратор устанавливает ограничения на использование мобильных технических средств в соответствии с задачами ИС, также осуществляется мониторинг и контроль применения мобильных технических средств на предмет их несанкционированного использования.

В ИС обеспечивается исключение НСД в программном и (или) техническим ресурсам средства вычислительной техники ИС на этапе его загрузки, для этого необходимо осуществлять:

- блокирование попыток несанкционированной загрузки нештатной ОС (среды) или недоступность информационных ресурсов для чтения или модификации в случае загрузки нештатной ОС;
- контроль доступа пользователей к процессу загрузки операционной системы;
- контроль целостности ПО и аппаратных компонентов средств вычислительной техники.

В ИС применяется доверенная загрузка на уровне базовой системы ввода-

вывода.

5.3.3 Защита машинных носителей персональных данных (ЗНИ).

Съемные машинные носители учитываются с присвоением им регистрационных номеров. Учет съемных машинных носителей информации ведется в журналах учета машинных носителей информации.

При маркировке машинных носителей информации администратора указывает информацию о возможности использования машинного носителя информации вне ИС и информацию о возможности использования машинного носителя информации за пределами КЗ, также администратор определяет должностных лиц, имеющих физический доступ к машинным носителям информации, уточняя к каким именно носителям доступ разрешен.

Администратор обеспечивает исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных ИС. Для этого осуществляется контроль доступа в помещения, предназначенные для хранения машинных носителей.

При передаче машинных носителей администратор безопасности должен обеспечить уничтожение информации на них, при этом оператором должны быть обеспечены регистрация и контроль действий по удалению защищаемой информации и уничтожению машинных носителей информации, также оператором должны проводиться периодическая проверка процедур и тестирование средств стирания информации и контроля удаления информации, кроме того, оператором перед подключением к ИС должно быть обеспечено уничтожение (стирание) информации с носителей информации после их приобретения и при первичном подключении к ИС, при использовании в иных ИС, при передаче для постоянного использования от одного пользователя другому пользователю, после возвращения из ремонта, а также в иных случаях, определяемых оператором. При уничтожении администратором должна применяться полная многократная перезапись машинного носителя информации специальными битовыми последова-

тельностью, зависящими от типа накопителя и используемого метода кодирования информации, затем очистка всего физического пространства накопителя, включая сбойные и резервные элементы памяти специализированными программами или утилитами производителя.

5.3.4 Регистрация событий безопасности (РСБ).

Администратор ИС определяет события безопасности, подлежащие регистрации и сроки их хранения. К событиям безопасности, подлежащим регистрации в ИС, должны быть отнесены любые проявления состояния ИС и ее СЗИ, указывающие на возможность нарушения конфиденциальности, целостности или доступности информации, доступности компонентов ИС, нарушения процедур, установленных организационно-распорядительными документами по защите информации оператора, а также на нарушение штатного функционирования СЗИ. Перечень событий безопасности пересматривается администратором 1 раз в год. В перечень должны входить события безопасности, связанные с действиями администраторов. Осуществляется хранение записей о выявленных событиях безопасности и записей системных журналов.

Состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности включают дату и время события безопасности, идентификационную информацию источника события безопасности, результат события безопасности (успешно или неуспешно), субъект доступа (пользователь и (или) процесс), связанный с данным событием безопасности, дополнительно осуществляется полнотекстовая запись системных команд.

При возникновении сбоев регистрации событий безопасности, в том числе аппаратных и программных ошибок, сбоев в механизмах сбора информации и достижения предела или переполнения объема (емкости) памяти администратор ИС незамедлительно должен сообщить об этом администратору безопасности для принятия мер по предотвращению ошибок.

Записи событий безопасности хранятся в течение двух лет.

Доступ к записям аудита предоставляется только уполномоченным

должностным лицам, также осуществляется резервное копирование событий аудита.

5.3.5 Антивирусная защита (АВЗ).

Администратор устанавливает средства антивирусной защиты на каждое АРМ, используемое в ИСПДн. В промышленном предприятии используется антивирус «Kaspersky Endpoint Security 8». Управление осуществляется администратором безопасности централизованно. Обновление базы данных производится каждые 10 дней администратором.

5.3.6 Контроль (анализ) защищенности персональных данных (АНЗ)

Порядок выявления, анализа и устранения уязвимостей в информационной системе:

- выявление (поиск) уязвимостей, связанных с ошибками кода в программном (микропрограммном) обеспечении (общесистемном, прикладном, специальном), а также ПО СЗИ, правильностью установки и настройки СЗИ, технических средств и ПО, а также корректностью работы СЗИ при их взаимодействии с техническими средствами и ПО;
- разработка по результатам выявления (поиска) уязвимостей отчетов с описанием выявленных уязвимостей и планом мероприятий по их устранению;
- анализ отчетов с результатами поиска уязвимостей и оценки достаточности реализованных мер защиты информации;
- устранение выявленных уязвимостей, в том числе путем установки обновлений ПО СЗИ, общесистемного ПО, прикладного ПО или микропрограммного обеспечения технических средств.

Контроль установки обновлений проводится с один раз в шесть месяцев и фиксируется в соответствующих журналах.

При контроле работоспособности, параметров настройки и правильности функционирования ПО и СЗИ осуществляется:

- контроль работоспособности (неотключения) ПО и СЗИ;
- проверка правильности функционирования (тестирование на тестовых данных, приводящих к известному результату) ПО и СЗИ, объем и

содержание которой определяется оператором;

- контроль соответствия настроек ПО и СЗИ параметрам настройки, приведенным в эксплуатационной документации на систему защиты информации и СЗИ;

- восстановление работоспособности (правильности функционирования) и параметров настройки ПО И СЗИ (при необходимости), в том числе с использованием резервных копий и (или) дистрибутивов.

При контроле состава технических средств, ПО и СЗИ осуществляется:

- контроль соответствия состава технических средств, ПО и СЗИ приведенному в эксплуатационной документации с целью поддержания актуальной (установленной в соответствии с эксплуатационной документацией) конфигурации ИС и принятие мер, направленных на устранение выявленных недостатков;

- контроль состава технических средств, ПО и СЗИ на соответствие сведениям действующей (актуализированной) эксплуатационной документации и принятие мер, направленных на устранение выявленных недостатков;

- контроль выполнения условий и сроков действия сертификатов соответствия на СЗИ и принятие мер, направленных на устранение выявленных недостатков;

- исключение (восстановление) из состава ИС несанкционированно установленных (удаленных) технических средств, ПО и СЗИ.

В ИС обеспечивается регистрация событий, связанных со сменой паролей пользователей, заведением и удалением учетных записей пользователей, изменением правил разграничения доступа и полномочий пользователей.

5.3.7 Контроль (анализ) защищенности персональных данных (АНЗ).

Порядок выявления, анализа и устранения уязвимостей в информационной системе:

- выявление (поиск) уязвимостей, связанных с ошибками кода в программном (микропрограммном) обеспечении (общесистемном, прикладном, специальном), а также ПО СЗИ, правильностью установки и настройки СЗИ,

технических средств и ПО, а также корректностью работы СЗИ при их взаимодействии с техническими средствами и ПО;

- разработка по результатам выявления (поиска) уязвимостей отчетов с описанием выявленных уязвимостей и планом мероприятий по их устранению;
- анализ отчетов с результатами поиска уязвимостей и оценки достаточности реализованных мер защиты информации;
- устранение выявленных уязвимостей, в том числе путем установки обновлений ПО СЗИ, общесистемного ПО, прикладного ПО или микропрограммного обеспечения технических средств.

Контроль установки обновлений проводится с один раз в шесть месяцев и фиксируется в соответствующих журналах.

При контроле работоспособности, параметров настройки и правильности функционирования ПО и СЗИ осуществляется:

- контроль работоспособности (неотключения) ПО и СЗИ;
- проверка правильности функционирования (тестирование на тестовых данных, приводящих к известному результату) ПО и СЗИ, объем и содержание которой определяется оператором;
- контроль соответствия настроек ПО и СЗИ параметрам настройки, приведенным в эксплуатационной документации на систему защиты информации и СЗИ;
- восстановление работоспособности (правильности функционирования) и параметров настройки ПО и СЗИ (при необходимости), в том числе с использованием резервных копий и (или) дистрибутивов.

При контроле состава технических средств, ПО и СЗИ осуществляется:

- контроль соответствия состава технических средств, ПО и СЗИ приведенному в эксплуатационной документации с целью поддержания актуальной (установленной в соответствии с эксплуатационной документацией) конфигурации ИС и принятие мер, направленных на устранение выявленных недостатков;
- контроль состава технических средств, ПО и СЗИ на соответствие

сведениям действующей (актуализированной) эксплуатационной документации и принятие мер, направленных на устранение выявленных недостатков;

- контроль выполнения условий и сроков действия сертификатов соответствия на СЗИ и принятие мер, направленных на устранение выявленных недостатков;
- исключение (восстановление) из состава ИС несанкционированно установленных (удаленных) технических средств, ПО и СЗИ.

В ИС обеспечивается регистрация событий, связанных со сменой паролей пользователей, заведением и удалением учетных записей пользователей, изменением правил разграничения доступа и полномочий пользователей.

5.3.8 Защита технических средств (ЗТС).

Администратор безопасности обеспечивает контроль и управление физическим доступом к техническим средствам, СЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, СЗИ и средствам обеспечения функционирования ИС и помещения и сооружения, в которых они установлены.

Контроль и управление физическим доступом должны предусматривает:

- определение лиц, допущенных к техническим средствам, СЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены;
- санкционирование физического доступа к техническим средствам, СЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены;
- учет физического доступа к техническим средствам, СЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены.

Устройства вывода информации (принтеры, мониторы) размещаются таким образом, чтобы исключить ее несанкционированный просмотр.

5.3.9 Защита информационной системы, ее средств и систем связи и передачи данных (ЗИС).

В ИС осуществляется обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов (защита от атак типа «человек посередине»). После окончания сетевого соединения идентификатор сеанса связи признается недействительным.

В ИС обеспечивается защита архивных файлов, параметров настройки СЗИ и ПО, иных данных, не подлежащих изменению в процессе обработки информации.

ИС разбивается на сегменты, периметры сегментов защищаются.

5.3.10 Управление конфигурацией ИС и системы защиты ПДн (УКФ).

В организационно-распорядительных документах по защите ПДн организации, определяются лица, которым разрешены действия по внесению изменений в конфигурацию ИС и системы защиты ПДн.

В организационно-распорядительных документах по защите ПДн, определяются порядок управления изменениями конфигурации ИС и системы защиты ПДн.

В организации проводится анализ потенциального воздействия планируемых изменений в конфигурации ИС и системы защиты ПДн на обеспечение защиты ПДн.

Все изменения в конфигурации ИС и системы защиты ПДн документируются.

5.4 Адаптация и уточнение мер по обеспечению безопасности персональных данных в информационной системе персональных данных «Сотрудники»

Далее аналогично была произведена адаптация и уточнение мер по обеспечению безопасности ПДн в ИСПДн №2 «Сотрудники» с учетом не выбранных

ранее мер, приведенных в приказе ФСТЭК от 18 февраля 2013 г. N 21. Результаты приведены в таблице 21.

Таблица 21 — Адаптация и уточнение мер по обеспечению безопасности ПДн в ИСПДн №2 «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 сотрудником оператора.
УПД.13 Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	+		Исключена из набора мер в связи с отсутствием внешних информационно-телекоммуникационных сетей в организации.
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.
ЗНИ.4 Исключение возможности несанкционированного ознакомления с содержанием персональных данных, хранящихся на машинных носителях, и (или) использования носителей персональных данных в иных информационных системах		+	Добавлена для предотвращения утечки персональных данных путем несанкционированного доступа к ним.
РСБ.4 Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти		+	Добавлена для предотвращения переполнения объема памяти
ОЦЛ.7 Контроль точности, полноты и правильности данных, вводимых в информационную систему		+	Добавлена для предотвращения введения ложной информации.

Продолжение таблицы 21

Мера по обеспечению безопасности ПДн	Адаптация	Уточнение	Обоснование
ЗСВ Защита среды виртуализации	+		Исключены все меры, связанные со средой виртуализации в связи с отсутствием среды виртуализации в данной организации.

С учетом адаптированного и уточненного перечня мер по обеспечению безопасности для ИСПДн №2 «Сотрудники» было составлено описание полученного набора мер.

5.5 Описание защитных мер для ИСПДн №2 «Сотрудники»

5.5.1 Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ).

В ИС предусмотрена идентификация и аутентификация пользователей, являющихся работниками оператора.

При доступе в ИС осуществляется идентификация и аутентификация пользователей, являющихся работниками оператора, и процессов, запускаемых от имени этих пользователей, а также процессов, запускаемых от имени системных учетных записей.

В ИС существует возможность однозначного сопоставления идентификатора пользователя с запускаемыми от его имени процессами.

В ИС до начала информационного взаимодействия (передачи защищаемой информации от устройства к устройству) должна осуществляться идентификация и аутентификация устройств (технических средств).

Характеристики пароля:

- минимальная длина должна быть не менее 8 символов;
- алфавит должен состоять из латинских букв в двух регистрах и цифр;
- минимальный срок действия пароля должен составлять 60 дней;
- максимальное количество неуспешных попыток должно составлять 6;
- вводимые символы пароля отображаются условными знаками «*».

5.5.2 Управление доступом субъектов доступа к объектам доступа (УПД).

В обязанности администратора ИС входит заведение, активация, блокирование и уничтожение учетных записей пользователей, предоставление пользователям прав доступа к объектам доступа ИС, основываясь на задачах, решаемых пользователями в ИС и взаимодействующими с ней ИС.

Администратором используются автоматизированные средства поддержки управления учетными записями пользователей.

По окончании установленного периода времени использования учетных записей они блокируются. Период времени неиспользования равен 45 дням.

В ИСПДн №1 «Контрагенты» используется ролевой метод управления доступом. Правила разграничения доступа реализуются на основе установленных администратором матриц доступа.

В ИС осуществляется управление информационными потоками при передаче информации между устройствами.

При достижении максимального числа неуспешных попыток доступа учетная запись пользователя автоматически блокируется и может быть разблокирована только администратором.

Блокирование сеанса пользователя происходит при его не активности в течение 5 минут, при этом происходит гашение экрана.

До прохождения процедуры идентификации и аутентификации работникам оператора не разрешены никакие действия.

В ИС обеспечивается поддержка (обновление, назначение, изменение) и сохранение атрибутов безопасности (меток безопасности), установленных оператором, связанных с информацией в процессе ее хранения и обработки.

Администратором устанавливаются ограничения на использование мобильных технических средств в соответствии с задачами ИС, также осуществляется мониторинг и контроль применения мобильных технических средств на предмет их несанкционированного использования.

В ИС обеспечивается исключение НСД в программным и (или) техническим ресурсам средства вычислительной техники ИС на этапе его загрузки, для

этого необходимо осуществлять:

- блокирование попыток несанкционированной загрузки нештатной ОС (среды) или недоступность информационных ресурсов для чтения или модификации в случае загрузки нештатной ОС;
- контроль доступа пользователей к процессу загрузки операционной системы;
- контроль целостности ПО и аппаратных компонентов средств вычислительной техники.

В ИС применяется доверенная загрузка на уровне базовой системы ввода-вывода.

5.5.3 Регистрация событий безопасности (РСБ).

Администратор ИС определяет события безопасности, подлежащие регистрации и сроки их хранения. К событиям безопасности, подлежащим регистрации в ИС, должны быть отнесены любые проявления состояния ИС и ее СЗИ, указывающие на возможность нарушения конфиденциальности, целостности или доступности информации, доступности компонентов ИС, нарушения процедур, установленных организационно-распорядительными документами по защите информации оператора, а также на нарушение штатного функционирования СЗИ. Перечень событий безопасности пересматривается администратором 1 раз в год. В перечень должны входить события безопасности, связанные с действиями администраторов. Осуществляется хранение записей о выявленных событиях безопасности и записей системных журналов.

Состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности включают дату и время события безопасности, идентификационную информацию источника события безопасности, результат события безопасности (успешно или неуспешно), субъект доступа (пользователь и (или) процесс), связанный с данным событием безопасности, дополнительно осуществляется полнотекстовая запись системных команд.

При возникновении сбоев регистрации событий безопасности, в том числе

аппаратных и программных ошибок, сбоев в механизмах сбора информации и достижения предела или переполнения объема (емкости) памяти администратор ИС незамедлительно должен сообщить об этом администратору безопасности для принятия мер по предотвращению ошибок.

Записи событий безопасности хранятся в течение двух лет.

Доступ к записям аудита предоставляется только уполномоченным должностным лицам, также осуществляется резервное копирование событий аудита.

5.5.4 Антивирусная защита (АВЗ).

Администратор устанавливает средства антивирусной защиты на каждое АРМ, используемое в ИСПДн. В промышленном предприятии используется антивирус «Kaspersky Endpoint Security 8». Управление осуществляется администратором безопасности централизованно. Обновление базы данных производится каждые 10 дней администратором.

5.5.5 Контроль (анализ) защищенности персональных данных (АНЗ)

Порядок выявления, анализа и устранения уязвимостей в информационной системе:

- выявление (поиск) уязвимостей, связанных с ошибками кода в программном (микропрограммном) обеспечении (общесистемном, прикладном, специальном), а также ПО СЗИ, правильностью установки и настройки СЗИ, технических средств и ПО, а также корректностью работы СЗИ при их взаимодействии с техническими средствами и ПО;
- разработка по результатам выявления (поиска) уязвимостей отчетов с описанием выявленных уязвимостей и планом мероприятий по их устранению;
- анализ отчетов с результатами поиска уязвимостей и оценки достаточности реализованных мер защиты информации;
- устранение выявленных уязвимостей, в том числе путем установки обновлений ПО СЗИ, общесистемного ПО, прикладного ПО или микропрограммного обеспечения технических средств.

Контроль установки обновлений проводится с один раз в шесть месяцев и

фиксируется в соответствующих журналах.

При контроле работоспособности, параметров настройки и правильности функционирования ПО и СЗИ осуществляется:

- контроль работоспособности (неотключения) ПО и СЗИ;
- проверка правильности функционирования (тестирование на тестовых данных, приводящих к известному результату) ПО и СЗИ, объем и содержание которой определяется оператором;
- контроль соответствия настроек ПО и СЗИ параметрам настройки, приведенным в эксплуатационной документации на систему защиты информации и СЗИ;
- восстановление работоспособности (правильности функционирования) и параметров настройки ПО и СЗИ (при необходимости), в том числе с использованием резервных копий и (или) дистрибутивов.

При контроле состава технических средств, ПО и СЗИ осуществляется:

- контроль соответствия состава технических средств, ПО и СЗИ приведенному в эксплуатационной документации с целью поддержания актуальной (установленной в соответствии с эксплуатационной документацией) конфигурации ИС и принятие мер, направленных на устранение выявленных недостатков;
- контроль состава технических средств, ПО и СЗИ на соответствие сведениям действующей (актуализированной) эксплуатационной документации и принятие мер, направленных на устранение выявленных недостатков;
- контроль выполнения условий и сроков действия сертификатов соответствия на СЗИ и принятие мер, направленных на устранение выявленных недостатков;
- исключение (восстановление) из состава ИС несанкционированно установленных (удаленных) технических средств, ПО и СЗИ.

В ИС обеспечивается регистрация событий, связанных со сменой паролей пользователей, заведением и удалением учетных записей пользователей, изменением правил разграничения доступа и полномочий пользователей.

5.5.6 Контроль (анализ) защищенности персональных данных (АНЗ).

Порядок выявления, анализа и устранения уязвимостей в информационной системе:

- выявление (поиск) уязвимостей, связанных с ошибками кода в программном (микропрограммном) обеспечении (общесистемном, прикладном, специальном), а также ПО СЗИ, правильностью установки и настройки СЗИ, технических средств и ПО, а также корректностью работы СЗИ при их взаимодействии с техническими средствами и ПО;
- разработка по результатам выявления (поиска) уязвимостей отчетов с описанием выявленных уязвимостей и планом мероприятий по их устранению;
- анализ отчетов с результатами поиска уязвимостей и оценки достаточности реализованных мер защиты информации;
- устранение выявленных уязвимостей, в том числе путем установки обновлений ПО СЗИ, общесистемного ПО, прикладного ПО или микропрограммного обеспечения технических средств.

Контроль установки обновлений проводится с один раз в шесть месяцев и фиксируется в соответствующих журналах.

При контроле работоспособности, параметров настройки и правильности функционирования ПО и СЗИ осуществляется:

- контроль работоспособности (неотключения) ПО и СЗИ;
- проверка правильности функционирования (тестирование на тестовых данных, приводящих к известному результату) ПО и СЗИ, объем и содержание которой определяется оператором;
- контроль соответствия настроек ПО и СЗИ параметрам настройки, приведенным в эксплуатационной документации на систему защиты информации и СЗИ;
- восстановление работоспособности (правильности функционирования) и параметров настройки ПО и СЗИ (при необходимости), в том числе с использованием резервных копий и (или) дистрибутивов.

При контроле состава технических средств, ПО и СЗИ осуществляется:

- контроль соответствия состава технических средств, ПО и СЗИ приведенному в эксплуатационной документации с целью поддержания актуальной (установленной в соответствии с эксплуатационной документацией) конфигурации ИС и принятие мер, направленных на устранение выявленных недостатков;
- контроль состава технических средств, ПО и СЗИ на соответствие сведениям действующей (актуализированной) эксплуатационной документации и принятие мер, направленных на устранение выявленных недостатков;
- контроль выполнения условий и сроков действия сертификатов соответствия на СЗИ и принятие мер, направленных на устранение выявленных недостатков;
- исключение (восстановление) из состава ИС несанкционированно установленных (удаленных) технических средств, ПО и СЗИ.

В ИС обеспечивается регистрация событий, связанных со сменой паролей пользователей, заведением и удалением учетных записей пользователей, изменением правил разграничения доступа и полномочий пользователей.

5.5.7 Защита технических средств (ЗТС).

Администратор безопасности обеспечивает контроль и управление физическим доступом к техническим средствам, СЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, СЗИ и средствам обеспечения функционирования ИС и помещения и сооружения, в которых они установлены.

Контроль и управление физическим доступом должны предусматривает:

- определение лиц, допущенных к техническим средствам, СЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены;
- санкционирование физического доступа к техническим средствам, СЗИ, средствам обеспечения функционирования, а также в помещения и

сооружения, в которых они установлены;

- учет физического доступа к техническим средствам, СЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены.

Устройства вывода информации (принтеры, мониторы) размещаются таким образом, чтобы исключить ее несанкционированный просмотр.

5.5.8 Защита информационной системы, ее средств и систем связи и передачи данных (ЗИС).

Администратором обеспечивается защита информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны. Защита информации обеспечивается путем защиты каналов связи от несанкционированного физического доступа (подключения) к ним и (или) применения в соответствии с законодательством Российской Федерации средств криптографической защиты информации или иными методами.

В ИС осуществляется обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов (защита от атак типа «человек посередине»). После окончания сетевого соединения идентификатор сеанса связи признается недействительным.

В ИС обеспечивается защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения, иных данных, не подлежащих изменению в процессе обработки информации.

ИС разбивается на сегменты, периметры сегментов защищаются.

6 Выбор и обоснование средств защиты информации для автоматизированной системы «Отдел кадров» в защищенном исполнении

Было проведено сопоставление защитных мер к каждой угрозе и угроз к каждой защитной мере для ИСПДн №1 «Контрагенты». Результаты представлены в таблицах 22 и 23 соответственно.

Таблица 22 – Сопоставление защитных мер для устранения каждой актуальной угрозы для ИСПДн №1 «Контрагенты»

Наименование угрозы	Перечень защитных мер для её устранения
Угрозы утечки видовой информации [У1]	УПД.10, ЗТС.3, ЗТС.4
Угроза действия вредоносных программ (вирусов) [У2]	УПД.17, РСБ.1, РСБ.2, РСБ.3, РСБ.4, РСБ.7, АВЗ.1, АВЗ.2, ОЦЛ.4, СОВ.1, СОВ.2, АНЗ.1
Установка ПО, не связанного с исполнением служебных обязанностей [У3]	ОПС.3, ЗНИ.7, АНЗ.2
Угроза разглашения информации, модификация, уничтожение сотрудниками допущенными к ее обработке [У4]	УПД.1, УПД.2, УПД.3, УПД.4, УПД.5, УПД.6, УПД.11, УПД.12, УПД.15, ИАФ.1, ИАФ.3, ИАФ.4, ИАФ.5, ЗНИ.4, РСБ.1, РСБ.2, РСБ.3, РСБ.4, РСБ.7, ОЦЛ.7, ЗИС.3, УКФ.1, УКФ.3
Утечка информации через порты ввода/вывода [У5]	ИАФ.1, ИАФ.3, ИАФ.4, ИАФ.5, УПД.1, УПД.2, УПД.3, УПД.4, УПД.5, УПД.6, УПД.11, УПД.12, УПД.15, РСБ.1, РСБ.2, РСБ.3, РСБ.7, ЗНИ.4, АНЗ.4

Таблица 23 – Сопоставление актуальных угроз для каждой защитной меры для ИСПДн №1 «Контрагенты»

Защитные меры	Угрозы
ИАФ.1	У4, У5
ИАФ.3	У4, У5
ИАФ.4	У4, У5
ИАФ.5	У4, У5
УПД.1	У4, У5
УПД.2	У4, У5
УПД.3	У4, У5
УПД.4	У4, У5
УПД.5	У4, У5

Продолжение таблицы 23

Защитные меры	Угрозы
УПД.6	У4, У5
УПД.10	У1
УПД.11	У4, У5
УПД.12	У4, У5
УПД.15	У4, У5
ЗНИ.4	У4, У5
ЗНИ.7	У3
РСБ.1	У2, У4, У5
РСБ.2	У2, У4, У5
РСБ.3	У2, У4, У5
РСБ.4	У2, У4
РСБ.7	У2, У4, У5
АВЗ.1	У2
АВЗ.2	У2
АНЗ.1	У2
АНЗ.2	У3
АНЗ.4	У5
ЗИС.3	У4
ЗТС.3	У1
ЗТС.4	У1
УКФ.1	У4
УКФ.3	У4
ОЦЛ.7	У4

Сопоставление защитных мер к каждой угрозе и угроз к каждой защитной мере для ИСПДн №2 «Сотрудники» представлено в таблицах 24 и 25 соответственно.

Таблица 24 – Сопоставление защитных мер для устранения каждой актуальной угрозы для ИСПДн №2 «Сотрудники»

Наименование угрозы	Перечень защитных мер для её устранения
Угрозы утечки видовой информации [У1]	УПД.10, ЗТС.3, ЗТС.4

Продолжение таблицы 24

Наименование угрозы	Перечень защитных мер для её устранения
Угроза действия вредоносных программ (вирусов) [У2]	УПД.17, РСБ.1, РСБ.2, РСБ.3, РСБ.4, РСБ.7, АВЗ.1, АВЗ.2, ОЦЛ.4, СОВ.1, СОВ.2, АНЗ.1
Установка ПО, не связанного с исполнением служебных обязанностей [У3]	ОПС.3, ЗНИ.7, АНЗ.2
Угроза разглашения информации, модификация, уничтожение сотрудниками допущенными к ее обработке [У4]	УПД.1, УПД.2, УПД.3, УПД.4, УПД.5, УПД.6, УПД.11, УПД.12, УПД.15, ИАФ.1, ИАФ.3, ИАФ.4, ИАФ.5, ЗНИ.4, РСБ.1, РСБ.2, РСБ.3, РСБ.4, РСБ.7, ОЦЛ.7, ЗИС.3, УКФ.1, УКФ.3
Утечка информации через порты ввода/вывода [У5]	ИАФ.1, ИАФ.3, ИАФ.4, ИАФ.5, УПД.1, УПД.2, УПД.3, УПД.4, УПД.5, УПД.6, УПД.11, УПД.12, УПД.15, РСБ.1, РСБ.2, РСБ.3, РСБ.7, ЗНИ.4, АНЗ.4

Таблица 25 – Сопоставление актуальных угроз для каждой защитной меры для ИСПДн №2 «Сотрудники»

Защитные меры	Угрозы
ИАФ.1	У4, У5
ИАФ.3	У4, У5
ИАФ.4	У4, У5
ИАФ.5	У4, У5
УПД.1	У4, У5
УПД.2	У4, У5
УПД.3	У4, У5
УПД.4	У4, У5
УПД.5	У4, У5
УПД.6	У4, У5
УПД.10	У1
УПД.11	У4, У5
УПД.12	У4, У5
УПД.15	У4, У5
ЗНИ.4	У4, У5
ЗНИ.7	У3
РСБ.1	У2, У4, У5
РСБ.2	У2, У4, У5

Продолжение таблицы 25

Защитные меры	Угрозы
РСБ.3	У2, У4, У5
РСБ.4	У2, У4
РСБ.7	У2, У4, У5
АВЗ.1	У2
АВЗ.2	У2
АНЗ.1	У2
АНЗ.2	У3
АНЗ.4	У5
ЗИС.3	У4
ЗТС.3	У1
ЗТС.4	У1
УКФ.1	У4
УКФ.3	У4
ОЦЛ.7	У4

На АРМ установлена операционная система Microsoft Windows 7.

В целях защиты информации от НСД локального, а также со стороны ЛВС и открытых каналов связи в АС используется СЗИ НСД «Secret Net Studio 8.0»

СЗИ НСД «Secret Net Studio» имеет сертификат № 3745 от 16.05.2017г., действительный до 16.05.2020 г., выданный ФСТЭК России, соответствует требованиям документов: РД СВТ (5), Требования к САВЗ (А четвертого класса защиты. ИТ.САВЗ.А4.ПЗ), Требования к САВЗ (Б четвертого класса защиты. ИТ.САВЗ.Б4.ПЗ), Требования к САВЗ (В четвертого класса защиты. ИТ.САВЗ.В4.ПЗ), Требования к САВЗ (Г четвертого класса защиты. ИТ.САВЗ.Г4.ПЗ), Требования к СКН, Профиль защиты СКН (контроля подключения съемных машинных носителей информации четвертого класса защиты. ИТ.СКН.П4.ПЗ), Требования к МЭ, Профиль защиты МЭ (В четвертого класса защиты. ИТ.МЭ.В4.ПЗ), Требования к СОВ (узла четвертого класса защиты. ИТ.СОВ.У4.ПЗ), РД НДВ (4).

Антивирусная программа «Kaspersky Endpoint Security 10 для Windows» имеет сертификат № 3025 от 25.11.2013 г., действительный до 25.11.2019 г., выданный ФСТЭК России на соответствие требованиям документов «Требования к

средствам антивирусной защиты» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа Б второго класса защиты. ИТ.САВЗ.Б2.ПЗ» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа В второго класса защиты. ИТ.САВЗ.В2.ПЗ» (ФСТЭК России, 2012) и «Профиль защиты средств антивирусной защиты типа Г второго класса защиты. ИТ.САВЗ.Г2.ПЗ» (ФСТЭК России, 2012).

Защищенный программный комплекс 1С: Предприятие, версия 8.3z имеет сертификат № 3442 от 02.09.2015 г., действительный до 02.09.2018 г., выданный ФСТЭК России на соответствие РД СВТ по 5 классу и РД НДВ по 4 уровню.

СУБД Microsoft SQL Server 2014 имеет сертификат № 3518 от 15.02.2016 г., действительный до 15.02.2019 г., выданный ФСТЭК России, системы управления базами данных Microsoft SQL Server 2014 в редакциях Enterprise Edition (EE), Business Intelligence (BI), Standard (Std), Web, Express, Express with tools - на соответствие ТУ.

Программное изделие «Kaspersky Security Center 10» имеет сертификат № 3155 от 06.05.2014 г., действительный до 06.05.2020 г., выданный ФСТЭК России, соответствует требованиям документов: Требования к САВЗ(А второго класса защиты. ИТ.САВЗ.А2.ПЗ).

Для пользователей в качестве штатных средств предусмотрены:

- «Microsoft Windows 7»;
- СЗИ НСД «Secret Net Studio 8.0»;
- «LibreOffice 6.0.4»;
- «1С: Предприятие, версия 8.3z»;
- «Консультант Плюс».

7 Описание АСЗИ «Отдел кадров»

На рисунке 6 представлена структура АСЗИ «Отдел кадров».

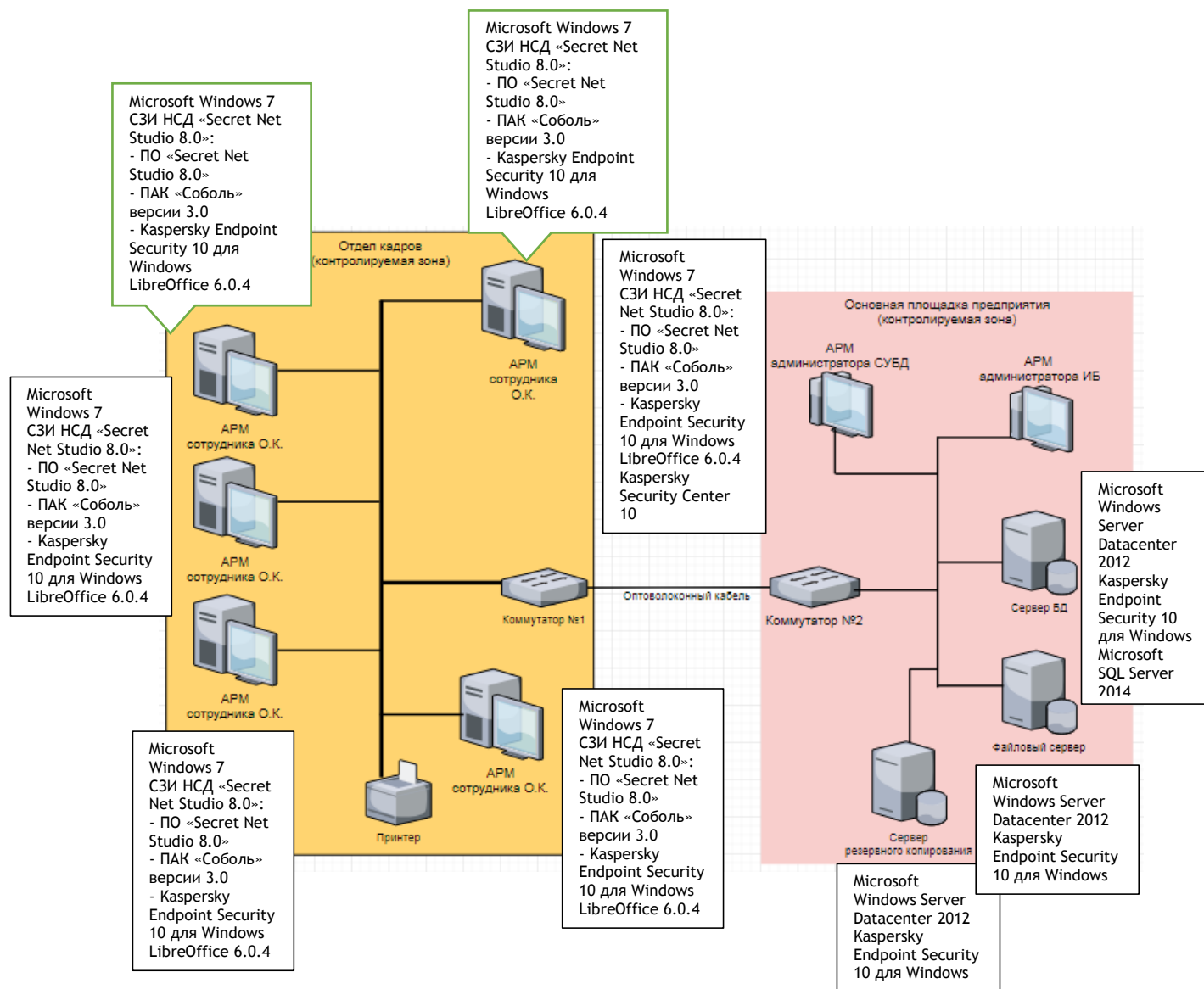


Рисунок 6 – Структура АСЗИ «Отдел кадров»

Здание отдела кадров находится под постоянной охраной. В здании действует пропускной режим входа, само здание охраняется круглосуточно. Двери в помещения отдела кадров оборудованы механическим замком, который закрыт все время, когда АРМ не эксплуатируется. Пользователи, работающие на АРМ, следят за отсутствием посторонних лиц в помещении во время работы на АРМ.

С целью защиты помещения отдела кадров от утечек информации по визуально-оптическому каналу объекты внутри помещения расположены так, чтобы исключить отражение света в стороны возможного расположения злоумышленника, а также были использованы средства преграждения или значительного ослабления отраженного света (на окна были повешены жалюзи).

После проведения мероприятий по защите помещения отдела кадров в исходный план помещения были внесены изменения. План этажа, на котором расположен отдел кадров после проведения работ по защите информации, представлен на рисунке 7.

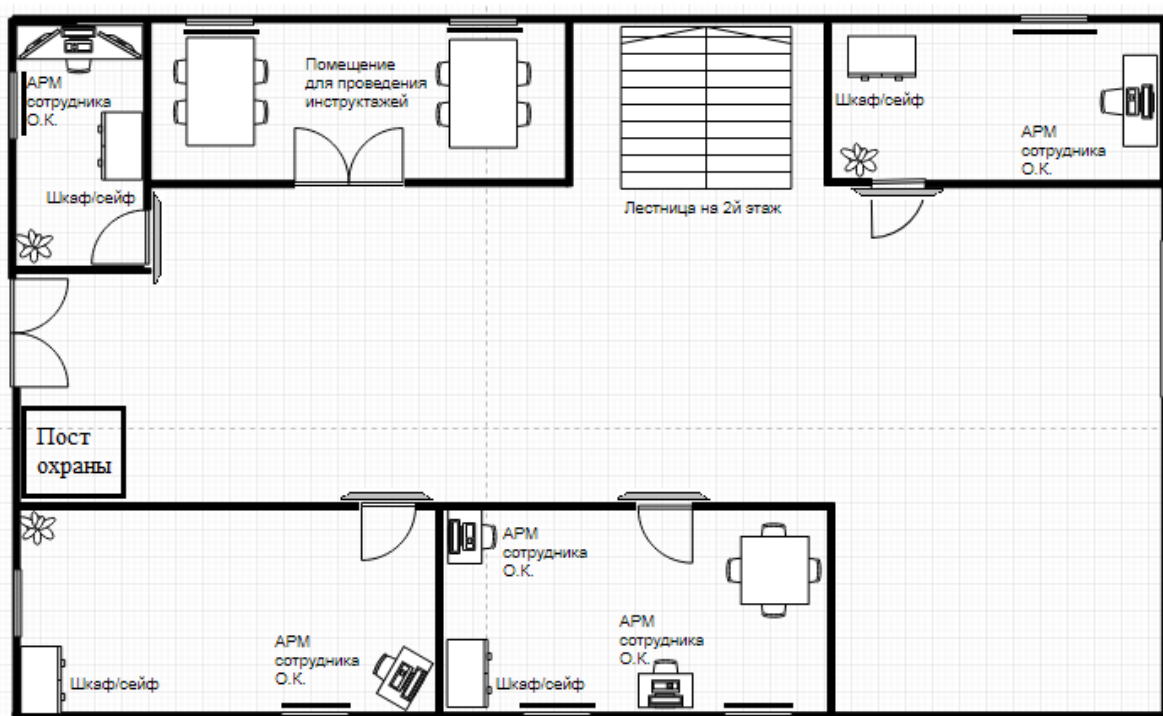


Рисунок 7 – Обновленный план помещения отдела кадров

8 Вредные психофизиологические факторы, влияющие на опорно-двигательный аппарат специалиста по защите информации, методы и средства физической культуры, снижающие их воздействие

Работа специалиста по защите информации, являющимся пользователем ЕСМИБ ТУ, сопровождается напряженностью труда. Наибольшее влияние на напряженность оказывают психофизиологические факторы. Психофизиологические факторы – факторы, обусловленные особенностями физиологии и психологии человека, которые могут нанести вреда при определенных обстоятельствах. Психофизиологические факторы могут влиять на следующие органы и состояние специалиста:

- опорно-двигательный аппарат;
- сосудисто-сердечная система;
- органы зрения;
- нервная система;
- психоэмоциональное состояние.

Психофизиологическими факторами, влияющими на опорно-двигательную систему, могут быть:

- постоянное неподвижное положение;
- интенсивная работа с клавиатурой;
- синдром запястного канала;
- неправильная осанка.

Продолжительное нахождение в неподвижном положении, положение специалиста по защите информации сидя долгое время за компьютером - всё это приводит к усталости и возникновению болей в позвоночнике, шее, плечевых суставах, а также к развитию слабости мышц и изменениям формы позвоночника.

Долгая работа за клавиатурой вызывает болевые ощущения в локтевых суставах, предплечьях, запястьях, в кистях и пальцах рук. Часто присутствуют жалобы на онемение шеи, боль в плечах и пояснице или покалывание в ногах. Но существуют и более серьезные заболевания. Наиболее распространенным является синдром запястного канала, при котором нервные окончания руки

повреждаются вследствие частой и длительной работы на компьютере. Самая тяжелая форма этого синдрома проявляется в виде мучительных болей, лишаящих человека трудоспособности.

Синдром запястного канала (СЗК) – травма запястья и патология. Это заболевание вызывается ущемлением срединного нерва в запястном канале. Оно возникает при распухании срединного нерва и/или сухожилий кисти. Чаще всего СЗК проявляется из-за долгого сидения за компьютером с неправильной осанкой. С течением времени эта травма вызывает накопление продуктов распада в области запястного канала. Если сотрудник не делает регулярных перерывов и не выполняет простые упражнения для кисти, продукты распада провоцируют распухание, а затем и развитие этого опасного заболевания.

Проблемы с осанкой бывают различных типов и могут приводить к различным проблемам: сгорбленное положение во время работы увеличивает нагрузку на позвоночник, приводит к чрезмерному растяжению мышц, поддерживающих осанку. Сгорбленное положение – одно из причин синдрома запястного канала, оно приводит к грыжам межпозвоночных дисков поясничного отдела, грыжам межпозвоночных дисков шейного отдела. Если в результате неправильной осанки голова выдвинута вперед, то усиливается прогиб шейного отдела позвоночника, вытягивание головы вперед вызывает напряжение мышц основания головы и шеи, что ограничивает кровоток в сосудах шеи, кровоснабжение головы и отток крови от нее – всё это приводит к головным болям, болям в шее, болям в руках и кистях. Одной из основных причин неправильной осанки является сутулость.

Сутулость вызывает излишнюю нагрузку на плечевые сухожилия, что приводит к напряжению мышц плеча. Она может привести к развитию синдрома запястного канала, а также к синдрому ущемления плеча.

Профилактикой проблем с опорно-двигательной системой являются:

- эргономичная организация рабочего места для сведения к минимуму рабочей нагрузки на область запястного канала;
- упражнения на растягивание и укрепление мышц запястья и ладони;

- регулярные перерывы в работе с мышью и клавиатурой;
- правильная осанка.

Заключение

В ходе выполнения выпускной квалификационной работы было описано текущее состояние автоматизированной системы «Отдел кадров», выявлены и описаны информационные системы персональных данных в отдела кадров. Далее разработана модель нарушителя и модель угроз персональных данных отдела кадров. Для актуальных угроз ИБ выбраны и обоснованы выбранные средства защиты информации для автоматизированной системы «Отдел кадров» в защищенном исполнении. На последнем этапе была описана автоматизированная система отдела кадров на ФГУП ФНПЦ «ПО «Старт» им. М.В.Проценко» в защищенном исполнении.

В ходе достижения цели были получены навыки в области обеспечения безопасности персональных данных в информационных системах персональных данных отдела кадров предприятия.

Результатом выпускной квалификационной работы является спроектированная автоматизированная система «Отдел кадров» на ФГУП ФНПЦ «ПО «Старт» им. М.В.Проценко» в защищенном исполнении в соответствии с утвержденными ФСТЭК России нормативными документами.

Таким образом, задание на выпускную квалификационную работу было выполнено в полном объеме.

Список использованных источников

- 1 Статья 3. Основные понятия, используемые в настоящем Федеральном законе [Электронный ресурс]: Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 29.07.2017) "О персональных данных" Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/ , свободный (дата обращения: 02.03.2018)
- 2 Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Режим доступа: <http://fstec.ru/component/attachments/download/289>, свободный (дата обращения: 10.03.2018)
- 3 Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 год. Режим доступа: <https://fstec.ru/component/attachments/download/290>, свободный (дата обращения: 18.03.2018)
- 4 Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_137356, свободный (дата обращения: 05.04.2018)
- 5 Приказ ФСТЭК от 18 февраля 2013г. №21 "Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных". Режим доступа: <http://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21>, свободный (дата обращения: 13.04.2018)
- 6 Методический документ. Меры защиты информации в государственных информационных системах. ФСТЭК России, 2014 год. Режим доступа: <https://fstec.ru/component/attachments/download/675>, свободный (дата обращения: 22.04.2018)

7 Классификация опасных и вредных производственных факторов.
Режим доступа: <http://vesbiz.ru/personal/klassifikaciya-opasnyx-i-vrednyx-proizvodstvennyx-faktorov.html>, свободный (дата обращения: 02.05.2018)