

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 –

Специализация -

Информационная безопасность
автоматизированных систем
Защищенные автоматизированные
системы управления

ДИПЛОМНЫЙ ПРОЕКТ

на тему

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

Студент

 Шпагин Денис Юрьевич

Руководитель начальник отдела
системного программирования

 С.Н. Совватейкин

Нормоконтролёр

 А.Г. Фатеев

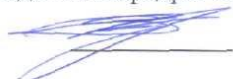
Рецензент заместитель начальника

УИТ

 В.Г. Курамов

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

Заведующий кафедрой

 С.Л. Зефирова

Работа защищена с отметкой

хорошо

(протокол заседания ГЭК

от 27.06.18 № 12)

Секретарь ГЭК

 А.П. Иванов

Пенза 2018

Проверил Саллов 
25.06.2018 /Саллов/

Оглавление

Введение.....	4
1 Описание текущего состояния автоматизированной системы «Бухгалтерия».....	5
1.1 Описание автоматизированной системы «Бухгалтерия», её целей функционирования, основных процессов.....	5
1.2 Идентификация информационных процессов, с помощью которых реализуются задачи деятельности организации.....	6
1.3 Разработка структуры автоматизированной системы «Бухгалтерия» и состав технических средств обработки информации.....	8
1.4 Проектирование физической модели автоматизированной системы «Бухгалтерия».....	13
1.5 Выявление и описание информационных систем персональных данных в бухгалтерии.....	14
1.6 Общее описание информационных систем персональных данных бухгалтерии, эксплуатируемых при осуществлении соответствующих видов деятельности.....	17
2 Разработка модели нарушителя.....	21
3 Разработка модели угроз персональных данных бухгалтерии предприятия.....	25
4 Определение уровня защищенности информационных систем персональных данных бухгалтерии.....	38
5 Определение организационных и организационно-технических требований к обеспечению уровней защищенности персональных данных в информационных системах персональных данных бухгалтерии.....	40
5.1 Определение базового набора мер по обеспечению безопасности для информационных системах персональных данных.....	40

5.2	Адаптация и уточнение мер по обеспечению безопасности персональных данных в информационной системе персональных данных «Контрагенты»	42
5.3	Адаптация и уточнение мер по обеспечению безопасности персональных данных в информационной системе персональных данных «Сотрудники».....	45
6	Выбор и обоснование средств защиты информации для автоматизированной системы «Бухгалтерия» в защищенном исполнении.....	47
7	Вредные психофизиологические факторы, влияющие на органы зрения специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие.....	55
	Заключение.....	58
	Список используемых источников.....	59

Введение

В настоящее время защита персональных данных граждан Российской Федерации является актуальной задачей. Практически все предприятия различных форм собственности и размеров для ведения своей деятельности обрабатывают персональные данные. Для регулирования информационных правоотношений в области персональных данных законодателем установлен целый ряд нормативно-правовых актов.

Владельцам персональных данных может быть нанесен материальный и/или моральный ущерб, если эти данные станут доступны лицам, не имеющим на это полномочий.

Процесс создания АСЗИ заключается в совокупности набора мероприятий, которые направлены на разработку и применение технологий, обеспечивающих защиту информации.

Актуальность выпускной квалификационной работы заключается в проектировании автоматизированной системы бухгалтерии предприятия в защищенном исполнении в соответствии с методическими документами и базой нормативных актов в сфере защиты персональных данных в их последних редакциях.

1 Описание текущего состояния автоматизированной системы «Бухгалтерия»

1.1 Описание автоматизированной системы «Бухгалтерия», её целей функционирования, основных процессов

Целью функционирования бухгалтерии ФГУП ФНПЦ «ПО «Старт» им. М.В.Проценко» является формирование и обеспечение полной и достоверной информации о финансовой деятельности, а также обеспечение информацией, необходимой внутренним и внешним пользователям бухгалтерской отчетности.

Для достижения этой цели бухгалтерия выполняет следующие функции:

- формирование и предоставление достоверного бухгалтерского учета финансовой деятельности предприятия;
- организация финансового документооборота;
- анализ результатов деятельности предприятия;
- налоговое планирование.

Целью АС «Бухгалтерия» является обеспечение руководства предприятия достоверной финансовой информацией, которая поможет принять взвешенные решения при выборе альтернатив использования ограниченных активов.

Функции, выполняемые в организации, для достижения цели:

- расчет по заработной плате и иным выплатам сотрудникам предприятия;
- составления бухгалтерского баланса и другой бухгалтерской отчетности.

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

Схема информационного процесса «Расчеты по заработной плате и иным выплатам сотрудникам предприятия» представлена на рисунке 1.

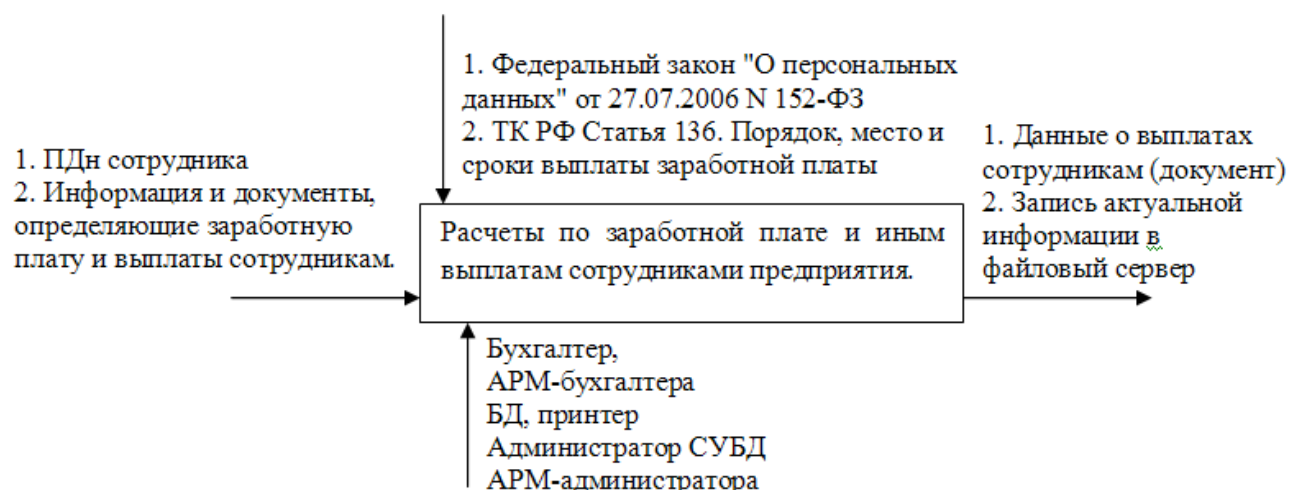


Рисунок 1 – Структурная модель информационного процесса «Расчеты по заработной плате и иным выплатам сотрудникам предприятия»

Входной информацией в данном процессе являются ПДн сотрудников, а также информация и документы, определяющие заработную плату и выплаты сотрудникам.

Работники предприятия предоставляют свои ПДн на бумажном носителе сотрудникам бухгалтерии. Те вносят эту информацию в БД, где она и будет храниться, и откуда она будет поступать в электронном виде в бухгалтерию. Затем в бухгалтерии с использованием этой информации составляется бухгалтерский баланс, и другая отчетная документация.

Бухгалтера ежемесячно осуществляют обработку данных. Результатом этого процесса являются данные о выплатах сотрудникам (документ), хранимые в электронном виде на файловом сервере и в сейфе.

Информация на бумажном носителе обрабатывается в данные, которые хранятся в электронном виде в БД бухгалтерии. Обработанная информация продолжает храниться в течение 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.

Схема информационного процесса «Составление квартального отчета» представлена на рисунке 2.

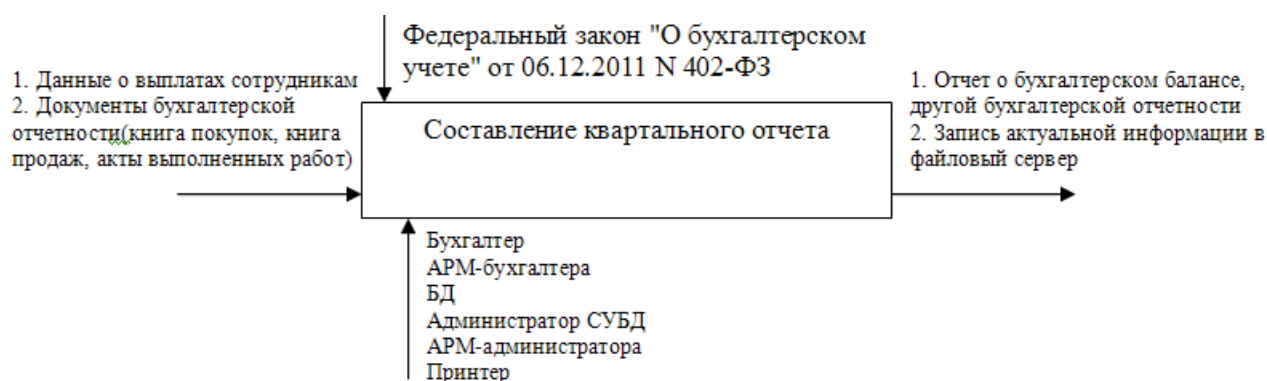


Рисунок 2 – Структурная модель информационного процесса «Составление квартального отчета»

Входной информацией в данном процессе являются данные о выплатах сотрудникам (документ) и документы бухгалтерской отчетности.

Главный бухгалтер запрашивает данные о выплатах сотрудникам (документ) у подчиненных бухгалтеров.

Затем с использованием документов бухгалтерской отчетности (книга покупок, книга продаж, акты выполненных работ) главный бухгалтер осуществляет обработку данных. Результатом этого процесса являются отчет о бухгалтерском балансе, и другая бухгалтерская отчетность. Информация хранится в электронном виде на файловом сервере и в сейфе.

Информация на бумажном носителе обрабатывается в данные, которые хранятся в электронном виде в БД бухгалтерии. Обработанная информация продолжает храниться 75 лет в соответствии со ст. 22 ФЗ «Об архивном деле в РФ». При наличии доступа у сотрудника к запрошенной информации, обработанная информация поступает на АРМ. Выводится информация на монитор в удобном виде для восприятия сотрудником.

В таблице 1 представлен Перечень сведений конфиденциального характера.

Таблица 1 - Перечень сведений конфиденциального характера

№ п/п	Наименование сведений	Примечание
1	ПДн сотрудника	ИОД
2	Информация и документы, определяющие заработную плату и выплаты сотрудникам	Коммерческая тайна
3	Данные о выплатах сотрудникам (документ)	Коммерческая тайна
4	Документы бухгалтерской отчетности (книга покупок, книга продаж, акты выполненных работ)	Коммерческая тайна
5	Отчет о бухгалтерском балансе, другой бухгалтерской отчетности	Коммерческая тайна

1.3 Разработка структуры автоматизированной системы «Бухгалтерия» и состав технических средств обработки информации

Для описания структуры АС «Бухгалтерия» были описаны 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;
- 1С: Бухгалтерия 7.7;
- клиент MySQL 4.7.11;
- СУБД Postgres SQL 9;
- антивирус «Kaspersky Endpoint Security 8».

- сервер резервного копирования в составе:
- сервер ProLiant DL360 HPM Gen9 E5-2660v4 Rack(1U)/2xXeon14C / 2.0GHz(35MB)/ 4x16GbR1D_2400 / (2GB/RAID) / noHDD – 1 шт;
- жесткий диск HPE 300GB – 3 шт;
- модуль памяти KTH-PL424S/16G Kingston fo HP/Compaq – 4 шт;
- панель HPE DVD/USB Universal Media Bay (DVD-RW, USB 2.0, and VGA) – 1 шт.
- принтер HP LaserJet Pro M402dn (G3V21A);
- источник бесперебойного питания APC SRT5KRMXLI Smart-UPS SRT RM, 5000VA/4500W;
- АРМ бухгалтерии. АРМ имеют типовую структуру и одинаковы для всех сотрудников. Все АРМ находятся за пределами КЗ. На АРМ бухгалтеров и главного бухгалтера установлены следующие программные средства:
 - ОС Windows 7;
 - Libreoffice 5.4.1;
 - компьютерная справочная правовая система «Консультант Плюс»;
 - Audit Expert;
 - 1С: Бухгалтерия 7.7;
 - антивирус «Kaspersky Endpoint Security 8»;
 - СЗИ от НСД «Secret Net 7»;
 - 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 – 1 шт;
 - сетевой адаптер Gigabit Ethernet Single port Fiber Gigabit – 1 шт;
 - монитор 24" Dell U2412M, BK/BK S-IPS, LED 1920x1200 – 1 шт.

В состав АРМ администратора входят следующие программные компоненты:

- Ubuntu Gnome 16.04 LTS;
 - Libreoffice 5.4.1;
 - антивирус «Kaspersky Endpoint Security 8»;
 - ПЭВМ MT i5-7500 (3.4GHz, QC,6M), 16GB DDR4 2400MHz, 2TB SATA 7.2k – 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 – 1 шт;
 - монитор 24" Dell U2412M, BK/BK S-IPS, LED 1920x1200 – 1 шт.
- АС бухгалтерии обменивается данными по локальной сети по Hyperline PC-кабелям Патч-корд F/UTP, Cat.5e, LSZH.

В качестве маршрутизатора используется маршрутизатор Cisco 861 Ethernet Security Router CISCO861-K9.

В качестве коммутационного оборудования используется 8 портовый коммутатор Cisco Catalyst WS-C2940-8TT-S.

После этого параметры АС «Бухгалтерия» были представлены в виде таблицы 2.

Таблица 2 – Параметры АС «Бухгалтерия»

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

Все аппаратные ресурсы АС «Бухгалтерия» объединены между собой. Была описана структура АС «Бухгалтерия», которая позволит выполнять

функции, на неё возлагаемые. Графическое изображение АС «Бухгалтерия» представлено на рисунке 3.

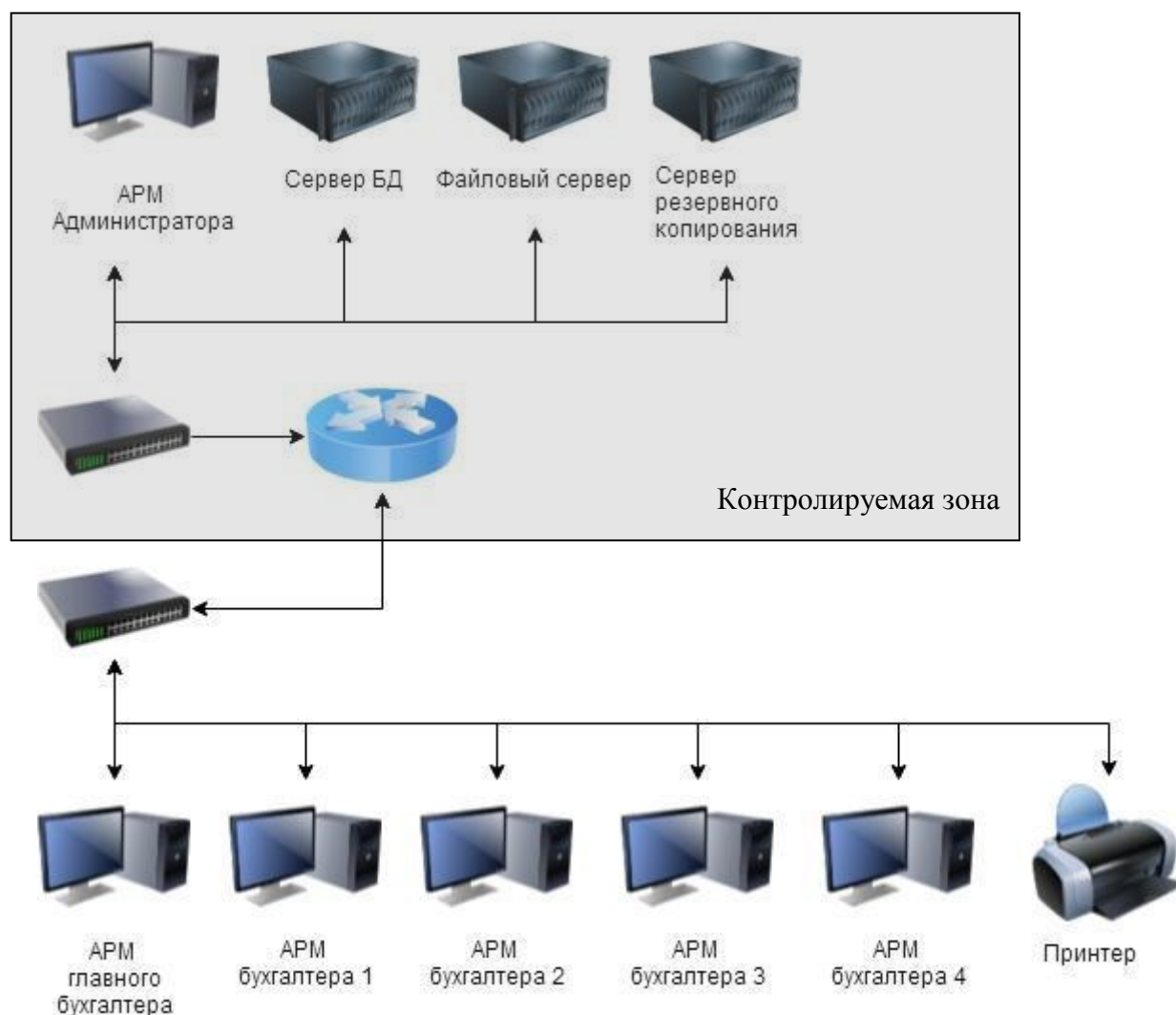


Рисунок 3 – Структура АС «Бухгалтерия»

Далее на основе структуры АС «Бухгалтерия» и описаний информационных процессов была разработана инфологическая модель АС «Бухгалтерия», показывающая циркуляцию информации путем использования информационных ресурсов в системе. Результат проделанной работы представлен на рисунке 4.

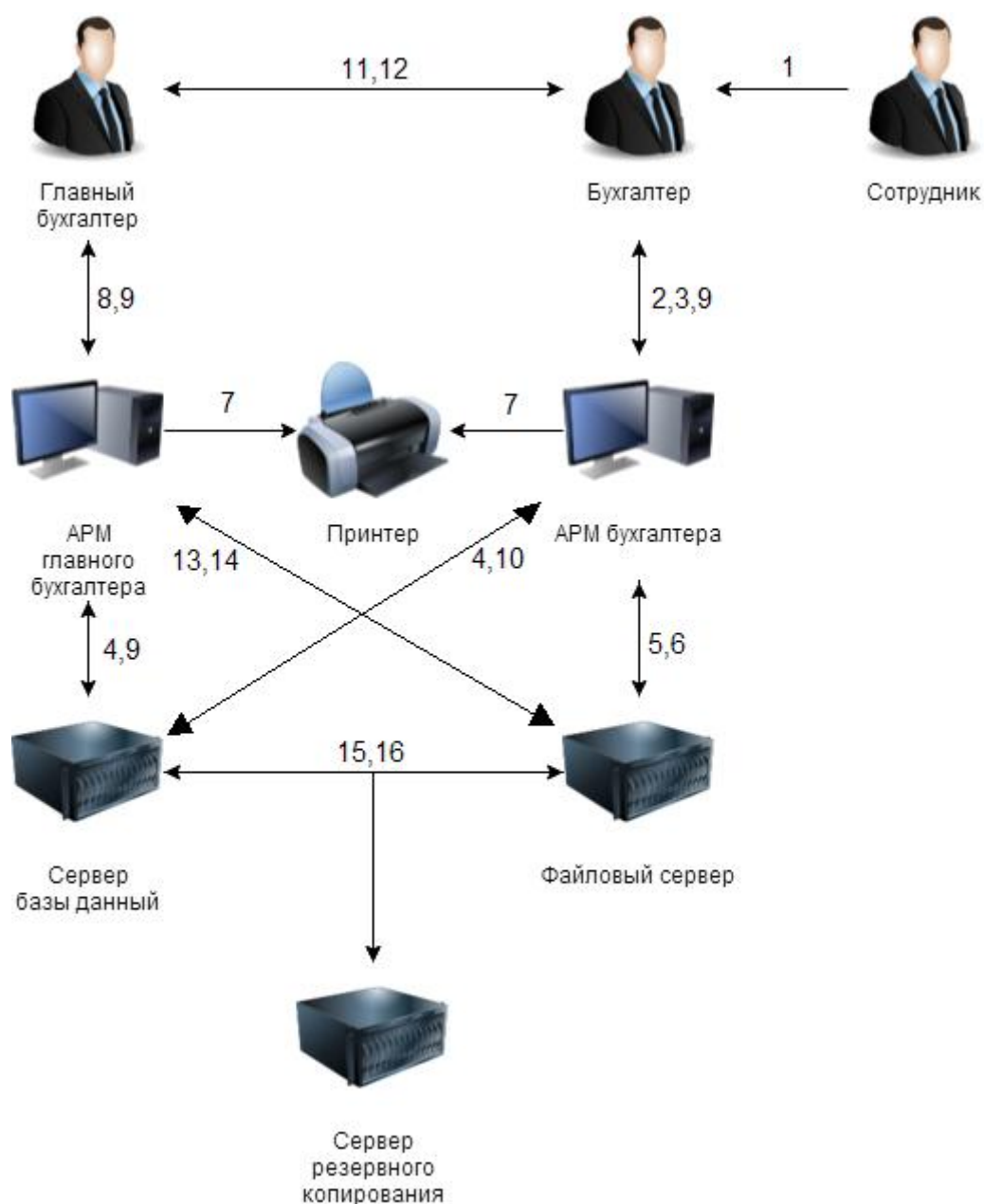


Рисунок 4 – Информационные потоки в АС «Бухгалтерия»

Обозначения информационных потоков показано в таблице 3.

Таблица 3 – Информационные потоки

Обозначение потока	Информационный поток
1	Предоставление ПДн на бумажном носителе
2	Заполнение специальной формы
3	Внесение ПДн
4	Запрос ПДн сотрудника
5	Запрос информации и документов, определяющих заработную плату и выплаты сотрудникам
6	Оправка данных о выплатах сотрудникам (документ) на файловый сервер

Продолжение таблицы 3

Обозначение потока	Информационный поток
7	Отправка данных на принтер
8	Ввод данных о выплатах сотрудникам (документ)
9	Вывод данных в электронном виде
10	Отправка ПДн на сервер базы данных
11	Запрос данных о выплатах сотрудникам (документ)
12	Предоставление данных о выплатах сотрудникам (документ)
13	Запрос документов бухгалтерской отчетности (книга покупок, книга продаж, акты выполненных работ)
14	Оправка отчета о бухгалтерском балансе, и другой бухгалтерской отчетности на файловый сервер
15	Создание/отправка резервной копии/последних обновлений на сервер резервного копирования
16	Восстановление данных из резервной копии

1.4 Проектирование физической модели автоматизированной системы «Бухгалтерия»

Бухгалтерия располагается на одном из этажей четырехэтажного здания, являющегося зданием «Отдела кадров». Общая площадь «Отдела кадров» составляет 630 кв. метров. Высота потолка составляет 3,2 метра. Материал внешних и внутренних стен – керамический кирпич.

Был описан план помещения бухгалтерии, на котором будут располагаться компоненты АС. Были определены размеры, площадь, высота потолков, материалы внутренних стен, были указаны места расположения рабочих станций, оконечных сетевых устройств.

Общее количество бухгалтеров - 5 человек. В помещении бухгалтерии располагаются: 1 АРМ главного бухгалтера, 4 АРМ бухгалтеров, принтер шкаф/сейф.

На рисунке 5 представлено размещение всех АРМ, а также расположение шкафа/сейфа.

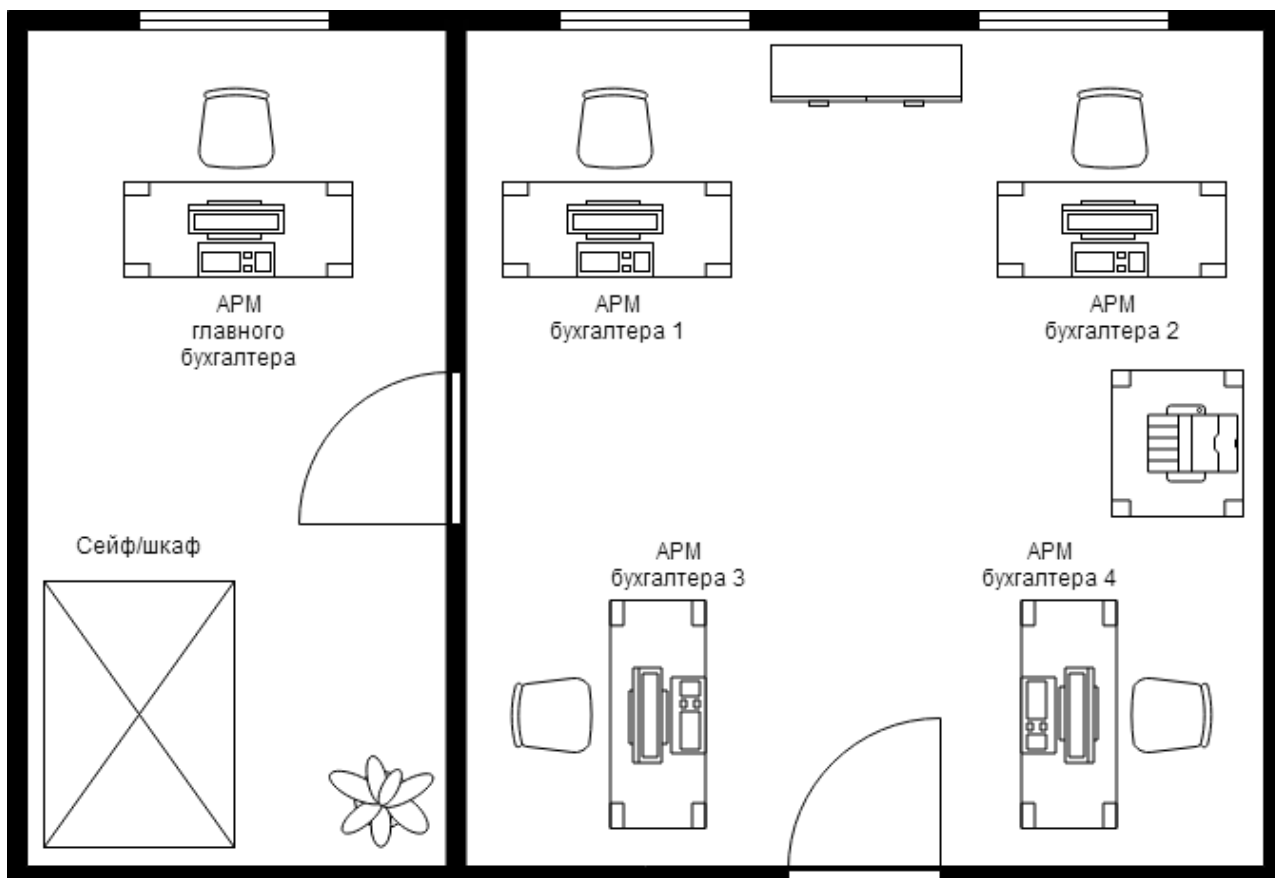


Рисунок 5 – Помещение бухгалтерии

Площадь помещения бухгалтерии составляет 30 кв. метров. Бухгалтерия состоит из двух комнат. Высота потолка составляет 3,2 метра. Материал внешних и внутренних стен – керамический кирпич.

1.5 Выявление и описание информационных систем персональных данных в бухгалтерии

В процессе выполнения данного пункта, пользуясь разработанными на предыдущем этапе описаниями информационных процессов, описаны условия создания и использования ПДн.

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

- цель обработки ПДн в данной ИСПДн;
- перечни ПДн, обрабатываемых в бухгалтерии 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 ПДн, 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, ПДн которых обрабатываются.

Затем ПДн были категорированы 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 4.

Таблица 4 – Перечень персональных данных, обрабатываемых в автоматизированной системе «Бухгалтерия»

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	Осуществление финансовых операций	Трудовые отношения между работником и	Срок обработки зависит от срока работы	Иные	Смешанный

Продолжение таблицы 4

Содержание ПДн	Цели обработки ПДн	Основание для обработки ПДн	Сроки обработки и хранения ПДн, основания для прекращения обработки ПДн	Категория ПДн	Вид обработки (с использование м средств автоматизации, без использования средств автоматизации, смешанная)
Обработка ПДн сотрудников организации					
Паспортные данные (серия/номер/д ата/кем выдан) Пол Дата рождения (число/месяц/г од) 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	(выплата зарботной платы, отпускные, оплата больничного листа)	Фондом (ст. 16 ТК РФ). Трудовой договор с работником	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		

Продолжение таблицы 4

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 субъектов ПДн, не являющихся сотрудниками организации					
Фамилия, имя, отчество Паспортные данные (серия/номер /дата/кем выдан) контактный телефон, ИНН	Составление финансово- расчетных документов о взаимодейств ии с контрагентам и	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 Основанием для прекращения обработки ПДн служит расторжение договора с контрагентами	Иные	Смешанный

1.6 Общее описание информационных систем персональных данных бухгалтерии, эксплуатируемых при осуществлении соответствующих видов деятельности

Был разработан перечень ИСПДн. Для это была составлена матрица доступа сотрудников предприятия к ПДн, отражающая права всех групп

пользователей ПДн на действия с ПДн, которые 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 5.

Таблица 5 – Матрица доступа организации

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

Продолжение таблицы 5

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

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 бухгалтерии и матрицы доступа к этим ПДн были установлены следующие ИСПДн: ИСПДн№1 «Контрагенты» и ИСПДн №2 «Сотрудники».

Описание установленных ИСПДн представлено в таблице 6.

Таблица 6 – 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

Внешние нарушители — лица, не имеющие физический доступ, но 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 содержащейся в них информации. 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 7.

Таблица 7 — Внешние и внутренние источники угроз

Обозначение	Источник угроз
ИУ1	Разработчики, производители, поставщики программных, технических и программно-технических средств
ИУ2	Лица, привлекаемые для установки, наладки, монтажа 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

У нарушители с базовым потенциалом есть возможность:

- получать информацию о методах и средствах реализации УБИ, что опубликованы в открытом доступе;
- получать информацию об уязвимостях отдельных компонентов системы, что опубликованы в открытом доступе;
- самостоятельно реализовать создание методов и создавать инструменты, позволяющие реализовывать атаки на ИС.

У нарушителей со средним потенциалом имеются те же возможности, что у нарушителей с базовым, а также:

- возможность получения информации об уязвимостях отдельных компонентов ИС (с использованием свободно доступных программных средств) путем анализа кода прикладного ПО и отдельных программных компонентов общесистемного ПО;
- имеют осведомленность о ЗМ, применяемых в ИС;
- обладают доступом к информации о структурно-функциональных характеристиках и особенностях ИС.

Нарушители с высоким потенциалом обладают всеми возможностями нарушителей со средним потенциалом, имеют:

- возможность получить доступ к ПО микропрограммам, системному и прикладному ПО, телекоммуникационному оборудованию и другим программно-техническим средствам ИС;
- возможность осуществлять НСД из выделенных сетей связи, к которым возможен физический доступ;
- осведомленность о ЗМ ЗИ, применяемых в ИС, об алгоритмах, аппаратных и программных средствах, используемых в ИС;

— возможность создавать методы и средства реализации УБИ с помощью привлечения узкоспециализированных научных организаций, а также реализуют УБИ благодаря специально разработанным средствам;

— возможность получать сведения об уязвимостях с помощью исследований (в том числе с привлечением специализированных научных организаций) и применения специальных средств для анализа ПО;

— возможность создавать и применять специальных технических средств для воздействия на информацию, распространяющейся в виде явлений или физических полей.

Возможными целями (мотивацией) для реализации УБИ нарушителями в АС «Бухгалтерия» могут являться:

— причинение ущерба организации, ее отдельным областям деятельности;

— дестабилизация, дискредитация деятельности организации;

— получение конкурентных преимуществ;

— внедрение дополнительных функциональных возможностей в ПО или программно-технические средства на стадии разработки;

— реализация УБИ из мести;

— реализация УБИ непреднамеренно из-за неосторожности или некомпетентных действий.

Основные методы реализации угроз в АС «Бухгалетрия» приведены в таблице 8.

Таблица 8 — Основные методы реализации угроз в АС «Бухгалтерия»

Обозначение	Методы реализации угроз
M1	НСД и (или) воздействия на объекты на аппаратном уровне
M2	НСД и (или) воздействия на объекты на общесистемном уровне
M3	НСД и (или) воздействия на объекты на прикладном уровне (СУБД, иные прикладные программы общего и специального назначения)
M4	несанкционированного физического доступа и (или) воздействия на каналы связи, технические средства, машинные носители информации
M5	воздействия на пользователей, администраторов безопасности, администраторов ИС или обслуживающий персонал

В итоге была разработана модель нарушителя ИБ АС «Бухгалтерия», результаты которой приведены в таблице 9, которая является составной частью модели угроз ИБ АС «Бухгалтерия» и содержит:

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

Таблица 9 — Модель нарушителя ИБ АС «Бухгалтерия»

№ п/п	Тип нарушителя	Вид нарушителя	Потенциал нарушителя	Методы реализации угроз
1	Внешние	ИУ1	Средний	M1, M2, M3
		ИУ2	Средний	M1
		ИУ3	Низкий	M4, M5
2	Внутренние	ИУ4	Средний	M3
		ИУ5	Высокий	M3, M4
		ИУ6	Высокий	M2, M3, M4

3 Разработка модели угроз персональных данных бухгалтерии

Цель определения угроз БИ заключается в определении существования возможности нарушения конфиденциальности, целостности или доступности информации, которая содержится в системе, и повлечет ли нарушение хотя бы одного из указанных свойств БИ за собой неприемлемые негативные последствия (ущерб) для обладателя информации или оператора, а также в случае обработки ПДн и для субъектов ПДн.

Детализированные угрозы БИ были подобраны на основе данных, приведенных, в банке данных угроз безопасности информации ФСТЭК России, где размещены и сведения об уязвимостях.

На данном этапе были идентифицированы наиболее актуальные для ПДн бухгалтерии угрозы и разработана частная модель угроз. При обработке ПДн в бухгалтерии предприятия в соответствии с методическим документом ФСТЭК «Базовая модель угроз безопасности ПДн при их обработке в ИСПДн» были определены угрозы, представленные в таблице 10. Таблица заполнялась символами «К», «Ц», «Д», если нарушается – конфиденциальность, целостность, доступность, соответственно.

Таблица 10 — Угрозы безопасности

№ п/п	Описание угрозы	Источник угрозы	Нарушаемые свойства	Объекты воздействия	Уязвимость
Угрозы от утечки по техническим каналам:					
1	Угрозы утечки видовой информации [2]	Персонал, не имеющий доступ в контролируемую зону, но имеющий доступ 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 в использовании физического управления доступом к помещениям, в которых расположены ИСПДн.

Продолжение таблицы 10

№ п/п	Описание угрозы	Источник угрозы	Нарушаемые свойства	Объекты воздействия	Уязвимость
Угрозы хищения, несанкционированной модификации или блокирования информации за счет НСД					
2	Угроза действия вредоносных программ (вирусов) [2]	Наличие сетевого взаимодействия	К, Д	Информация, обрабатываемая на АРМ ИСПДн, информация, обрабатываемая на серверах ИСПДн	Отсутствие контроля над состоянием ПО, бездействие администратора безопасности
Угрозы преднамеренных действий внутренних нарушителей					
3	Угроза несанкционированной модификации информации [2]	Персонал, имеющий доступ к компонентам ИСПДн	К, Ц	Информация, обрабатываемая на АРМ ИСПДн, информация, обрабатываемая на серверах	Наличие в системе незаблокированных учётных записей пользователей
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

Угроза является актуальной, если она может быть реализована в ИСПДн, и которая представляет опасность для ПДн. Рекомендуемый подход к составлению перечня актуальных угроз состоит в следующем.

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

Уровнем исходной защищенности ИСПДн является обобщенный показатель, который зависит от технических и эксплуатационных характеристик ИСПДн, приведенных в таблице 11 и 12.

Таблица 11 – 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: ИСПДн, физически отделенная от сети общего пользования;	+	–	–
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 определенный перечень сотрудников 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);	+	–	–

Продолжение таблицы 11

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
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, предоставляющая часть ПДн	–	+	–

По результатам анализа таблицы 11 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.[3]

Таблица 12 – 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: ИСПДн, физически отделенная от сети общего пользования;	+	–	–
3. По встроенным (легальным) операциям с записями баз персональных данных: запись, удаление, сортировка;	–	+	–

Продолжение таблицы 12

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
4. По разграничению доступа к персональным данным: ИСПДн, к которой имеют доступ определенный перечень сотрудников 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 12 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 [3].

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 лицами, не имеющими легального доступа в помещение, где последние хранятся);

— низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты информации);

— 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 13 и 14.

Таблица 13 – Оценка возможности реализации угроз в ИСПДн №1 «Контрагенты»

№	Угрозы	Вероятность реализации и 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	Угроза несанкционированной модификации информации	Низкая		2	0,35	Средняя
4	Угроза разглашения информации, модификация, уничтожение сотрудниками допущенными к ее обработке	Средняя		5	0,5	Средняя

Таблица 14 – Оценка возможности реализации угроз в ИСПДн №2 «Сотрудники»

№	Угрозы	Вероятность реализации и угроз	Y1	Y2	Y	Возможность реализации угрозы
1	Угрозы утечки видовой информации	Средняя	5	2	0,35	Средняя
2	Угроза действия вредоносных программ (вирусов)	Высокая		10	0,75	Высокая

Продолжение таблицы 14

№	Угрозы	Вероятность реализации и угроз	Y1	Y2	Y	Возможность реализации угрозы
3	Угрозы нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в аппаратном и программном обеспечении, а также от угроз не антропогенного и стихийного характера	Низкая	5	2	0,35	Средняя
4	Угроза разглашения информации, модификация, уничтожение сотрудниками допущенными к ее обработке	Средняя		5	0,5	Средняя

Была проведена оценка опасности каждой угрозы на основе опроса экспертов (специалистов в области защиты информации). В результате 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 значению или объему 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 репутационным, моральным, финансовым потерям для субъекта, вплоть до потери средств к существованию, здоровья, жизни.

На основе опроса экспертов был определен показатель опасности для каждой угрозы. Результаты оценки опасности угроз для ИСПДн №1 «Контрагенты» представлены в таблице 15.

Таблица 15 – 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	Угроза несанкционированной модификации информации	Средняя
4	Угроза разглашения информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	Высокая

Результаты оценки опасности угроз для ИСПДн №2 «Сотрудники» представлены в таблице 16.

Таблица 16 – Оценка опасности угроз для ИСПДн №2 «Сотрудники»

№	Угрозы	Показатель опасности угрозы
1	Угрозы утечки видовой информации	Средняя
2	Угроза действия вредоносных программ (вирусов)	Высокая
3	Угроза несанкционированной модификации информации	Средняя
4	Угроза разглашения информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	Высокая

Затем был осуществлен выбор из предварительного перечня угроз безопасности тех, что относятся к актуальным для данной ИСПДн, в соответствии с правилами, приведенными в таблице 17.

Таблица 17 — 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

Результат определения актуальности угроз для ИСПДн №1 «Контрагенты» представлены в таблице 18.

Таблица 18 – 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
Угроза несанкционированной модификации информации	Средняя	Средняя	Актуальная
Угроза разглашения информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	Средняя	Высокая	Актуальная

Результат определения актуальности угроз для ИСПДн №2 «Сотрудники» представлены в таблице 19.

Таблица 19 – Актуальность угроз для ИСПДн №2 «Сотрудники»

Угроза	Возможность реализации угрозы	Показатель опасности угрозы	Актуальность
Угрозы утечки видовой информации	Средняя	Средняя	Актуальная
Угроза действия вредоносных программ (вирусов)	Высокая	Высокая	Актуальная
Угроза несанкционированной модификации информации	Средняя	Средняя	Актуальная
Угроза разглашения информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	Средняя	Высокая	Актуальная

Актуальные угрозы безопасности ПДн - это совокупность условий и факторов, создающих актуальную опасность НСД, в том числе случайного, к ПДн при их обработке в ИС, в результате которой ПДн могут быть уничтожены, изменены, блокированы, скопированы, распространены, 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 20.

Таблица 20 — Модель угроз безопасности ПДн бухгалтерии промышленного предприятия

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
Угроза несанкционированной модификации информации	Средняя	Средняя	Средняя	Актуальная	Нарушение К, Ц	3
Угроза разглашения информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	Средняя	Средняя	Высокая	Актуальная	Нарушение К, Ц, Д	3

Продолжение таблицы 20

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	Средняя	Актуальная	Нарушение К	3
Угроза действия вредоносных программ (вирусов)	Высокая	Высокая	Высокая	Актуальная	Нарушение К, Д	3
Угроза несанкционированной модификации информации	Средняя	Средняя	Средняя	Актуальная	Нарушение К, Ц	3
Угроза разглашения информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	Средняя	Средняя	Высокая	Актуальная	Нарушение К, Ц, Д	3

4 Определение уровня защищенности информационных систем персональных данных бухгалтерии

Данный этап посвящен определению уровней защищенности персональных данных в бухгалтерии предприятия.

Актуальной угрозой является та, что может быть реализована в ИСПДн, и которая представляет опасность для ПДн. Согласно Постановлению Правительства РФ №1119 для ИСПДн различают 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 является третий тип.

В бухгалтерии промышленного предприятия 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 промышленного 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 4-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 бухгалтерии

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 21.

Таблица 21 — 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 21

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
ОЦЛ.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.

5.3 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 22.

Таблица 22 — 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.

Продолжение таблицы 22

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 сбой при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбой в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти		+	Добавлена для предотвращения переполнения объема памяти

6 Выбор и обоснование средств защиты информации для автоматизированной системы «Бухгалтерия» 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 23 и 24 соответственно.

Таблица 23 – 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
Угроза несанкционированной модификации информации [У3]	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
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, АНЗ.5, ОЦЛ.7, ЗИС.3, УКФ.1, УКФ.3

Таблица 24 – Сопоставление актуальных угроз для каждой защитной меры для ИСПДн №1 «Контрагенты»

Защитные меры	Угрозы
ИАФ.1	У3, У4
ИАФ.3	У3, У4
ИАФ.4	У3, У4
ИАФ.5	У3, У4
УПД.1	У3, У4
УПД.2	У3, У4
УПД.3	У3, У4
УПД.4	У3, У4

Продолжение таблицы 24

Защитные меры	Угрозы
УПД.5	У3, У4
УПД.6	У3, У4
УПД.10	У1, У4
УПД.11	У3, У4
УПД.12	У3, У4
УПД.15	У3, У4
ЗНИ.4	У3, У4
ЗНИ.8	У3, У4
РСБ.1	У2, У3, У4
РСБ.2	У2, У3, У4
РСБ.3	У2, У3, У4
РСБ.7	У2, У3, У4
АВЗ.1	У2
АВЗ.2	У2
АНЗ.1	У3
АНЗ.2	У4
АНЗ.3	У4
АНЗ.4	У4
ЗИС.3	У2, У4
ЗТС.3	У1
ЗТС.4	У1
УКФ.1	У3, У4
УКФ.3	У3, У4
ОЦЛ.7	У4

Сопоставление защитных мер к каждой угрозе и угроз к каждой защитной мере для ИСПДн №2 «Сотрудники» представлено в таблицах 25 и 26 соответственно.

Таблица 25 – 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 25

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
Угроза несанкционированной модификации информации [У3]	ИАФ.1, ИАФ.3, ИАФ.4, ИАФ.5, УПД.1, УПД.2, УПД.3, УПД.4, УПД.5, УПД.6, УПД.12, УПД.15, РСБ.1, РСБ.2, РСБ.3, РСБ.7, ЗНИ.4;
Угроза разглашения информации, модификация, уничтожение сотрудниками, допущенными к ее обработке [У4]	УПД.1, УПД.2, УПД.3, УПД.4, УПД.5, УПД.6, УПД.12, УПД.15, ИАФ.1, ИАФ.3, ИАФ.4, ИАФ.5, ЗНИ.4, РСБ.1, РСБ.2, РСБ.3, РСБ.4, РСБ.7, АНЗ.5, ОЦЛ.7, ЗИС.3, УКФ.1, УКФ.3.

Таблица 26 – Сопоставление актуальных угроз для каждой защитной меры для ИСПДн №2 «Сотрудники»

Защитные меры	Угрозы
ИАФ.1	У3, У4
ИАФ.3	У4
ИАФ.4	У4
ИАФ.5	У4
УПД.1	У4
УПД.2	У4
УПД.3	У4
УПД.4	У4
УПД.5	У4
УПД.6	У4
УПД.15	У4
ЗНИ.4	У4
РСБ.1	У2, У4
РСБ.2	У2, У4

Продолжение таблицы 26

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

Далее были описаны сертифицированные защитные меры.

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 СКН»;
- «Профиль защиты СКН(контроля подключения съемных машинных носителей информации четвертого класса защиты. ИТ.СКН.П4.ПЗ)»;
- «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, В, Г второго класса защиты. ИТ.САВЗ.Б2.ПЗ, ИТ.САВЗ.В2.ПЗ, 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».

Здание отдела кадров, в котором располагается помещение бухгалтерии, находится под постоянной охраной. В здании действует пропускной режим входа, само здание охраняется круглосуточно. Дверь в помещение бухгалтерии оборудована 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 бухгалтерии 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 бухгалтерии в исходный план помещения были внесены изменения.

План помещения бухгалтерии после проведения работ по защите информации представлен на рисунке 6.

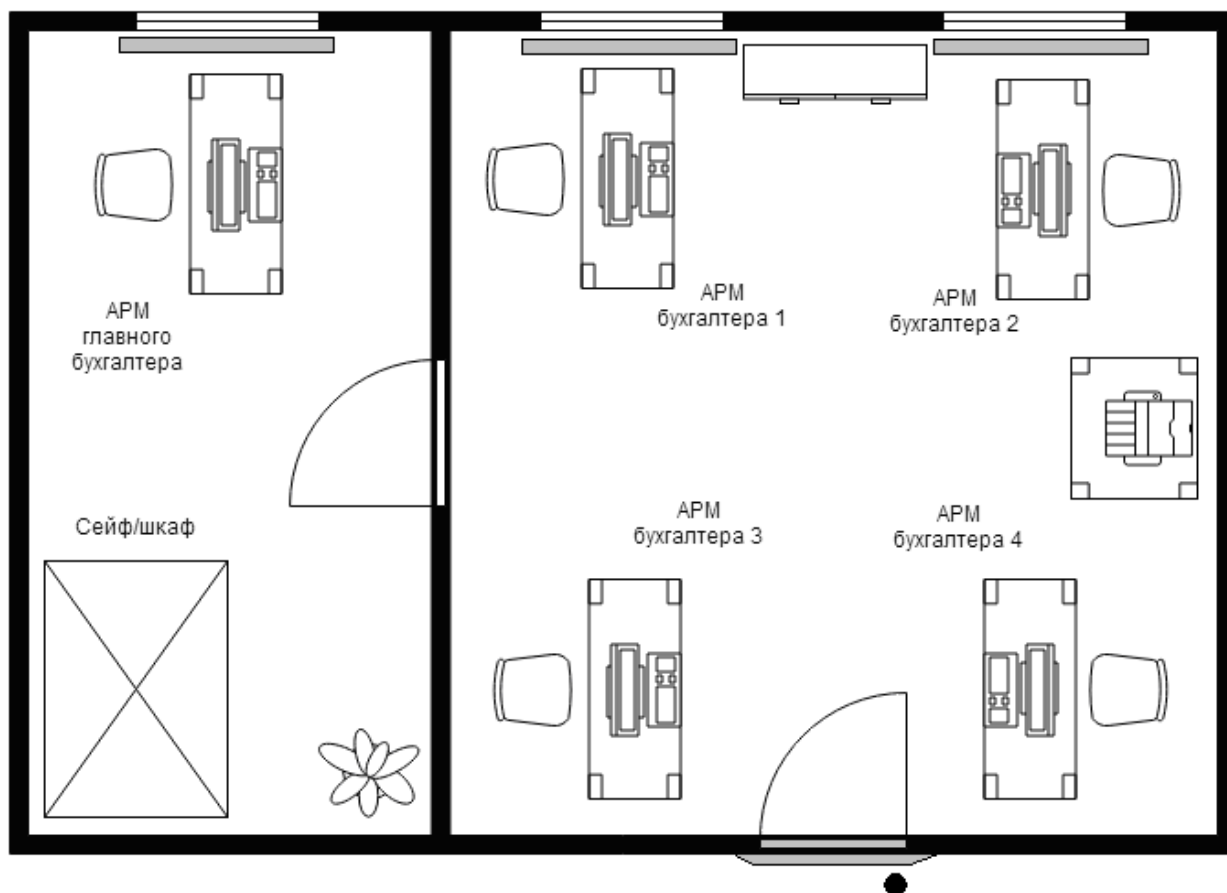


Рисунок 6 – Обновленный план помещения бухгалтерии

Структура АС «Бухгалтерия» после применения защитных мер приведена на рисунке 7.

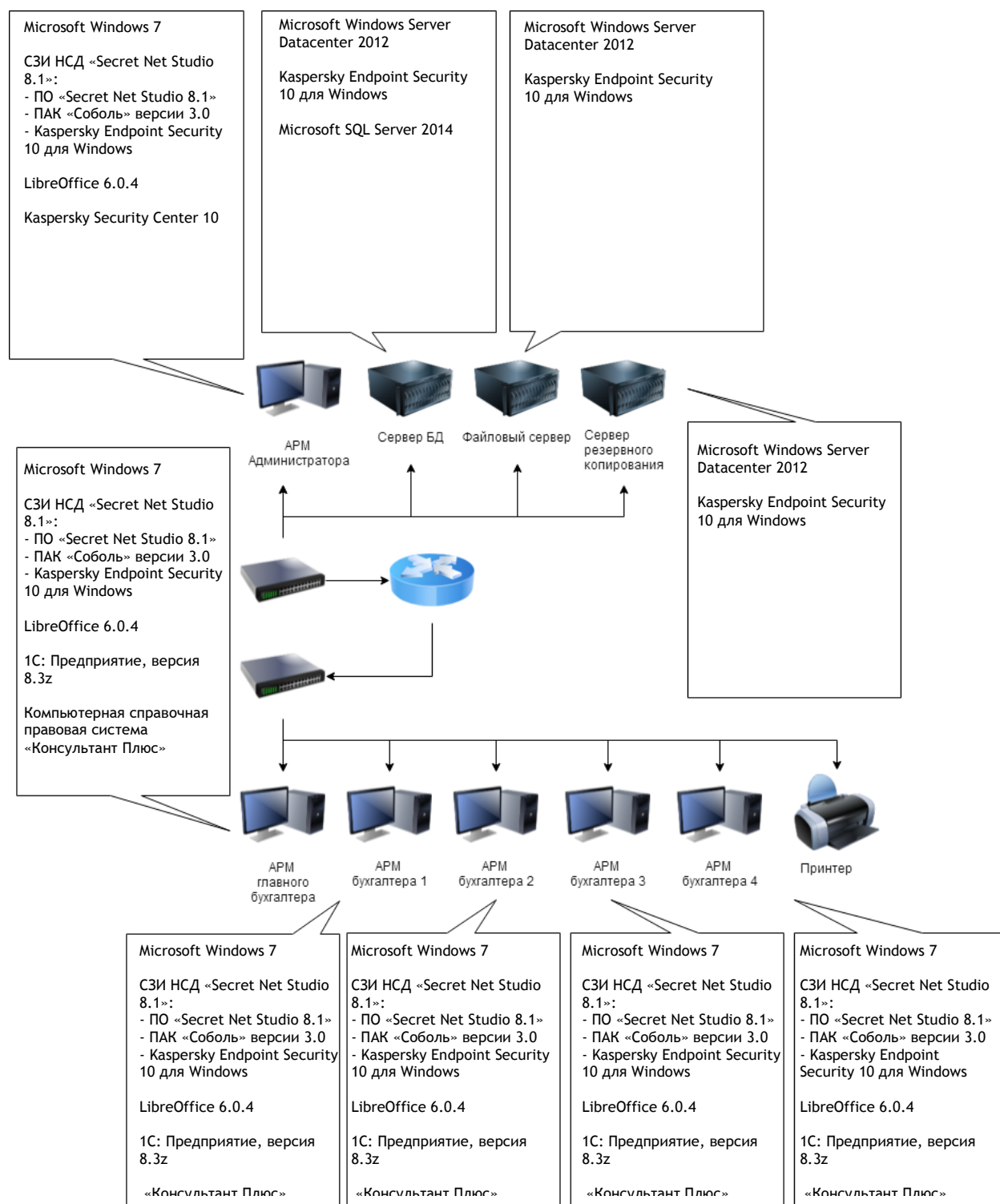


Рисунок 7 – Структура АСЗИ «Бухгалтерия»

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

При выполнении задач специалисты в области защиты информации подвержены воздействию опасных и вредных производственных факторов. Соответственно, специалисты должны быть осведомлены и проинструктированы о воздействии тех или иных негативных факторов.

К вредным и опасным производственным факторам относятся: физические, химические, биологические и психофизиологические[7].

Последние подразделяются на: недостаток или отсутствие естественного освещения, слабое искусственное освещение АРМ, повышенная яркость и контрастность света, зрительное напряжение.

Деятельность специалиста в области защиты информации связана с обработкой больших объёмов информации, использовании АРМ, реализации необходимых решений в короткие сроки.

Продолжительная работа на АРМ (работа за монитором) способствует чрезмерной нагрузке на компоненты зрительного аппарата, а также способствует появлению усталости и переутомлению глазного анализатора, что является причиной большинства болезней органов зрения.

Такая работа вызывает заболевания глаз, а именно: боль и резь в глазах, их покраснения, возникновение пелены, раздвоение предметов, неприятное мерцание, чрезмерную утомляемость и т.д. Это влечет за собой нарушение зрительных органов и снижение работоспособности специалиста.

Специалистам в области ИБ необходима регулярная проверка зрения, направленная на поддержание и улучшение здоровья глаз.

С целью снизить риски возникновения заболеваний глаз, важно соблюдать правила безопасности, также необходимо прибегать к методам, обеспечивающим расслабление глазного аппарата.

На основе выявленных опасных факторов, были выбраны методы и средства обеспечения безопасности работы на АРМ, описанные ниже.

Необходимо избегать излишнего напряжения глаз. Для их защиты не следует длительное время фокусироваться на одном и том же предмете. Рекомендуется, в качестве профилактики, время от времени отвлекаться и переводить взгляд на предметы вдаль, что поспособствует четкости объектов на сетчатке, а также позволит сохранить упругость мышц глаз.

Успешно себя зарекомендовала методика У. Г. Бейтса Пальминга. Простая тренировка для глаз, направленная на расслабление мышц глаза и восстановление зрения. На глаза следует положить ладони обеих рук, таким образом, чтоб пальцы рук перекрещивались на лбу. Так необходимо находиться на протяжении 5 минут. Упражнение выполняется без усилий, чтобы не вызвать напряжения на глаза.

Моргание – простая и эффективная профилактика, обеспечивающая временный отдых для глаз. Слезная жидкость имеет дезинфицирующие и увлажняющие свойства:

- укрепление нервных волокон сетчатки;
- обеспечение расслабления глазных мышц;
- улучшение способности глаза фокусироваться на изображении.

Глазам необходим не только в периодический отдых и расслабление, но естественный свет. Чтобы предотвратить ухудшение зрения следует постоянно укреплять сетчатку. Каждый день следует начинать с принятия световых ванн (соляризации). Рекомендуется подставить закрытые глаза на несколько минут солнцу, либо, при его отсутствии, другому источнику света. Это усилит кровообращение, нормализуются процессы в глазных мышцах, повысится вероятность сохранения зрения.

Значимый фактор, влияющий на остроту зрения и предотвращающий его ухудшение, это правильная освещенность. От искусственного освещения не должна чувствоваться резь в глазах, но оно должно быть ярким. Чтобы сохранить зрение при работе за письменным столом, рекомендуется

использовать настольные лампы мощностью 60 Вт с плафонами. Источник искусственного освещения следует располагать слева (у правшей) в 50 см от документов.

Выполнение перечисленных упражнений для глаз способствует их расслаблению и тренировке, а также снизит воздействие вредных психофизиологических факторов, влияющих на работу.

Заключение

В ходе выполнения выпускной квалификационной работы было описано текущее состояние автоматизированной системы «Бухгалтерия». Были выявлены и описаны информационные системы персональных данных в бухгалтерии. Была разработана модель нарушителя и модель угроз персональных данных бухгалтерии. Были определены уровни защищенности информационных систем персональных данных бухгалтерии. Были определены организационные и организационно-технические требования к обеспечению уровней защищенности персональных данных в информационных системе персональных данных бухгалтерии. Были выбраны и обоснованы выбранные средства защиты информации для автоматизированной системы «Бухгалтерия» в защищенном исполнении. Была описана автоматизированная система бухгалтерии на ФГУП ФНПЦ «ПО «Старт» им. М.В.Проценко» в защищенном исполнении. Были описанные вредные психофизиологические факторы, влияющие на органы зрения специалиста по защите информации, методы и средства физической культуры, снижающие их воздействие.

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

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

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

Список используемых 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)